5 802.1X ................................................. 85
   Important Points to Remember ........................................ 86

6 Access Control Lists (ACL) ........................................ 101
   Overview ........................................................................ 101
   Commands Common to all ACL Types ................................ 101
   Common IP ACL Commands ............................................. 104
   Standard IP ACL Commands ........................................... 108
   Extended IP ACL Commands .......................................... 112
   Common MAC Access List Commands ................................ 127
   Standard MAC ACL Commands ....................................... 130
   Extended MAC ACL Commands ...................................... 133
   IP Prefix List Commands .............................................. 137
   Route Map Commands .................................................. 142

7 Bidirectional Forwarding Detection (BFD) ......................... 153
   Overview ........................................................................ 153
   Commands ..................................................................... 153

8 Border Gateway Protocol IPv4 (BGPv4) ............................. 165
   Overview ........................................................................ 165
   BGPv4 Commands .......................................................... 165
   MBGP Commands .......................................................... 234
   BGP Extended Communities (RFC 4360) ............................ 234
   IPv6 BGP Commands ..................................................... 239
   IPv6 MBGP Commands .................................................. 242

9 Content Addressable Memory (CAM) ............................... 243
   Overview ........................................................................ 243
   CAM Profile Commands .................................................. 243
   Important Points to Remember ........................................ 243

10 Control Plane Policing (CoPP) ....................................... 249
   Overview ........................................................................ 249
   Commands ..................................................................... 249

11 Data Center Bridging .................................................... 253
   Overview ........................................................................ 253
   DCB Command ............................................................... 253
   PFC Commands ............................................................. 253
   ETS Commands ............................................................. 254
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>575</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>575</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>575</td>
</tr>
<tr>
<td></td>
<td>LLDP-MED Commands</td>
<td>583</td>
</tr>
<tr>
<td>30</td>
<td>Multicast Source Discovery Protocol (MSDP)</td>
<td>591</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>591</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>591</td>
</tr>
<tr>
<td>31</td>
<td>Multiple Spanning Tree Protocol (MSTP)</td>
<td>601</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>601</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>601</td>
</tr>
<tr>
<td>32</td>
<td>Multicast</td>
<td>615</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>615</td>
</tr>
<tr>
<td></td>
<td>IPv4 Multicast Commands</td>
<td>615</td>
</tr>
<tr>
<td></td>
<td>IPv6 Multicast Commands</td>
<td>620</td>
</tr>
<tr>
<td>33</td>
<td>Neighbor Discovery Protocol (NDP)</td>
<td>623</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>623</td>
</tr>
<tr>
<td>34</td>
<td>Open Shortest Path First (OSPF)</td>
<td>627</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>627</td>
</tr>
<tr>
<td></td>
<td>OSPFv2 Commands</td>
<td>627</td>
</tr>
<tr>
<td></td>
<td>OSPFv3 Commands</td>
<td>677</td>
</tr>
<tr>
<td>35</td>
<td>Port Monitoring</td>
<td>695</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>695</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>695</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
<td>695</td>
</tr>
<tr>
<td>36</td>
<td>PIM-Sparse Mode (PIM-SM)</td>
<td>701</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>701</td>
</tr>
<tr>
<td></td>
<td>IPv4 PIM-Sparse Mode Commands</td>
<td>701</td>
</tr>
<tr>
<td></td>
<td>IPv6 PIM-Sparse Mode Commands</td>
<td>721</td>
</tr>
<tr>
<td>37</td>
<td>Private VLAN (PVLAN)</td>
<td>731</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>731</td>
</tr>
<tr>
<td></td>
<td>Private VLAN Concepts</td>
<td>732</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>38</td>
<td>Per-VLAN Spanning Tree Plus (PVST+)</td>
<td>741</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>741</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>741</td>
</tr>
<tr>
<td>39</td>
<td>Quality of Service (QoS)</td>
<td>753</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>753</td>
</tr>
<tr>
<td></td>
<td>Global Configuration Commands</td>
<td>753</td>
</tr>
<tr>
<td></td>
<td>Per-Port QoS Commands</td>
<td>754</td>
</tr>
<tr>
<td></td>
<td>Policy-Based QoS Commands</td>
<td>759</td>
</tr>
<tr>
<td>40</td>
<td>Routing Information Protocol (RIP)</td>
<td>783</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>783</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>783</td>
</tr>
<tr>
<td>41</td>
<td>Remote Monitoring (RMON)</td>
<td>799</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>799</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>799</td>
</tr>
<tr>
<td>42</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
<td>811</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>811</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>811</td>
</tr>
<tr>
<td>43</td>
<td>Security</td>
<td>823</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>823</td>
</tr>
<tr>
<td></td>
<td>AAA Accounting Commands</td>
<td>823</td>
</tr>
<tr>
<td></td>
<td>Authorization and Privilege Commands</td>
<td>823</td>
</tr>
<tr>
<td></td>
<td>Authentication and Password Commands</td>
<td>826</td>
</tr>
<tr>
<td></td>
<td>RADIUS Commands</td>
<td>829</td>
</tr>
<tr>
<td></td>
<td>TACACS+ Commands</td>
<td>840</td>
</tr>
<tr>
<td></td>
<td>SSH Server and SCP Commands</td>
<td>844</td>
</tr>
<tr>
<td></td>
<td>Secure DHCP Commands</td>
<td>847</td>
</tr>
<tr>
<td></td>
<td></td>
<td>858</td>
</tr>
<tr>
<td>44</td>
<td>sFlow</td>
<td>863</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>863</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
<td>863</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>864</td>
</tr>
<tr>
<td>45</td>
<td>Service Provider Bridging</td>
<td>871</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>871</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
<td>871</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
<td>871</td>
</tr>
</tbody>
</table>
About this Guide

This book provides information about the Dell Networking operating software (FTOS) command line interface (CLI). It includes some information about the protocols and features found in FTOS and on the Dell Networking systems supported by FTOS.

This chapter includes:
• Objectives
• Audience
• Conventions
• Information Symbols
• Related Documents

Objectives

This document is intended as a reference guide for the FTOS CLI commands, with detailed syntax statements, usage information, and sample output examples.

For details about when to use the commands, refer to the FTOS Configuration Guide. This guide contains an Appendix with a list of the request for comment (RFCs) and management information base files (MIBs) supported.

Audience

This document is intended for system administrators who are responsible for configuring or maintaining networks. This document assumes you are knowledgeable in Layer 2 and Layer 3 networking technologies.

Conventions

This document uses the following conventions to describe command syntax:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyword</td>
<td>Keywords are in bold and must be entered in the CLI as listed.</td>
</tr>
<tr>
<td>parameter</td>
<td>Parameters are in italics and require a number or word to be entered in the CLI.</td>
</tr>
<tr>
<td>{X}</td>
<td>Keywords and parameters within braces must be entered in the CLI.</td>
</tr>
<tr>
<td>[X]</td>
<td>Keywords and parameters within brackets are optional.</td>
</tr>
</tbody>
</table>
Table 1-1 describes the symbols contained in this document.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Brief</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📑</td>
<td>Note</td>
<td>This symbol signals important operational information.</td>
</tr>
<tr>
<td>△</td>
<td>Caution</td>
<td>This symbol signals information about situations that could result in equipment damage or loss of data.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Warning</td>
<td>This symbol signals information about hardware handling that could result in injury.</td>
</tr>
</tbody>
</table>

Related Documents

For more information about the system, refer to the following documents:

- *FTOS Configuration Guide*
- *Installation and maintenance guides* for the MXL 10/40GbE Switch system
- *Release Notes* for the MXL 10/40GbE Switch system and FTOS version 8.3.16.4
CLI Basics

This chapter describes the command structure and command modes. The Dell Networking operating software (FTOS) commands are in a text-based interface that allows you to use launch commands, change the command modes, and configure interfaces and protocols.

This chapter includes the following sections:

- Accessing the Command Line
- Multiple Configuration Users
- Navigating the Command Line Interface
- Obtaining Help
- Using the Keyword no
- Filtering show Commands
- Command Modes

Accessing the Command Line

When the system boots successfully, you are positioned on the command line in EXEC mode and not prompted to log in. You can access the commands through a serial console port or a Telnet session. When you Telnet into the switch, you are prompted to enter a login name and password.

Figure 2-1 is an example of a successful Telnet login session.

Figure 2-1. Login Example

```
telnet 172.31.1.53
Trying 172.31.1.53...
Connected to 172.31.1.53.
Escape character is '^]'.
Login: username
Password:
FTOS>
```

After you log into the switch, the prompt provides you with current command-level information (Table 2-1).
Multiple Configuration Users

When a user enters CONFIGURATION mode and another user(s) is already in that configuration mode, FTOS generates an alert warning message similar to Figure 2-2:

Figure 2-2. Configuration Mode User Alert

```
FTOS#conf
 % Warning: The following users are currently configuring the system:
User "" on line console0
User "admin" on line vty0 (123.12.1.123)
User "admin" on line vty1 (123.12.1.123)
User "Irene" on line vty3 (123.12.1.321)
FTOS#conf
```

When another user enters CONFIGURATION mode, FTOS sends a message similar to the following, (the user in this case is “admin” on vty2):

```
% Warning: User "admin" on line vty2 "172.16.1.210" is in configuration
```

Navigating the Command Line Interface

The command line interface (CLI) prompt displayed by FTOS is comprised of:

- “hostname”— the initial part of the prompt, “FTOS” by default. You can change it with the `hostname` command, as described in `hostname`.
- The second part of the prompt, reflecting the current CLI mode, is shown in Table 2-1.

The CLI prompt changes as you move up and down the levels of the command structure.

Table 2-1 lists the prompts and their corresponding command levels, called modes. Starting with CONFIGURATION mode, the command prompt adds modifiers to further identify the mode. The command modes are explained in Command Modes.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>CLI Command Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS-&gt;</td>
<td>EXEC</td>
</tr>
<tr>
<td>FTOS#</td>
<td>EXEC Privilege</td>
</tr>
<tr>
<td>FTOS(conf)#</td>
<td>CONFIGURATION</td>
</tr>
<tr>
<td>FTOS(conf-if)#</td>
<td>INTERFACE</td>
</tr>
<tr>
<td>FTOS(conf-if-te-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-fo-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-lo-0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-nu-0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-po-1)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-vl-1)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-range)#</td>
<td></td>
</tr>
</tbody>
</table>
Table 2-1. Command Prompt and Corresponding Command Mode

<table>
<thead>
<tr>
<th>Prompt</th>
<th>CLI Command Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS(conf-ext-nacl)#</td>
<td>IP ACCESS LIST</td>
</tr>
<tr>
<td>FTOS(conf-std-nacl)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-line-console)#</td>
<td>LINE</td>
</tr>
<tr>
<td>FTOS(conf-line-vty)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-ext-macl)#</td>
<td>MAC ACCESS LIST</td>
</tr>
<tr>
<td>FTOS(conf-std-macl)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-mon-sess)#</td>
<td>MONITOR SESSION</td>
</tr>
<tr>
<td>FTOS(conf-stp)#</td>
<td>STP</td>
</tr>
<tr>
<td>FTOS(conf-mstp)#</td>
<td>MULTIPLE SPANNING TREE</td>
</tr>
<tr>
<td>FTOS(conf-pvst)#</td>
<td>Per-VLAN SPANNING TREE Plus</td>
</tr>
<tr>
<td>FTOS(conf-rstp)#</td>
<td>RAPID SPANNING TREE</td>
</tr>
<tr>
<td>FTOS(conf-gvrp)#</td>
<td>PROTOCOL GVRP</td>
</tr>
<tr>
<td>FTOS(conf-route-map)#</td>
<td>ROUTE-MAP</td>
</tr>
<tr>
<td>FTOS(conf-nprefixl)#</td>
<td>PREFIX-LIST</td>
</tr>
<tr>
<td>FTOS(conf-router_rip)#</td>
<td>ROUTER RIP</td>
</tr>
<tr>
<td>FTOS(conf-router_ospf)#</td>
<td>ROUTER OSPF</td>
</tr>
<tr>
<td>FTOS(conf-stp)#</td>
<td>SPANNING TREE</td>
</tr>
</tbody>
</table>

Obtaining Help

As soon as you are in a command mode, there are several ways to access help.

- To obtain a list of keywords at any command mode, do the following:
  - Enter a ? at the prompt or after a keyword. There must always be a space before the ?.
- To obtain a list of keywords with a brief functional description, do the following:
  - Enter help at the prompt.
- To obtain a list of available options, do the following:
  - Type a keyword followed by a space and a ?
- Type a partial keyword followed by a ?
  - A display of keywords beginning with the partial keyword is listed.
Figure 2-3 shows the results of entering `ip ?` at the prompt.

**Figure 2-3.  Partial Keyword Example**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>Named access-list</td>
</tr>
<tr>
<td>control-plane</td>
<td>Control plane configuration</td>
</tr>
<tr>
<td>dhcp</td>
<td>DHCP configuration commands</td>
</tr>
<tr>
<td>domain-list</td>
<td>Domain name to complete unqualified host name</td>
</tr>
<tr>
<td>domain-lookup</td>
<td>Enable IP Domain Name System hostname translation</td>
</tr>
<tr>
<td>domain-name</td>
<td>Define the default domain name</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP configuration commands</td>
</tr>
<tr>
<td>helper-address</td>
<td>DHCP relay agent configuration</td>
</tr>
<tr>
<td>host</td>
<td>Add an entry to the ip hostname table</td>
</tr>
<tr>
<td>igmp</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>max-frag-count</td>
<td>Max. fragmented packets allowed in IP re-assembly</td>
</tr>
<tr>
<td>mroute</td>
<td>Multicast routes and counters</td>
</tr>
<tr>
<td>msdp</td>
<td>Multicast source discovery protocol</td>
</tr>
<tr>
<td>multicast-limit</td>
<td>Max entries in Multicast TIB</td>
</tr>
<tr>
<td>multicast-mdsp</td>
<td>Enable IP multicast MSDP protocol</td>
</tr>
<tr>
<td>multicast-routing</td>
<td>Enable IP multicast forwarding</td>
</tr>
<tr>
<td>name-server</td>
<td>Specify address of name server to use</td>
</tr>
<tr>
<td>pim</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>prefix-list</td>
<td>Build a prefix list</td>
</tr>
<tr>
<td>radius</td>
<td>Interface configuration for RADIUS</td>
</tr>
<tr>
<td>route</td>
<td>Establish static routes</td>
</tr>
<tr>
<td>scp</td>
<td>SCP configuration commands</td>
</tr>
<tr>
<td>source-route</td>
<td>Process packets with source routing header options</td>
</tr>
<tr>
<td>ssh</td>
<td>SSH configuration commands</td>
</tr>
<tr>
<td>tacacs</td>
<td>Interface configuration for TACACS+</td>
</tr>
<tr>
<td>telnet</td>
<td>Specify telnet options</td>
</tr>
<tr>
<td>tftp</td>
<td>TFTP configuration commands</td>
</tr>
</tbody>
</table>

When entering commands, you can take advantage of the following time saving features:

- The commands are not case sensitive.
- You can enter partial (truncated) command keywords. For example, you can enter `int tengig` *interface* for the `interface tengigabitethernet interface` command.
- Use the **TAB** key to complete keywords in commands.
- Use the **up arrow** key to display the last enabled command.
- Use either the **Backspace** key or the **Delete** key to erase the previous character.
Use the **left** and **right arrow** keys to navigate left or right in the FTOS command line. Table 2-2 defines the key combinations valid at the FTOS command line.

### Table 2-2.  Short-cut Keys and their Actions

<table>
<thead>
<tr>
<th>Key Combination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNTL-A</td>
<td>Moves the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>CNTL-B</td>
<td>Moves the cursor back one character.</td>
</tr>
<tr>
<td>CNTL-D</td>
<td>Deletes character at cursor.</td>
</tr>
<tr>
<td>CNTL-E</td>
<td>Moves the cursor to the end of the line.</td>
</tr>
<tr>
<td>CNTL-F</td>
<td>Moves the cursor forward one character.</td>
</tr>
<tr>
<td>CNTL-I</td>
<td>Completes a keyword.</td>
</tr>
<tr>
<td>CNTL-K</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>CNTL-N</td>
<td>Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key</td>
</tr>
<tr>
<td>CNTL-P</td>
<td>Recalls commands, beginning with the last command</td>
</tr>
<tr>
<td>CNTL-U</td>
<td>Deletes the line.</td>
</tr>
<tr>
<td>CNTL-W</td>
<td>Deletes the previous word.</td>
</tr>
<tr>
<td>CNTL-X</td>
<td>Deletes the line.</td>
</tr>
<tr>
<td>CNTL-Z</td>
<td>Comes back to EXEC mode from any CONFIGURATION mode</td>
</tr>
<tr>
<td>Esc B</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc F</td>
<td>Moves the cursor forward one word.</td>
</tr>
<tr>
<td>Esc D</td>
<td>Deletes all characters from the cursor to the end of the word.</td>
</tr>
</tbody>
</table>

### Using the Keyword no

To disable, delete, or return to default values, use the `no` form of the commands. For most commands, if you type the keyword `no` in front of the command, you will disable that command or delete it from the running configuration. In this document, the `no` form of the command is described in the “Command Syntax” portion of the command description.

### Filtering show Commands

You can filter the display output of a `show` command to find specific information, to display certain information only, or to begin the command output at the first instance of a regular expression or phrase.

When you execute a `show` command, followed by a pipe ( | ) and one of the parameters listed below and a regular expression, the resulting output either excludes or includes those parameters, as defined by the parameter:

- **except** — display only text that does not match the pattern (or regular expression)
- **find** — search for the first occurrence of a pattern
- **grep** — display text that matches a pattern
no-more — do not paginate the display output
save — copy output to a file for future use

Note: FTOS accepts a space before or after the pipe, no space before or after the pipe, or any combination. For example:

```
FTOS#command | grep ten|gigabit |except regular-expression | find regular-expression
```

The `grep` command option has an `ignore-case` sub-option that makes the search case-insensitive. For example, the commands:

- show run | grep Ethernet returns a search result with instances containing a capitalized “Ethernet,” such as interface TenGigabitEthernet 0/0.
- show run | grep ethernet does not return the search result above because it only searches for instances containing a non-capitalized “ethernet”.
- show run | grep Ethernet ignore-case returns instances containing both “Ethernet” and “ethernet”.

Displaying All Output

To display the output all at once (not one screen at a time), use the no-more command after the pipe. This is similar to the terminal length `screen-length` command except that the no-more option affects the output of just the specified command. For example:

```
FTOS#show running-config | no-more
```

Filtering Command Output Multiple Times

You can filter a single command output multiple times. To do this, place the `save` option as the last filter. For example:

```
FTOS# command | grep regular-expression | except regular-expression | grep other-regular-expression | find regular-expression | no-more | save
```

Command Modes

To navigate to various CLI modes, use specific commands to launch each mode. Navigation to these modes is described in the following sections.

EXEC Mode

When you initially log in to the switch, by default you are logged into EXEC mode. This mode allows you to view settings and to enter EXEC Privilege mode to configure the device. While you are in EXEC mode, the `>` prompt is displayed following the “hostname” prompt (which is “FTOS” by default). You can change this using the `hostname` command. For more information, refer to the `hostname` command. Each mode prompt is preceded by the hostname.
EXEC Privilege Mode

The `enable` command accesses EXEC Privilege mode. If an administrator has configured an `Enable` password, you are prompted to enter the password here.

EXEC Privilege mode allows you to access all commands accessible in EXEC mode, plus other commands, such as to clear ARP entries and IP addresses. In addition, you can access CONFIGURATION mode to configure interfaces, routes, and protocols on the switch. While you are logged in to EXEC Privilege mode, the `#` prompt displays.

CONFIGURATION Mode

In EXEC Privilege mode, use the `configure` command to enter CONFIGURATION mode and configure routing protocols and access interfaces.

To enter CONFIGURATION mode:

1. Verify that you are logged in to EXEC Privilege mode.
2. Enter the `configure` command. The prompt changes to include (conf).

From this mode, you can enter INTERFACE mode by using the `interface` command.

INTERFACE Mode

Use INTERFACE mode to configure interfaces or IP services on those interfaces. An interface can be physical (for example, a TenGigabit Ethernet port) or virtual (for example, the Null interface).

To enter INTERFACE mode:

1. Verify that you are logged into CONFIGURATION mode.
2. Enter the `interface` command followed by an interface type and interface number that is available on the switch.
3. The prompt changes to include the designated interface and slot/port number (Table 2-3).

Table 2-3. Interface prompts

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Interface Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS(conf-if)#</td>
<td>INTERFACE mode</td>
</tr>
<tr>
<td>FTOS(conf-if-te-0/0)#</td>
<td>Ten Gigabit Ethernet interface followed by slot/port information</td>
</tr>
<tr>
<td>FTOS(conf-if-fo-0/0)#</td>
<td>Forty Gigabit Ethernet interface followed by slot/port information</td>
</tr>
<tr>
<td>FTOS(conf-if-lo-0)#</td>
<td>Loopback interface number.</td>
</tr>
<tr>
<td>FTOS(conf-if-nu-0)#</td>
<td>Null Interface followed by zero</td>
</tr>
<tr>
<td>FTOS(conf-if-po-1)#</td>
<td>Port-channel interface number</td>
</tr>
<tr>
<td>FTOS(conf-if-vl-1)#</td>
<td>VLAN Interface followed by VLAN number (range 1 to 4094)</td>
</tr>
<tr>
<td>FTOS(conf-if-ma-0/0)#</td>
<td>Management Ethernet interface followed by slot/port information</td>
</tr>
<tr>
<td>FTOS(conf-if-range)#</td>
<td>Designated interface range (used for bulk configuration; refer to interface range).</td>
</tr>
</tbody>
</table>
LINE Mode

Use LINE mode to configure console or virtual terminal parameters.

To enter LINE mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the line command. You must include the keywords console or vty and their line number available on the switch. The prompt changes to include (config-line-console) or (config-line-vty).

You can exit this mode by using the exit command.

MAC ACCESS LIST Mode

While in CONFIGURATION mode, use the mac access-list standard or mac access-list extended commands to enter MAC ACCESS LIST mode and configure either standard or extended access control lists (ACL).

To enter MAC ACCESS LIST mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Use the mac access-list standard or mac access-list extended command. You must include a name for the ACL. The prompt changes to include (conf-std-macl) or (conf-ext-macl).

You can return to CONFIGURATION mode by using the exit command.

IP ACCESS LIST Mode

While in CONFIGURATION mode, use the ip access-list standard or ip access-list extended commands to enter IP ACCESS LIST mode and configure either standard or extended access control lists (ACL).

To enter IP ACCESS LIST mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Use the ip access-list standard or ip access-list extended command. You must include a name for the ACL. The prompt changes to include (conf-std-nacl) or (conf-ext-nacl).

You can return to CONFIGURATION mode by using the exit command.

ROUTE-MAP Mode

While in CONFIGURATION mode, use the route-map command to enter ROUTE-MAP mode and configure a route map.

To enter ROUTE-MAP mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Use the route-map map-name [permit | deny] [sequence-number] command. The prompt changes to include (route-map).

You can return to CONFIGURATION mode by using the exit command.
**PREFIX-LIST Mode**

While in CONFIGURATION mode, use the `ip prefix-list` command to enter PREFIX-LIST mode and configure a prefix list.

To enter PREFIX-LIST mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip prefix-list` command. You must include a name for the prefix list. The prompt changes to include (conf-nprefixl).

You can return to CONFIGURATION mode by using the `exit` command.

**SPANNING TREE Mode**

Use STP mode to enable and configure the spanning tree protocol (STP), as described in Spanning Tree Protocol (STP).

To enter STP mode:
1. Verify that you are logged into CONFIGURATION mode.
2. Enter the `protocol spanning-tree 0` command.

You can return to CONFIGURATION mode by using the `exit` command.

**Per-VLAN SPANNING TREE Plus Mode**

Use PVST+ mode to enable and configure the per-VLAN spanning tree (PVST+) protocol, as described in Per-VLAN Spanning Tree Plus (PVST+).

- **Note:** The protocol is PVST+, but the plus sign is dropped at the CLI prompt.

To enter PVST+ mode:
1. Verify that you are logged into CONFIGURATION mode.
2. Enter the `protocol spanning-tree pvst` command.

You can return to CONFIGURATION mode by using the `exit` command.

**RAPID SPANNING TREE Mode**

Use RSTP mode to enable and configure the rapid spanning tree protocol (RSTP), as described in Rapid Spanning Tree Protocol (RSTP).

To enter RSTP mode:
1. Verify that you are logged into CONFIGURATION mode.
2. Enter the `protocol spanning-tree rstp` command.

You can return to CONFIGURATION mode by using the `exit` command.
MULTIPLE SPANNING TREE Mode

Use MULTIPLE SPANNING TREE mode to enable and configure the multiple spanning tree protocol (MSTP), as described in Multiple Spanning Tree Protocol (MSTP).

To enter MULTIPLE SPANNING TREE mode:
1. Verify that you are logged into CONFIGURATION mode.
2. Enter the protocol spanning-tree mstp command.
You can return to CONFIGURATION mode by using the exit command.

PROTOCOL GVRP Mode

Use the PROTOCOL GVRP mode to enable and configure generic attribute registration protocol (GARP) virtual LAN (VLAN) registration protocol (GVRP), as described in GARP VLAN Registration (GVRP).

To enter PROTOCOL GVRP mode:
1. Verify that you are logged into CONFIGURATION mode.
2. Enter the protocol gvrp command syntax.
You can return to CONFIGURATION mode by using the exit command.

ROUTER OSPF Mode

Use the ROUTER OSPF mode to configure open shortest path first (OSPF), as described in Open Shortest Path First (OSPF).

To enter ROUTER OSPF mode:
1. Verify that you are logged into CONFIGURATION mode.
2. Use the router ospf {process-id} command. The prompt changes to include (conf-router_ospf-id).
You can switch to INTERFACE mode by using the interface command or you can switch to ROUTER RIP mode by using the router rip command.

ROUTER RIP Mode

Use the ROUTER RIP mode to configure routing information protocol (RIP), as described in Routing Information Protocol (RIP).

To enter ROUTER RIP mode:
1. Verify that you are logged into CONFIGURATION mode.
2. Enter the router rip command. The prompt changes to include (conf-router_rip).
You can switch to INTERFACE mode by using the interface command or you can switch to ROUTER OSPF mode by using the router ospf command.
File Management

Overview

This chapter contains commands needed to manage the configuration files and includes other file management commands found in the Dell Networking operating software (FTOS).

Basic File Management Commands

The commands included in this chapter are:

- cd
- copy
- copy running-config startup-config
- delete
- dir
- format flash
- logging coredump
- logging coredump server
- pwd
- rename
- show boot system
- show file
- show file-systems
- show os-version
- show running-config
- show startup-config
- show version
- upgrade boot
- upgrade system
cd

Change to a different working directory.

**Syntax**

```
cd directory
```

**Parameters**

- `directory` (OPTIONAL) Enter one of the following:
  - `flash`: (internal Flash) or any sub-directory
  - `usbflash`: (external Flash) or any sub-directory

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**copy**

Copy one file to another location. FTOS supports IPv4 addressing for FTP, TFTP, and SCP (in the `hostip` field).

**Syntax**

```
copy source-file-url destination-file-url
```

**Parameters**

- `file-url` Enter the following location keywords and information:
  - To copy a file from the internal FLASH, enter `flash://` followed by the filename.
  - To copy the running configuration, enter the keyword `running-config`.
  - To copy the startup configuration, enter the keyword `startup-config`.
  - To copy a file on the external FLASH, enter `usbflash://` followed by the filename.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

FTOS supports a maximum of 100 files, at the root directory level, on both the internal and external Flash.

The `usbflash` commands are supported. For a list of approved USB vendors, refer to the FTOS Release Notes.

When copying a file to a remote location (for example, using Secure Copy [SCP]), enter only the keywords and FTOS prompts you for the rest of the information.

For example, when using SCP, you can enter `copy running-config scp:`

The `running-config` is the source, and the target is specified in the ensuing prompts. FTOS prompts you to enter any required information, as needed for the named destination—remote destination, destination filename, user ID and password, etc.

When you use the `copy running-config startup-config` command to copy the running configuration (the startup configuration file amended by any configuration changes made since the system was started) to the startup configuration file, FTOS creates a backup file on the internal flash of the startup configuration.
FTOS supports copying the running-configuration to a TFTP server or to an FTP server:

```
copy running-config tftp:
copy running-config ftp:
```

**Example**

**Figure 3-1.  copy running-config scp: Command Example**

```plaintext
FTOS#copy running-config scp:
Address or name of remote host []: 10.10.10.1
Port number of the server [22]: 99
Destination file name [startup-config]: old_running
User name to login remote host: sburgess
Password to login remote host:
Password to login remote host? dilling
```

In this example — **copy scp: flash:** — specifying SCP in the first position indicates that the target is to be specified in the ensuing prompts. Entering **flash:** in the second position means that the target is the internal Flash. In this example the source is on a secure server running SSH, so the user is prompted for the UDP port of the SSH server on the remote host.

**Example**

**Figure 3-2.  Using scp to copy from an SSH Server**

```plaintext
FTOS#copy scp: flash:
Address or name of remote host []: 10.11.199.134
Port number of the server [22]: 99
Source file name []: test.cfg
User name to login remote host: admin
Password to login remote host:
Destination file name [test.cfg]: test1.cfg
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the working directory.</td>
</tr>
</tbody>
</table>

**copy running-config startup-config**

Copy running configuration to the startup configuration.

**Syntax**

```
copy running-config startup-config {duplicate}
```

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

This command is useful for quickly making a changed configuration on one chassis available on external flash in order to move it to another chassis.
delete

Delete a file from the flash. Once deleted, files cannot be restored.

Syntax

```
delete flash: ([flash://]filepath) usbflash ([usbflash://]filepath)
```

Parameters

- `flash-url` Enter the following location and keywords:
  - For a file or directory on the internal Flash, enter `flash://` followed by the filename or directory name.
  - For a file or directory on the external Flash, enter `usbflash://` followed by the filename or directory name.

- `no-confirm` (OPTIONAL) Enter the keyword `no-confirm` to specify that FTOS does not require user input for each file prior to deletion.

Command Modes

- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

dir

Display the files in a file system. The default is the current directory.

Syntax

```
dir [filename | directory name:]
```

Parameters

- `filename | directory name:` (OPTIONAL) Enter one of the following:
  - For a file or directory on the internal Flash, enter `flash://` followed by the filename or directory name.
  - For a file or directory on the external Flash, enter `usbflash://` followed by the filename or directory name:

Command Modes

- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```
FTOS#dir
Directory of flash:
  1  drwx  4096  Jan 01 1980 00:00:00 +00:00.
  2  drwx  2048  Mar 06 2010 00:36:21 +00:00 ..
  3  drwx  4096  Feb 25 2010 23:32:50 +00:00 TRACE_LOG_DIR
  4  drwx  4096  Feb 25 2010 23:32:50 +00:00 CORE_DUMP_DIR
  5  d---  4096  Feb 25 2010 23:32:50 +00:00 ADMIN_DIR
  6  -rwx  720969768  Mar 05 2010 03:25:40 +00:00 6gb
  7  -rwx  4260  Mar 03 2010 22:04:50 +00:00 prem-23-5-12
  8  -rwx  31969685  Mar 05 2010 17:56:26 +00:00 FTOS-XL-8-3-16-148.bin
  9  -rwx  3951  Mar 06 2010 00:36:18 +00:00 startup-config
flash: 2143281152 bytes total (1389801472 bytes free)
FTOS#
```

Related Commands

- `cd` Changes the working directory.
format flash

Erase all existing files and reformat the filesystem in the internal flash memory. After the filesystem is formatted, files cannot be restored.

Syntax
format {flash: | usbflash:}

Default
flash memory

Command Modes
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
You must include the colon (:) when entering this command.

Caution: This command deletes all files, including the startup configuration file. So, after executing this command, consider saving the running config as the startup config (use the write memory command or the copy run start command).

Related Commands
- copy
- show file
- show file-systems

logging coredump

Enable coredump.

Syntax
logging coredump stack-unit all

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
The Kernel core dump can be large and may take up to five to 30 minutes to upload. FTOS does not overwrite application core dumps so delete them as necessary to conserve space on the flash; if the flash is out of memory, the coredump is aborted. FTOS completes the coredump process and waits until the upload is complete before rebooting the system.

Related Commands
- logging coredump server
- Designates a sever to upload kernel core-dumps.
logging coredump server

Designate a server to upload core dumps.

**Syntax**

```
logging coredump server \{ipv4-address\} username name password [type] password
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ipv4-address}</td>
<td>Enter the server IPv4 address (A.B.C.D)</td>
</tr>
<tr>
<td>name</td>
<td>Enter a username to access the target server.</td>
</tr>
<tr>
<td>type</td>
<td>Enter the password type:</td>
</tr>
<tr>
<td></td>
<td>• Enter 0 to enter an unencrypted password.</td>
</tr>
<tr>
<td></td>
<td>• Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.</td>
</tr>
<tr>
<td>password</td>
<td>Enter a password to access the target server.</td>
</tr>
</tbody>
</table>

**Defaults**

- Crash kernel files are uploaded to flash by default.

**Command Modes**

- CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Because flash space may be limited, using this command ensures your entire crash kernel files are uploaded successfully and completely. Only a single coredump server can be configured. Configuration of a new coredump server over-writes any previously configured server.

**Note:** You must disable `logging coredump` before you designate a new server destination for your core dumps.

**Related Commands**

- `logging coredump` Disables the kernel coredump

**pwd**

Display the current working directory.

**Syntax**

```
pwd
```

**Command Modes**

- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
Figure 3-4. pwd Command Example

FTOS#pwd
flash:
FTOS#
```

**Related Commands**

- `cd` Changes the directory.
rename

Rename a file in the local file system.

Syntax

rename url url

Parameters

url Enter the following keywords and a filename:
- For a file on the internal Flash, enter flash:// followed by the filename.
- For a file on the external Flash, enter usbflash:// followed by the filename.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

show boot system

Displays information about boot images currently configured on the system.

Syntax

show boot system stack-unit {0-5 | all}

Parameters

0-5 Enter this information to display the boot image information of only the entered stack-unit
all Enter this keyword to display the boot image information of all the stack-units in the stack

Defaults

none

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 3-5. show boot system Command Example

FTOS#show boot system stack-unit all
Current system image information in the system:
---------------------------------------------------------------
Type Boot Type A B
Stack-unit 0 is not present.
Stack-unit 1 is not present.
Stack-unit 2 is not present.
Stack-unit 3 is not present.
Stack-unit 4 is not present.
Stack-unit 5 DOWNLOAD BOOT 9-1-0-675 9-1-0-684
show file

Display contents of a text file in the local filesystem.

**Syntax**

show file *url*

**Parameters**

*url* Enter one of the following:
- For a file on the internal Flash, enter flash:// followed by the filename.
- For a file on the external Flash, enter usbflash:// followed by the filename.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

*Figure 3-6. show file Command Example (Partial)*

```
FTOS#show file flash://startup-config
! Version E8-3-16-29
! Last configuration change at Thu Apr 26 19:19:02 2012 by default
! Startup-config last updated at Thu Apr 26 19:19:04 2012 by default
!
boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.11.200.241/dt-m1000e-5-c2
boot system gateway 10.11.209.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 3
redundancy disable-auto-reboot stack-unit 4
redundancy disable-auto-reboot stack-unit 5
!
service timestamps log datetime
logging coredump stack-unit all
!
hostname FTOS
--More--
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>format flash</td>
<td>Erases all existing files and reformats the filesystem in the internal flash memory.</td>
</tr>
<tr>
<td>show file-systems</td>
<td>Displays information about the file systems on the system.</td>
</tr>
</tbody>
</table>

show file-systems

Display information about the file systems on the system.

**Syntax**

show file-systems

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example Figure 3-7. show file-system Command Example

Related Commands

Table 3-1. show file-systems Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size(b)</td>
<td>Lists the size in bytes of the storage location. If the location is remote, no size is listed.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Lists the available size in bytes of the storage location. If the location is remote, no size is listed.</td>
</tr>
<tr>
<td>Feature</td>
<td>Displays the formatted DOS version of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of storage. If the location is remote, the word network is listed.</td>
</tr>
<tr>
<td>Flags</td>
<td>Displays the access available to the storage location. The following letters indicate the level of access:</td>
</tr>
<tr>
<td></td>
<td>• r = read access</td>
</tr>
<tr>
<td></td>
<td>• w = write access</td>
</tr>
<tr>
<td>Prefixes</td>
<td>Displays the name of the storage location.</td>
</tr>
</tbody>
</table>

show os-version

Display the release and software image version information of the image file specified.

Syntax

```
show os-version [file-url]
```

Parameters

<table>
<thead>
<tr>
<th>file-url</th>
<th>(OPTIONAL) Enter the following location keywords and information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For a file on the internal Flash, enter flash:// followed by the filename.</td>
</tr>
<tr>
<td></td>
<td>• For a file on an FTP server, enter ftp://user:password@hostip/filepath</td>
</tr>
<tr>
<td></td>
<td>• For a file on a TFTP server, enter tftp://hostip/filepath</td>
</tr>
<tr>
<td></td>
<td>• For a file on the external Flash, enter usbflash:// followed by the filename.</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

EXEC Privilege
Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Note: A filepath that contains a dot (.) is not supported.

Example

Figure 3-8. show os-version Command Example

```plaintext
FTOS#show os-version
RELEASE IMAGE INFORMATION :
 Platform          Version        Size           ReleaseTime
IOM-Series:  XL        9-1-0-848    31962011    Mar 20 2012 09:26:46
TARGET IMAGE INFORMATION :
 Type          Version                   Target    checksum
runtime        9-1-0-848        Control Processor      passed
BOOT IMAGE INFORMATION :
 Type          Version                   Target    checksum
boot flash        4.0.1.0bt        Control Processor      passed
BOOTSEL IMAGE INFORMATION :
 Type          Version                   Target    checksum
boot selector        4.0.0.0bt        Control Processor      passed
CPLD IMAGE INFORMATION :
 Card          CPLD Name    Version
Stack-unit 5                IOM SYSTEM CPLD          5
FTOS#
```
show running-config
Display the current configuration and display changes from the default values.

Syntax
show running-config [entity] [configured] [status]

Parameters

entity
(Optional) Enter one of the keywords listed below to display that entity's current (non-default) configuration. Note that, if nothing is configured for that entity, nothing is displayed and the prompt returns:

- aaa for the current AAA configuration
- acl for the current ACL configuration
- arp for the current static ARP configuration
- as-path for the current AS-path configuration
- bfd for the current BFD configuration
- bgp for the current BGP configuration
- boot for the current boot configuration
- cam-profile for the current CAM profile in the configuration
- class-map for the current class-map configuration
- community-list or the current community-list configuration
- ecmp-group for the current ECMP group configuration
- fefd for the current FEFD configuration
- ftp for the current ftp configuration
- fvrp for the current FVRP configuration
- gvrp for the current GVRP configuration
- host for the current host configuration
- hardware-monitor for hardware-monitor action-on-error settings
- hypervisor for hypervisor settings
- igmp for the current IGMP configuration
- interface for the current interface configuration
- interface tunnel for all configured tunnels. For a specific tunnel, enter the tunnel ID. The range is from 1 to 16383.
- ip for the current IP configuration
- isis for the current IS-IS configuration
- line for the current line configuration
- lldp for the current LLDP configuration
- load-balance for the current port-channel load-balance configuration
- logging for the current logging configuration
- mac for the current MAC ACL configuration
- mac-address-table for the current MAC configuration
- management-eis for the current management EIS configuration
- management-route for the current Management port forwarding configuration
- mld for the current MLD configuration
- monitor for the current Monitor configuration
- mroute for the current Mroutes configuration
- msdp for the current MSDP configuration
- ntp for the current NTP configuration
- ospf for the current OSPF configuration
- pim for the current PIM configuration
• policy-map-input for the current input policy map configuration
• policy-map-output for the current output policy map configuration
• po-failover-group for the current port-channel failover-group configuration
• prefix-list for the current prefix-list configuration
• privilege for the current privilege configuration
• qos-policy-input for the current input QoS policy configuration
• qos-policy-output for the current output QoS policy configuration
• radius for the current RADIUS configuration
• redirect-list for the current redirect-list configuration
• redundancy for the current RPM redundancy configuration
• resolve for the current DNS configuration
• rip for the current RIP configuration
• rmon for the current RMON configuration
• route-map for the current route map configuration
• sflow for the current sFlow configuration
• snmp for the current SNMP configuration
• spanning-tree for the current spanning tree configuration
• static for the current static route configuration
• status for the current file status configuration
• tacacs+ for the current TACACS+ configuration
• tftp for the current TFTP configuration
• trace-group for the current trace-group configuration
• trace-list for the current trace-list configuration
• uplink-state-group for the current uplink state group configuration
• users for the current users configuration
• vlt for the current VLT configuration
• wred-profile for the current wred-profile configuration

configured (OPTIONAL) Enter the keyword configuration to display line card interfaces with non-default configurations only.

status (OPTIONAL) Enter the keyword status to display the checksum for the running configuration and the start-up configuration.

EXEC Privilege

Command Modes

Command History

Version 9.2(0.0) Added support for as-path, bfd, bgp, cam-profile, community-list, ecmp-group, gvrp, hypervisor, interface-tunnel, ip, isis, lldp, management-eis, mld, monitor, msdp, po-failover-group, qos-policy-input, qos-policy-output, redirect-list, redundancy, rmon, sflow, status, trace-group, trace-list, uplink-state-group, and vlt entities.

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example Figure 3-9.  show running-config Command Example (Partial)

FTOS#show running-config
Current Configuration ... 
! Version E8-3-16-29 
! Last configuration change at Thu Apr 26 19:19:21 2012 by admin 
! Startup-config last updated at Thu Apr 26 19:19:04 2012 by default 
! boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.11.200.241/dt-m1000e-5-c2
boot system gateway 10.11.209.254 
! redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit 
! redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 5 
!--More--
service timestamps log datetime
logging coredump stack-unit all
!
hostname FTOS
!
... 

Example Figure 3-10.  show running-config Command Example

FTOS#show running-config status
running-config bytes 4306, checksum 0x4D55EE70
startup-config bytes 4344, checksum 0x6472C5E
FTOS#

Usage Information

The status option allows you to display the size and checksum of the running configuration and the startup configuration.

show startup-config

Display the startup configuration.

Syntax

show startup-config

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
show version

Display the current FTOS version information on the system.

Syntax

show version

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

FTOS#show version

Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 1.0
Dell Force10 Application Software Version: E8-3-16-29
Copyright (c) 1999-2012 by Dell Inc. All Rights Reserved.
Build Time: Thu Apr 26 05:41:48 PDT 2012
Build Path: /sites/sjc/work/build/buildSpaces/build03/E8-3-16/SW/SRC/Cp_src/
Tacacs
FTOS uptime is 13 hour(s), 29 minute(s)

System image file is "system://A"

System Type: MXL-10/40GbE
Control Processor: MIPS RMI XLP with 2147483648 bytes of memory.
256M bytes of boot flash memory.

1 34-port GE/TE/FG (XL)
48 Ten GigabitEthernet/IEEE 802.3 interface(s)
2 Forty GigabitEthernet/IEEE 802.3 interface(s)

Table 3-2. show version Command Fields

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell Force10 Network...</td>
<td>Name of the operating system</td>
</tr>
<tr>
<td>Dell Force10 Operating...</td>
<td>OS version number</td>
</tr>
</tbody>
</table>

Figure 3-12. show version Command Example

Figure 3-11. show startup-config Command Example (Partial)

FTOS#show startup-config
!
! Last configuration change at Thu Apr 26 19:19:02 2012 by default
! Startup-config last updated at Thu Apr 26 19:19:04 2012 by default
!
boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.11.200.241/dt-m1000e-5-c2
boot system gateway 10.11.209.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 3
--More--
upgrade boot

Upgrade the bootflash image or bootselector image.

Syntax

upgrade boot {all | bootflash-image | bootselector-image} stack-unit {0-5 | all} {booted | flash: |ftp: | tftp: | usbflash:} {A: | B:}

Parameters

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enter this keyword to change both the bootflash and bootselector images.</td>
</tr>
<tr>
<td>bootflash-image</td>
<td>Enter this keyword to change the bootflash image.</td>
</tr>
<tr>
<td>bootselector-image</td>
<td>Enter this keyword to change the bootselector image.</td>
</tr>
<tr>
<td>0-5</td>
<td>Enter this keyword to upgrade only the mentioned stack-unit.</td>
</tr>
<tr>
<td>all</td>
<td>Enter this keyword to upgrade all the member stack-units.</td>
</tr>
<tr>
<td>booted</td>
<td>Enter this keyword to upgrade from the current image in the MXL 10/40GbE Switch.</td>
</tr>
<tr>
<td>ftp</td>
<td>After entering this keyword you can either follow it with the location of the source file in this form: //userid:password@hostip/filepath, or press Enter to launch a prompt sequence.</td>
</tr>
<tr>
<td>tftp</td>
<td>After entering this keyword you can either follow it with the location of the source file in this form: //hostlocation/filepath, or press Enter to launch a prompt sequence.</td>
</tr>
<tr>
<td>flash</td>
<td>After entering this keyword you can either follow it with the location of the source file in this form: //filepath, or press Enter to launch a prompt sequence.</td>
</tr>
<tr>
<td>usbflash</td>
<td>After entering this keyword you can either follow it with the location of the source file in this form: //filepath, or press Enter to launch a prompt sequence.</td>
</tr>
<tr>
<td>A</td>
<td>Enter this keyword to upgrade the bootflash partition A.</td>
</tr>
<tr>
<td>B</td>
<td>Enter this keyword to upgrade the bootflash partition B.</td>
</tr>
</tbody>
</table>
upgrade system

Upgrade the bootflash image or system image.

Syntax

upgrade system {flash: | ftp: | scp: | tftp: | usbflash: | stack-unit {0-5 | all} {A: | B:}

Parameters

- **0-5** Enter this keyword to upgrade only the mentioned stack-unit
- **all** Enter this keyword to upgrade all the member units of the stack
- **ftp** After entering this keyword you can either follow it with the location of the source file in this form: `//userid:password@hostip/filepath`, or press Enter to launch a prompt sequence.
- **scp** After entering this keyword you can either follow it with the location of the source file in this form: `//userid:password@hostip/filepath`, or press Enter to launch a prompt sequence.
- **tftp** After entering this keyword you can either follow it with the location of the source file in this form: `//hostlocation/filepath`, or press Enter to launch a prompt sequence.
- **flash** After entering this keyword you can either follow it with the location of the source file in this form: `//filepath`, or press Enter to launch a prompt sequence.
- **usbflash** After entering this keyword you can either follow it with the location of the source file in this form: `//filepath`, or press Enter to launch a prompt sequence.
- **A** Enter this keyword to upgrade the bootflash partition A
- **B** Enter this keyword to upgrade the bootflash partition B

Defaults

one

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
You must reload FTOS after executing this command. Use the command `upgrade system stack-unit` to copy FTOS from the management unit to one or more stack members.

**Example**

Figure 3-14. upgrade system Command Example

```
FTOS#upgrade system ?
flash: Copy from flash file system (flash://filepath)
ftp: Copy from remote file system, IPv4 or IPv6, (ftp://
    /userid:password@hostip/filepath)
scp: Copy from remote file system, IPv4 or IPv6, (scp://
    /userid:password@hostip/filepath)
stack-unit Sync image to the stack-unit
/tftp: Copy from remote file system, IPv4 or IPv6, (tftp://
    /hostip/filepath)
usbflash: Copy from usbflash file system (usbflash://
Forty
```
Control and Monitoring

This chapter describes control and monitoring for the MXL 10/40GbE Switch IO Module.

Commands

This chapter includes the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset-tag</td>
<td>ip tftp source-interface</td>
</tr>
<tr>
<td>asf-mode</td>
<td>line</td>
</tr>
<tr>
<td>banner exec</td>
<td>motd-banner</td>
</tr>
<tr>
<td>banner login</td>
<td>ping</td>
</tr>
<tr>
<td>banner motd</td>
<td>reload</td>
</tr>
<tr>
<td>clear alarms</td>
<td>send</td>
</tr>
<tr>
<td>clear command history</td>
<td>service timestamps</td>
</tr>
<tr>
<td>clear line</td>
<td>show alarms</td>
</tr>
<tr>
<td>configure</td>
<td>show command-history</td>
</tr>
<tr>
<td>debug cpu-traffic-stats</td>
<td>show command-tree</td>
</tr>
<tr>
<td>debug ftpserver</td>
<td>show cpu-traffic-stats</td>
</tr>
<tr>
<td>disable</td>
<td>show debugging</td>
</tr>
<tr>
<td>do</td>
<td>show environment</td>
</tr>
<tr>
<td>enable</td>
<td>show inventory</td>
</tr>
<tr>
<td>enable optic-info-update interval</td>
<td>show memory</td>
</tr>
<tr>
<td>end</td>
<td>show processes cpu</td>
</tr>
<tr>
<td>exec-banner</td>
<td>show processes ipc flow-control</td>
</tr>
<tr>
<td>exec-timeout</td>
<td>show processes memory</td>
</tr>
<tr>
<td>exit</td>
<td>show software ifm</td>
</tr>
<tr>
<td>ftp-server enable</td>
<td>show system</td>
</tr>
<tr>
<td>ftp-server topdir</td>
<td>telnet</td>
</tr>
<tr>
<td>ftp-server username</td>
<td>terminal length</td>
</tr>
<tr>
<td>hostname</td>
<td>traceroute</td>
</tr>
<tr>
<td>ip ftp password</td>
<td>undebug all</td>
</tr>
<tr>
<td>ip ftp source-interface</td>
<td>virtual-ip</td>
</tr>
<tr>
<td>ip ftp username</td>
<td>write</td>
</tr>
<tr>
<td>ip telnet server enable</td>
<td></td>
</tr>
<tr>
<td>ip telnet source-interface</td>
<td></td>
</tr>
</tbody>
</table>
asset-tag

Assign and store a unique asset-tag to the stack member.

Syntax

asset-tag stack-unit unit id Asset-tag ID

To remove the asset tag, use no stack-unit unit-id Asset-tag ID command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit</td>
<td>Enter the keyword stack-unit followed by the unit-id to assign a tag to the specific member. The range is from 0 to 5.</td>
</tr>
<tr>
<td>unit-id</td>
<td>Enter a unique asset-tag ID to assign to the stack member. This option accepts a maximum of 10 characters, including all special characters except double quotes. To include a space in the asset-tag, enter a space within double quotes.</td>
</tr>
</tbody>
</table>

Defaults

No asset-tag is assigned.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show system Displays the current status of all stack members or a specific member.

asf-mode

Enable alternate store and forward (ASF) mode and forward packets as soon as a threshold is reached.

Syntax

asf-mode stack-unit {unit-id | all} queue size

To return to standard store and forward mode, use the no asf-mode stack-unit command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit-id</td>
<td>Enter the stack member unit identifier of the stack member to reset. Range: 0 - 5 all</td>
</tr>
<tr>
<td>queue size</td>
<td>Enter the queue size of the stack member. Range: 1 - 15</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You must save the configuration and reload the system to implement ASF. When you enter the command, the system sends a message stating that the new mode is enabled when the system reloads.
**banner exec**

Configure a message that is displayed when a user enters EXEC mode.

**Syntax**

`banner exec c line c`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>c</code></td>
<td>Enter the keywords <code>banner exec</code>, and then enter a character delineator, represented here by the letter <code>c</code>, and press ENTER.</td>
</tr>
<tr>
<td><code>line</code></td>
<td>Enter a text string for your banner message ending the message with your delineator. In the example below, the delineator is a percent character (%); the banner message is “testing, testing”.</td>
</tr>
</tbody>
</table>

**Defaults**

No banner is displayed.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

**Figure 4-1. banner exec Command Example**

```
FTOS(conf)#banner exec ?
LINE c banner-text(max length 255) c, where 'c' is a delimiting character
FTOS(conf)#banner exec %
Enter TEXT message. End with the character '%'.
This is the banner
FTOS(conf)#end
FTOS#exit
4d21h5m: %STKUNIT0-M P:CP %SEC-5-LOGOUT: Exec session is terminated for user on line console
This is the banner
Dell Force10 con0 now available
Press RETURN to get started.
This is the banner
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>banner login</code></td>
<td>Sets a banner for login connections to the system.</td>
</tr>
<tr>
<td><code>banner motd</code></td>
<td>Sets a Message of the Day banner.</td>
</tr>
<tr>
<td><code>exec-banner</code></td>
<td>Enables the display of a text string when the user enters EXEC mode.</td>
</tr>
<tr>
<td><code>line</code></td>
<td>Enables and configures the console and virtual terminal lines to the system.</td>
</tr>
</tbody>
</table>

**banner login**

Set a banner to be displayed when logging on to the system.
### Syntax

```
banner login {keyboard-interactive | no keyboard-interactive} [c line c]
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyboard-interactive</td>
<td>Enter this keyword to require a carriage return (CR) to get the message banner prompt.</td>
</tr>
<tr>
<td>c</td>
<td>Enter a delineator character to specify the limits of the text banner. In Figure 4-2, the % character is the delineator character.</td>
</tr>
<tr>
<td>line</td>
<td>Enter a text string for your text banner message ending the message with your delineator. In the example in Figure 4-2, the delineator is a percent character (%). Ranges:</td>
</tr>
<tr>
<td></td>
<td>* maximum of 50 lines</td>
</tr>
<tr>
<td></td>
<td>* up to 255 characters per line</td>
</tr>
</tbody>
</table>

### Defaults

No banner is configured and the CR is required when creating a banner.

### Command Modes

CONFIGURATION

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td></td>
<td>on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

### Usage Information

A login banner message is displayed only in EXEC Privilege mode after entering the `enable` command followed by the password. These banners are not displayed to users in EXEC mode.

### Example

**Figure 4-2. banner login Command Example**

```
FTOS(conf)#banner login ?
keyboard-interactive Press enter key to get prompt
LINE c banner-text(max length 255) c, where 'c' is a delimiting character
FTOS(conf)#no banner login ?
keyboard-interactive Prompt will be displayed by default
<cr>
FTOS(conf)#banner login keyboard-interactive

Enter TEXT message. End with the character '%'.
This is the banner%
FTOS(conf)#end
FTOS#exit

13d21h9m: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec session is terminated for user on line console
This is the banner
Dell Force10 con0 now available
Press RETURN to get started.
13d21h10m: STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user on line console
This is the banner
```

### Related Commands

- `banner exec` Sets a banner to be displayed when you enter EXEC Privilege mode.
- `banner motd` Sets a Message of the Day banner.

---

**banner motd**

Set a Message of the Day (MOTD) banner.

### Syntax

```
banner motd c line c
```


Parameters

- **c**: Enter a delineator character to specify the limits of the text banner. In the above figures, the % character is the delineator character.
- **line**: Enter a text string for your message of the day banner message ending the message with your delineator. In the example figures above, the delineator is a percent character (%).

Defaults
No banner is configured.

Command Modes
CONFIGURATION

Command History

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
A MOTD banner message is displayed only in EXEC Privilege mode after entering the `enable` command followed by the password. These banners are not displayed to users in EXEC (non-privilege) mode.

Related Commands
- **banner exec**: Sets a banner to be displayed when you enter the EXEC Privilege mode.
- **banner login**: Sets a banner to be displayed after successful login to the system.

---

**clear alarms**
Clear alarms on the system.

**Syntax**
clear alarms

**Command Modes**
EXEC Privilege

**Command History**

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**
This command clears alarms that are no longer active. If an alarm situation is still active, it is seen in the system output.

---

**clear command history**
Clear the command history log.

**Syntax**
clear command history

**Command Modes**
EXEC Privilege

**Command History**

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**
- **show command-history**: Displays a buffered log of all commands entered by all users along with a time stamp.
### clear line

Reset a terminal line.

**Syntax**

```
clear line \{line-number | console 0 | vty number\}
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line-number</td>
<td>Enter a number for one of the 12 terminal lines on the system. Range: 0 to 11.</td>
</tr>
<tr>
<td>console 0</td>
<td>Enter the keyword console 0 to reset the Console port.</td>
</tr>
<tr>
<td>vty number</td>
<td>Enter the keyword vty followed by a number to clear a Terminal line. Range: 0 to 9</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

| Version  | Introduced on the MXL 10/40GbE Switch IO Module. |

### configure

Enter CONFIGURATION mode from EXEC Privilege mode.

**Syntax**

```
command  [terminal]
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminal</td>
<td>(OPTIONAL) Enter the keyword terminal to specify that you are configuring from the terminal.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

| Version  | Introduced on the MXL 10/40GbE Switch IO Module. |

**Example**

Figure 4-3. configure Command Example

```
FTOS#configure
FTOS(conf)#
```

### debug cpu-traffic-stats

Enable the collection of CPU traffic statistics.

**Syntax**

```
drop cpu-traffic-stats
```

**Defaults**

Disabled

**Command Modes**

EXEC Privilege

**Command History**

| Version  | Introduced on the MXL 10/40GbE Switch IO Module. |
This command enables (and disables) the collection of CPU traffic statistics from the time this command is executed (not from system boot). However, excessive traffic received by a CPU automatically triggers (turns on) the collection of CPU traffic statistics. Use the `show cpu-traffic-stats` to view the traffic statistics.

If excessive traffic is received by CPU, traffic is rate controlled

**Note:** This command must be enabled before the `show cpu-traffic-stats` command displays traffic statistics. Dell Networking recommends disabling debugging (`no debug cpu-traffic-stats`) after troubleshooting is complete.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cpu-traffic-stats</code></td>
<td>Displays the cpu traffic statistics</td>
</tr>
</tbody>
</table>

### debug ftpserver

View transactions during an FTP session when a user is logged into the FTP server.

**Syntax**

ddebug ftpserver

**Command Modes**

EXEC Privilege

**Command History**

- Introduced on the MXL 10/40GbE Switch IO Module.

### disable

Return to EXEC mode.

**Syntax**

disable [level]

**Parameters**

- `level` (OPTIONAL) Enter a number for a privilege level of the FTOS.
  - Range: 0 to 15.
  - Default: 1

**Defaults**

1

**Command Modes**

EXEC Privilege

**Command History**

- Introduced on the MXL 10/40GbE Switch IO Module.

### do

Allows the execution of most EXEC-level commands from all CONFIGURATION levels without returning to the EXEC level.

**Syntax**

ddo command

**Parameters**

- `command` Enter an EXEC-level command.
Defaults: none

Command Modes:
- CONFIGURATION
- INTERFACE

Command History:
- Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information:
The following commands are not supported by the do command:
- enable
- disable
- exit
- config

Example:
**Figure 4-4. do Command Example**

```
FTOS(conf-if-te-5/0)#do clear counters
Clear counters on all interfaces [confirm]
FTOS(conf-if-te-5/0)#
FTOS(conf-if-te-5/0)#do clear logging
Clear logging buffer [confirm]
FTOS(conf-if-te-5/0)#
FTOS(conf-if-te-5/0)#do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
FTOS(conf-if-te-5/0)#
```

### enable

Enter EXEC Privilege mode or any other privilege level configured. After entering this command, you may need to enter a password.

**Syntax**
```
enable [level]
```

**Parameters**
- `level` (OPTIONAL) Enter a number for a privilege level of FTOS.
  - Range: 0 to 15.
  - Default: 15

**Defaults**
- 15

**Command Modes**
- EXEC

**Command History**
- Version 8.3.16.1: Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**
Users entering EXEC Privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the `enable password` command to configure a password for the `enable` command at a specific privilege level. If no privilege level is specified, the default is privilege level 15.

**Related Commands**
- `enable password`: Configures a password for the `enable` command and to access a privilege level.
enable optic-info-update interval

Enable polling intervals of optical information updates for SNMP.

Syntax

```bash
enable optical-info-update interval seconds
```

To disable optical power information updates, use the no enable optical-info-update interval command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval seconds</td>
<td>Enter the keyword <code>interval</code> followed by the polling interval in seconds. Range: 120 to 6000 seconds. Default: 300 seconds (5 minutes)</td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

- CONFIGURATION

Command History

- **Version 8.3.16.1** Replaces the `enable xfp-power-updates` command.

Usage Information

- The default interval for the polling is 300 seconds (5 minutes). Use this command to enable the polling and to configure the polling frequency.

end

Return to EXEC Privilege mode from other command modes (for example, CONFIGURATION or ROUTER OSPF modes).

Syntax

```bash
end
```

Command Modes

- CONFIGURATION
- SPANNING TREE
- MULTIPLE SPANNING TREE
- LINE
- INTERFACE
- VRRP
- ACCESS-LIST
- PREFIX-LIST
- ROUTER OSPF
- ROUTER RIP

Command History

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- exit Returns to the lower command mode.
exec-banner

Enable the display of a text string when the user enters EXEC mode.

**Syntax**

`exec-banner`

**Defaults**

Enabled on all lines (if configured, the banner appears).

**Command Modes**

LINE

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage**

Optionally, use the `banner exec` command to create a text string that is displayed when the user accesses EXEC mode. This command toggles that display.

**Related Commands**

- `banner exec` — Configures a banner to display when entering EXEC mode.
- `line` — Enables and configures console and virtual terminal lines to the system.

exec-timeout

Set a time interval for the system to wait for input on a line before disconnecting the session.

**Syntax**

`exec-timeout minutes [seconds]`

To return to default settings, enter `no exec-timeout`.

**Parameters**

- `minutes` — Enter the number of minutes of inactivity on the system before disconnecting the current session.
  - Range: 0 to 35791
  - Default: 10 minutes for console line; 30 minutes for VTY line.

- `seconds` — (OPTIONAL) Enter the number of seconds
  - Range: 0 to 2147483
  - Default: 0 seconds

**Defaults**

10 minutes for console line; 30 minutes for VTY lines; 0 seconds

**Command Modes**

LINE

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage**

To remove the time interval, use the `exec-timeout 0 0` command.

**Example**

**Figure 4-5. FTOS time-out display**

```
FTOS con0 is now available
Press RETURN to get started.
FTOS>
```
exit

Return to the lower command mode.

Syntax

exit

Command Modes

• EXEC Privilege
• CONFIGURATION
• LINE
• INTERFACE
• PROTOCOL GVRP
• SPANNING TREE
• MULTIPLE SPANNING TREE
• MAC ACCESS LIST
• ACCESS-LIST
• PREFIX-LIST
• ROUTER OSPF
• ROUTER RIP

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

end Returns to EXEC Privilege command mode.

ftp-server enable

Enable FTP server functions on the system.

Syntax

ftp-server enable

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
ftp-server topdir

Set the directory to be used for incoming FTP connections.

**Syntax**

```
ftp-server topdir directory
```

**Parameters**

- `directory` Enter the directory path.

**Defaults**

The internal flash is the default directory.

**Command Modes**

CONFIGURATION

**Command History**

- Introduced in version 8.3.16.1 on the MXL 10/40GbE Switch IO Module.

**Usage Information**

After you enable FTP server functions with the `ftp-server enable` command, Dell Networking recommends specifying a top-level directory path. Without a top-level directory path specified, the FTOS directs users to the flash directory when they log in to the FTP server.

**Related Commands**

- `ftp-server enable` — Enables FTP server functions on the MXL 10/40GbE Switch IO Module.
- `ftp-server username` — Sets a username and password for incoming FTP connections to the MXL 10/40GbE Switch IO Module.
**ftp-server username**

Create a user name and associated password for incoming FTP server sessions.

**Syntax**

```
ftp-server username username password [encryption-type] password
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Enter a text string up to 40 characters long as the user name.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Enter the keyword <code>password</code> followed by a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.</td>
</tr>
<tr>
<td><code>encryption-type</code></td>
<td>(OPTIONAL) After the keyword <code>password</code> enter one of the following numbers:</td>
</tr>
<tr>
<td></td>
<td>• 0 (zero) for an unencrypted (clear text) password</td>
</tr>
<tr>
<td></td>
<td>• 7 (seven) for hidden text password.</td>
</tr>
</tbody>
</table>

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**hostname**

Set the host name of the system.

**Syntax**

```
hostname name
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Enter a text string, up to 32 characters long.</td>
</tr>
</tbody>
</table>

**Defaults**

FTOS

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The hostname is used in the prompt.
ip ftp password

Specify a password for outgoing FTP connections.

**Syntax**

```
ip ftp password [encryption-type] password
```

**Parameters**

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption-type</td>
<td>(OPTIONAL) Enter one of the following numbers:</td>
</tr>
<tr>
<td>password</td>
<td>Enter a string up to 40 characters as the password.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The password is listed in the configuration file; you can view the password using the `show running-config ftp` command in EXEC mode.

Use the password configured by the `ip ftp password` command when you use the `ftp:` parameter in the `copy` command.

**Related Commands**

- `copy` Copies the files.
- `ip ftp username` Sets the user name for the FTP sessions.

ip ftp source-interface

Specify an interface’s IP address as the source IP address for FTP connections.

**Syntax**

```
ip ftp source-interface interface
```

**Parameters**

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For Loopback interfaces, enter the keyword <code>loopback</code> followed by a number from zero (0) to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code> TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <code> fortyGigE</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN interface, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Defaults**

The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
ip ftp username

Assign a user name for outgoing FTP connection requests.

**Syntax**

```
ip ftp username username
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Enter a text string as the user name up to 40 characters long.</td>
</tr>
</tbody>
</table>

**Defaults**

No user name is configured.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

You must also configure a password with the `ip ftp password` command.

**Related Commands**

- `ip ftp password` Sets the password for the FTP connections.

ip telnet server enable

Enable the Telnet server on the switch.

**Syntax**

```
ip telnet server enable
```

To disable the Telnet server, use the `no ip telnet server enable` command.

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `ip ssh server` Enables the SSH server on the system.
ip telnet source-interface

Set an interface’s IP address as the source address in outgoing packets for Telnet sessions.

**Syntax**

```
ip telnet source-interface interface
```

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  - For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16383.
  - For a Port Channel, enter the keyword `port-channel` followed by a number:
    - **Range:** 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

**Command Modes**

- `CONFIGURATION`

**Command History**

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `telnet` Telnets to another device.

ip tftp source-interface

Assign an interface’s IP address in outgoing packets for TFTP traffic.

**Syntax**

```
ip tftp source-interface interface
```

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  - For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16383.
  - For a Port Channel, enter the keyword `port-channel` followed by a number:
    - **Range:** 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

**Command Modes**

- `CONFIGURATION`

**Command History**

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
line

Enable and configure console and virtual terminal lines to the system. This command accesses LINE mode, where you can set the access conditions for the designated line.

**Syntax**

```
line {console 0 | vty number [end-number]}
```

**Parameters**

- **console 0**
  - Enter the keyword console 0 to configure the console port.
  - The console option is <0-0>.

- **vty number**
  - Enter the keyword vty followed by a number from 0 to 9 to configure a virtual terminal line for Telnet sessions.
  - The system supports 10 Telnet sessions.

- **end-number**
  - (OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure.
  - You can configure multiple lines at one time.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION

**Command History**

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

You cannot delete a terminal connection.

**Related Commands**

- **access-class**
  - Restricts incoming connections to a particular IP address in an IP access control list (ACL).
- **password**
  - Specifies a password for users on terminal lines.
- **show memory**
  - View current memory usage on the MXL switch.

motd-banner

Enable a Message of the Day (MOTD) banner to appear when you log in to the system.

**Syntax**

```
motd-banner
```

**Defaults**

Enabled on all lines.

**Command Modes**

LINE

**Command History**

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

ping

Test connectivity between the system and another device by sending echo requests and waiting for replies.

**Syntax**

```
ping [host | ip-address] [count {number | continuous}] [datagram-size] [timeout] [source (ip src-ipv4-address) | interface] [tos] [df-bit (y|n)] [validate-reply(y|n)] [pattern pattern] [sweep-min-size] [sweep-max-size] [sweep-interval] [ointerface (ip src-ipv4-address) | interface]
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>host</strong></td>
<td>Enter the host name of the devices to which you are testing connectivity. (OPTIONAL)</td>
</tr>
<tr>
<td><strong>ip-address</strong></td>
<td>Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format. (OPTIONAL)</td>
</tr>
<tr>
<td><strong>count</strong></td>
<td>Enter the number of echo packets to be sent. <strong>number:</strong> 1-2147483647 <strong>Continuous:</strong> transmit echo request continuously</td>
</tr>
<tr>
<td><strong>datagram size</strong></td>
<td>Enter the ICMP datagram size.</td>
</tr>
<tr>
<td><strong>timeout</strong></td>
<td>Enter the interval to wait for an echo reply before timing out. <strong>Range:</strong> 0-3600 seconds <strong>Default:</strong> 2 seconds</td>
</tr>
<tr>
<td><strong>source</strong></td>
<td>Enter the IPv4 source ip address or the source interface.</td>
</tr>
<tr>
<td><strong>tos</strong></td>
<td>Enter the type of service required. <strong>Range:</strong> 0-255 <strong>Default:</strong> 0</td>
</tr>
<tr>
<td><strong>df-bit</strong></td>
<td>Enter Y or N for the <strong>don't fragment</strong> bit in IPv4 header. <strong>Range:</strong> 0-255 <strong>Default:</strong> No</td>
</tr>
<tr>
<td><strong>validate-reply</strong></td>
<td>Enter Y or N for reply validation. <strong>Range:</strong> 0-255 <strong>Default:</strong> No</td>
</tr>
<tr>
<td><strong>pattern</strong></td>
<td>Enter the IPv4 data pattern. <strong>Range:</strong> 0-FFFF <strong>Default:</strong> 0xABCD</td>
</tr>
<tr>
<td><strong>sweep-min-size</strong></td>
<td>Enter the minimum size of datagram in sweep range. <strong>Range:</strong> 52-15359 bytes</td>
</tr>
<tr>
<td><strong>sweep-max-size</strong></td>
<td>Enter the maximum size of datagram in sweep range. <strong>Range:</strong> 53-15359 bytes</td>
</tr>
</tbody>
</table>
### sweep-interval

Enter the incremental value for sweep size.

1-15308 seconds

### ointerface

Enter the outgoing interface for multicast packets.
- Enter the IP address in A.B.C.D format
- For a Port Channel, enter the keyword `port-channel` followed by a number: 1-128
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
- For a VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

---

**Defaults**

See parameters above.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When you enter the ping command without specifying an IP address (Extended Ping), you are prompted for a target IP address, a repeat count, a datagram size (up to 1500 bytes), a timeout in seconds, and for Extended Commands. For information on the ICMP message codes that return from a ping command, refer to Appendix 57, Internet Control Message Protocol (ICMP) Message Types.

**Figure 4-7. ping (IPv4) Command Example**

```
FTOS#ping 172.31.1.255
    Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2 seconds:
Reply to request 1 from 172.31.1.208     0 ms
Reply to request 1 from 172.31.1.216     0 ms
Reply to request 1 from 172.31.1.205     16 ms
: :
Reply to request 5 from 172.31.1.209     0 ms
Reply to request 5 from 172.31.1.66      0 ms
Reply to request 5 from 172.31.1.87      0 ms

FTOS#
```

### reload

Reboot FTOS.

**Syntax**

```
reload
```

**Command Modes**

EXEC Privilege

**Command History**

**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information
If there is a change in the configuration, FTOS prompts you to save the new configuration. Or you can save your running configuration with the copy running-config command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy</td>
<td>Resets any designated stack member except the management unit.</td>
</tr>
<tr>
<td>disable-auto-reboot</td>
<td></td>
</tr>
</tbody>
</table>

**send**

Send messages to one or all terminal line users.

**Syntax**

```
send [*] | [line ] | [console] | [vty]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Enter the asterisk character * to send a message to all tty lines.</td>
</tr>
<tr>
<td>line</td>
<td>Send a message to a specific line. Range: 0 to 11</td>
</tr>
<tr>
<td>console</td>
<td>Enter the keyword console to send a message to the Primary terminal line.</td>
</tr>
<tr>
<td>vty</td>
<td>Enter the keyword vty to send a message to the Virtual terminal</td>
</tr>
</tbody>
</table>

**Defaults**

| Command Modes | EXEC |

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Messages can contain an unlimited number of lines; however, each line is limited to 255 characters. To move to the next line, use the <CR>. To send the message use CTR-Z, to abort a message use CTR-C.

**service timestamps**

Add time stamps to debug and log messages. This command adds either the uptime or the current time and date.

**Syntax**

```
service timestamps [debug | log] [datetime [localtime] | [msec] | [show-timezone] | uptime]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>(OPTIONAL) Enter the keyword debug to add timestamps to debug messages.</td>
</tr>
<tr>
<td>log</td>
<td>(OPTIONAL) Enter the keyword log to add timestamps to log messages with</td>
</tr>
<tr>
<td></td>
<td>severity 0 to 6.</td>
</tr>
<tr>
<td>datetime</td>
<td>(OPTIONAL) Enter the keyword datetime to have the current time and date added</td>
</tr>
<tr>
<td></td>
<td>to the message.</td>
</tr>
<tr>
<td>localtime</td>
<td>(OPTIONAL) Enter the keyword localtime to include the localtime in the</td>
</tr>
<tr>
<td></td>
<td>timestamp.</td>
</tr>
<tr>
<td>msec</td>
<td>(OPTIONAL) Enter the keyword msec to include milliseconds in the timestamp.</td>
</tr>
<tr>
<td>show-timezone</td>
<td>(OPTIONAL) Enter the keyword show-timezone to include the time zone</td>
</tr>
<tr>
<td></td>
<td>information in the timestamp.</td>
</tr>
<tr>
<td>uptime</td>
<td>(OPTIONAL) Enter the keyword uptime to have the timestamp based on time</td>
</tr>
<tr>
<td></td>
<td>elapsed since system reboot.</td>
</tr>
</tbody>
</table>
show alarms

View alarms.

Syntax

```
show alarms
```

Command Modes

- EXEC
- EXEC Privilege

Example

```
Figure 4-8. show alarms Command Example

FTOS# show alarms

-- Minor Alarms --
Alarm Type Duration
No minor alarms

-- Major Alarms --
Alarm Type Duration
No major alarms

FTOS#
```

show command-history

Display a buffered log of all commands entered by all users along with a time stamp.

Syntax

```
show command-history
```

Defaults

None.

Command Modes

- EXEC
- EXEC Privilege

Command History

```
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
```
One trace log message is generated for each command. No password information is saved to this file.

**Example**

```
FTOS#show command-history
[4/20 10:27:23]: CMD-(CLI):[enable]by default from console
[4/20 10:27:23]: CMD-(CLI):[configure terminal]by default from console

[4/20 10:27:23]: CMD-(CLI):[snmp-server community public ro]by default from console
[4/20 10:27:23]: CMD-(CLI):[logging 172.16.1.162]by default from console
[4/20 10:27:23]: CMD-(CLI):[logging 10.10.10.4]by default from console
[4/20 10:27:24]: CMD-(CLI):[logging 10.1.2.4]by default from console
[4/20 10:27:24]: CMD-(CLI):[logging 172.31.1.4]by default from console
[4/20 10:27:24]: CMD-(CLI):[management route 172.16.1.0 /24 10.11.209.4]by default from console
[4/20 10:27:24]: CMD-(CLI):[service timestamps log datetime]by default from console
[4/20 10:27:24]: CMD-(CLI):[line console 0]by default from console
[4/20 10:27:24]: CMD-(CLI):[exec-timeout 0]by default from console
[4/20 10:27:24]: CMD-(CLI):[exit]by default from console
[4/20 10:27:29]: CMD-(CLI):[show version]by default from console
[4/20 10:27:56]: CMD-(CLI):[show interfaces tengigabitethernet 0/3]by default from console
[4/20 10:55:8]: CMD-(CLI):[show lldp neighbors]by default from console
[4/20 15:17:6]: CMD-(CLI):[show cam-acl]by default from console
[4/20 16:34:59]: CMD-(CLI):[show running-config interface tengigabitethernet 0/55]by default from console
[4/20 16:38:14]: CMD-(CLI):[show vlan]by default from console
[5/4 9:11:52]: CMD-(TEL0):[show version]by admin from vty0 (10.11.68.14)
[5/4 9:12:9]: CMD-(TEL0):[show hosts]by admin from vty0 (10.11.68.14)
[5/4 9:14:38]: CMD-(TEL0):[show arp]by admin from vty0 (10.11.68.14)
[5/4 9:19:29]: CMD-(TEL0):[enable]by admin from vty0 (10.11.68.14)
[5/4 9:19:35]: CMD-(TEL0):[configure]by admin from vty0 (10.11.68.14)

- Repeated 1 time.

[5/4 9:19:50]: CMD-(TEL0):[interface tengigabitethernet 0/16]by admin from vty0 (10.11.68.14)
[5/4 9:20:11]: CMD-(TEL0):[exit]by admin from vty0 (10.11.68.14)

FTOS#
```

**clear command history**
Clears the command history log.

**show command-tree**
Display the entire CLI command tree, and optionally, display the utilization count for each command and its options.

**Syntax**
```
show command-tree [count | no]
```

**Parameters**

<table>
<thead>
<tr>
<th>count</th>
<th>Display the command tree with a usage counter for each command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Display all of the commands that may be preceded by the keyword no, which is the keyword used to remove a command from the running-configuration.</td>
</tr>
</tbody>
</table>

**Defaults**
None

**Command Mode**
EXEC
EXEC Privilege

**Command History**
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Reload the system to reset the command-tree counters.

**Example**

**Figure 4-10. show command-tree Command Example**

```
FTOS#show command-tree count
!
Enable privilege mode:

calendar command usage:5
  set option usage: 0
  hh:mm:ss option usage: 0
  <1-31> option usage: 0
  <MONTH> option usage: 0
  <1993-2035> option usage: 0
  <MONTH> option usage: 0
  <1-31> option usage: 0
  <1993-2035> option usage: 0

clear arp-cache command usage:2

clear ip dhcp binding A.B.C.D option usage: 0
  client option usage: 0
  statistics option usage: 0
  interface option usage: 0
  fastethernet option usage: 0
  fortyGigE option usage: 0
  SLOTPORT option usage: 0
  managementethernet option usage: 0
  SLOTPORT option usage: 0
  port-channel option usage: 0
  <1-128> option usage: 0
  tengigabitethernet option usage: 0
  SLOTPORT option usage: 0
  vlan option usage: 0
  <1-4094> option usage: 0
  conflict option usage: 0
  A.B.C.D option usage: 0
  server option usage: 0
  statistics option usage: 0
  snooping option usage: 0
  binding option usage: 0

clear ip fib command usage:4

clear ip route command usage:1

FTOS#
```

**show cpu-traffic-stats**

View the CPU traffic statistics.

**Syntax**

```
show cpu-traffic-stats [port number | all]
```

**Parameters**

<table>
<thead>
<tr>
<th><strong>port number</strong></th>
<th>(OPTIONAL) Enter the port number to display traffic statistics on that port only.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range: 1 to 1568</td>
</tr>
</tbody>
</table>

| **all**         | (OPTIONAL) Enter the keyword all to display traffic statistics on all the interfaces receiving traffic, sorted based on traffic. |

**Defaults**

- **all**

**Command Modes**

- **EXEC**
show debugging

View a list of all enabled debugging processes.

Syntax

show debugging

Command Mode

EXEC Privilege

Example

Figure 4-12. show debug Command Example

FTOS#show debug
Generic IP:  (Access List: test)
  IP packet debugging is on for   (Access List: test)
  TenGigabitEthernet 0/16
  ICMP packet debugging is on for
  TenGigabitEthernet 0/16
OSPF:
  OSPF packet debugging is on
DHCP:
  DHCP debugging is on
FTOS#

show environment

View system component status (for example, temperature, voltage).

Syntax

show environment [all | stack-unit unit-id]
**Parameters**

- `all` Enter the keyword `all` to view all components.
- `stack-unit unit-id` Enter the keyword `stack-unit` followed by the `unit-id` to display information on a specific stack member. Range: 0 to 5.
- `thermal sensor` Enter the keyword `thermal-sensor` to view all components.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Figure 4-13 shows the output of the `show environment fan` command as it appears prior to FTOS 7.8.1.0.

**Example**

**Figure 4-13. show environment all Command Example**

```
FTOS#show environment all
-- Unit Environment Status --
Unit Status Temp Voltage
---------------------------------------------------------------------------
* 0 online 47C ok
* Management Unit
-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6 Sensor7 Sensor8 Sensor9
---------------------------------------------------------------------------
--------------------
0 50 52 53 53 54 48 57 57 53
56
FTOS#
```

**Example**

**Figure 4-14. show environment stack-unit Command Example**

```
FTOS#show environment stack-unit 0
-- Unit Environment Status --
Unit Status Temp Voltage
---------------------------------------------------------------------------
0* online 49C ok
* Management Unit
```

**Example**

**Figure 4-15. show environment thermal-sensor Command Example**

```
FTOS#show environment thermal-sensor
-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6 Sensor7 Sensor8 Sensor9
---------------------------------------------------------------------------
--------------------
0 50 52 53 53 54 48 57 57 53
56
* Management Unit
FTOS#
```
show inventory

Displays the switch type, components (including media), FTOS version including hardware identification numbers and configured protocols.

**Syntax**

```plaintext
show inventory [media slot]
```

**Parameters**

- `media slot` (OPTIONAL) Enter the keyword `media` followed by the stack ID of the stack member for which you want to display pluggable media inventory.

**Defaults**

none

**Command Modes**

EXEC

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage**

If there are no fibre ports in the unit, only the header under `show inventory media` is displayed. If there are fibre ports but no optics inserted, the output displays the message “Media not present or accessible”.

**Example 1**

**Figure 4-16. show inventory for MXL 10/40GbE Switch IO Module Command Example**

```
FTOS#show inventory
System Type            : MXL-10/40GbE
System Mode            : 1.0
Software Version       : NAVASOTA-DEV-9-1-0-917
Unit Type               Serial Number  Part Number  Revision  
--------------------------------------------------------------
* 1  MXL-10/40GbE       TW282921F00048 0NVH81       2.0
   * - Management Unit
   Software Protocol Configured
   -----------------------------------
   SNMP
   LLDP
FTOS#
```

**Example 2**

**Figure 4-17. show inventory media Command Example**

```
FTOS#show inv media
Slot  Port  Type        Media               Serial Number        F10Qualid
-----------------------------------------------
  0   33  QSFP        40GBASE-CR4-1M      APF1149011J2Q           Yes
  0   37  QSFP        40GBASE-SR4         MLJ003P                  No
  0   41  QSFP        40GBASE-SR4         MLJ003P                  No
  0   42  QSFP        40GBASE-SR4         MLJ003P                  No
  0   43  QSFP        40GBASE-SR4         MLJ003P                  No
  0   44  QSFP        40GBASE-SR4         MLJ003P                  No
  0   45  QSFP        40GBASE-SR4         MLJ004Y                  No
  0   46  QSFP        40GBASE-SR4         MLJ004Y                  No
  0   47  QSFP        40GBASE-SR4         MLJ004Y                  No
  0   48  QSFP        40GBASE-SR4         MLJ004Y                  No
  0   49  QSFP        40GBASE-SR4         MK50012                 No
  0   50  QSFP        40GBASE-SR4         MK50012                 No
  0   51  QSFP        40GBASE-SR4         MK50012                 No
  0   52  QSFP        40GBASE-SR4         MK50012                 No
  0   53  QSFP        40GBASE-SR4         MK50012                 No
  0   54  QSFP        40GBASE-SR4         MK50012                 No
  0   55  QSFP        40GBASE-SR4         MK50012                 No
  0   56  QSFP        40GBASE-SR4         MK50012                 No
FTOS#
```
show memory

View current memory usage on the MXL switch.

Syntax

```
show memory [stack-unit 0-5]
```

Parameters

- `stack-unit 0-5` (OPTIONAL) Enter the keyword `stack-unit` followed by the stack unit ID of the stack member to display memory information on the designated stack member.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The output for the `show memory` command displays the memory usage of LP part (sysdlp) of the system. The Sysdlp is an aggregate task that handles all the tasks running on the CPU.

Example

```
Figure 4-18. show memory Command Example

FTOS#show memory stack-unit 0
Statistics On Unit 0 Processor

-----------------------------------------------
Total (b) Used (b) Free (b) Lowest (b) Largest (b)
268435456 4010354 264425102 264375410 264425102
```

show processes cpu

Display CPU usage information based on running processes.

Syntax

```
show processes cpu [management-unit 1-99 [details] | stack-unit 0-5 | summary | ipc | memory [stack-unit 0-5]]
```

Parameters

- `management-unit 1-99 [details]` (OPTIONAL) Display processes running in the control processor. The `1-99` variable sets the number of tasks to display in order of the highest CPU usage in the past five (5) seconds. Add the `details` keyword to display all running processes (except sysdlp). See Example 3.

- `stack-unit 0-5` (OPTIONAL) Enter the keyword `stack-unit` followed by the stack member ID (Range 0 to 5). As an option of `show processes cpu`, this option displays CPU usage for the designated stack member. See Example 2.

- `summary` (OPTIONAL) As an option of `memory`, this option limits the output of memory statistics to the designated stack member. See Example 5.
Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example 1

**Figure 4-19. show processes cpu summary Command Example**

```
FTOS#show processes cpu summary
CPU utilization 5Sec 1Min 5Min
-----------------------------
Unit0  0%   0%   0%
CPU utilization 5Sec 1Min 5Min
-----------------------------
Unit1*  1%  0%  0%
Unit2  0%   0%  0%
Unit3 0%   0%  0%
* Mgmt Unit
```

Example 2

**Figure 4-20. show processes cpu management-unit Command Example**

```
FTOS#show proc cpu management-unit 5
CPU utilization for five seconds: 6%/0%; one minute: 6%; five minutes: 7%
PID Process Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY
0x00000000 system 4650 465 10000 4.43% 4.43% 4.43% 0
0x00000112 sysd 56372590 5637259 10000 1.58% 1.78% 1.89% 0
0x00000107 sysdlp 9630080 963008 10000 0.79% 0.28% 0.33% 0
0x00000172 sysd 1435540 143554 10000 0.00% 0.10% 0.05% 0
0x000001fc igmp 1366570 136657 10000 0.00% 0.08% 0.05% 0
FTOS#
```
**Example 3**  
*Figure 4-21. show processes cpu stack-unit Command Example*

FTOS#show process cpu stack-unit 0

<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime(ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x763a7000</td>
<td>96806080</td>
<td>9680608</td>
<td>10000</td>
<td>3.00%</td>
<td>3.25%</td>
<td>2.93%</td>
<td>0</td>
</tr>
<tr>
<td>KP</td>
<td>26384050</td>
<td>2638405</td>
<td>10000</td>
<td>1.00%</td>
<td>0.50%</td>
<td>0.32%</td>
<td>0</td>
</tr>
<tr>
<td>frrpagt</td>
<td>491370</td>
<td>49137</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>F10StkMgr</td>
<td>665580</td>
<td>66558</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>lcMgr</td>
<td>37580</td>
<td>3758</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>dlia</td>
<td>452110</td>
<td>45211</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>sysAdmTsk</td>
<td>1751990</td>
<td>175199</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>timerMgr</td>
<td>14460</td>
<td>1446</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>PM</td>
<td>347970</td>
<td>34797</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>diagagt</td>
<td>90800</td>
<td>9080</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>ipc</td>
<td>50</td>
<td>5</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>tme</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>ttraceIpFlow</td>
<td>20</td>
<td>2</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>lnsScanUser_threads</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>isrTask</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>tTDB</td>
<td>22980</td>
<td>2298</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>tLogTask</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>GC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>bshell_reaper_threads</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>tSysLog</td>
<td>1106980</td>
<td>110698</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>tTimerTask</td>
<td>13131160</td>
<td>1313116</td>
<td>10000</td>
<td>0.00%</td>
<td>0.08%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>tExcTask</td>
<td>30</td>
<td>3</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>tLogTask</td>
<td>147650</td>
<td>14765</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
</tbody>
</table>
Example 4

Figure 4-22. show processes memory Command Example

Example 5

Figure 4-23. show processes memory stack-unit Command Example

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show hardware layer2 acl</td>
<td>Displays Layer 2 ACL data for the selected stack member and stack member port-pipe.</td>
</tr>
<tr>
<td>show hardware layer3</td>
<td>Displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.</td>
</tr>
<tr>
<td>show hardware stack-unit</td>
<td>Displays the data plane or management plane input and output statistics of the designated component of the designated stack member.</td>
</tr>
<tr>
<td>show hardware system-flow</td>
<td>Displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.</td>
</tr>
</tbody>
</table>
show processes ipc flow-control
Display the Single window protocol queue (SWPQ) statistics.

Syntax
show processes ipc flow-control [cp]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp</td>
<td>(OPTIONAL) Enter the keyword cp to view the Control Processor’s SWPQ statistics.</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example 1

Figure 4-24. show processes ipc flow-control Command Example

<table>
<thead>
<tr>
<th>Q Statistics on CP Processor</th>
<th>Cur Len</th>
<th>High Mark</th>
<th>Time Out</th>
<th>Retries</th>
<th>Msg Sent</th>
<th>Ack Rcvd</th>
<th>Aval Retra</th>
<th>Max Retra</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>ACL0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>ACL0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>ACL0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>ARPMSGR0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>LACP0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>RTM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>RTM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>60</td>
<td>60</td>
</tr>
</tbody>
</table>

FTOS#show processes ipc flow-control

Table 4-1 lists the definitions of the fields shown in Figure 4-24.

Table 4-1. Description of the show processes ipc flow-control cp output Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source QID /Tx Process</td>
<td>Source Service Identifier</td>
</tr>
<tr>
<td>Destination QID/Rx Process</td>
<td>Destination Service Identifier</td>
</tr>
<tr>
<td>Cur Len</td>
<td>Current number of messages enqueued</td>
</tr>
<tr>
<td>High Mark</td>
<td>Highest number of packets in the queue at any point of time</td>
</tr>
<tr>
<td>#of to / Timeout</td>
<td>Timeout count</td>
</tr>
<tr>
<td>#of Retr /Retries</td>
<td>Number of retransmissions</td>
</tr>
<tr>
<td>#msg Sent/Msg Sent/</td>
<td>Number of messages sent</td>
</tr>
<tr>
<td>#msg Ackd/Ack Rcvd</td>
<td>Number of messages acknowledged</td>
</tr>
</tbody>
</table>
The Single window protocol (SWP) provides flow control-based reliable communication between the sending and receiving software tasks.

**Important Points to Remember**

- A sending task enqueues messages into the SWP queue3 for a receiving task and waits for an acknowledgement.
- If no response is received within a defined period of time, the SWP timeout mechanism resubmits the message at the head of the FIFO queue.
- After retrying a defined number of times, the following timeout message is generated:
  
  SWP-2-NOMORETIMEOUT

- In the display output in Figure 4-24, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

**show processes memory**

Display memory usage information based on processes running in the system.

**Syntax**

```
show processes memory {management-unit | stack unit {0–5 | all | summary}}
```

**Parameters**

- `management-unit` Enter the keyword `management-unit` for CPU memory usage of the stack management unit.
- `stack unit 0–5` Enter the keyword `stack unit` followed by a stack unit ID of the member unit for which to display memory usage on the forwarding processor.
- `all` Enter the keyword `all` for detailed memory usage on all stack members.
- `summary` Enter the keyword `summary` for a brief summary of memory availability and usage on all stack members.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The output for the `show process memory` command displays the memory usage statistics running on CP part (sysd) of the system. The Sysd is an aggregate task that handles all the tasks running on MXL 10/40GbE Switch IO Module’s CP.
The output of `show memory` and this command will differ based on which FTOS processes are counted.

- In the `show memory` display output, the memory size is equal to the size of the application processes.
- In the output of this command, the memory size is equal to the size of the application processes plus the size of the system processes.

### Example

**Figure 4-25. show processes memory Command Example**

```
FTOS#show processes memory stack-unit 0
Total: 2147483648, MaxUsed: 378433536, CurrentUsed: 378433536, CurrentFree: 1769050112

<table>
<thead>
<tr>
<th>TaskName</th>
<th>TotalAllocated</th>
<th>TotalFreed</th>
<th>MaxHeld</th>
<th>CurrentHolding</th>
</tr>
</thead>
<tbody>
<tr>
<td>f10appioserv</td>
<td>225280</td>
<td>0</td>
<td>0</td>
<td>208896</td>
</tr>
<tr>
<td>ospf</td>
<td>573440</td>
<td>0</td>
<td>0</td>
<td>8716288</td>
</tr>
<tr>
<td>f10appioserv</td>
<td>225280</td>
<td>0</td>
<td>0</td>
<td>208896</td>
</tr>
<tr>
<td>fcoecntrl</td>
<td>262144</td>
<td>0</td>
<td>0</td>
<td>7917568</td>
</tr>
<tr>
<td>dhclient</td>
<td>548864</td>
<td>0</td>
<td>0</td>
<td>1310720</td>
</tr>
<tr>
<td>f10appioserv</td>
<td>225280</td>
<td>0</td>
<td>0</td>
<td>208896</td>
</tr>
<tr>
<td>ndpm</td>
<td>618496</td>
<td>0</td>
<td>0</td>
<td>7512064</td>
</tr>
<tr>
<td>f10appioserv</td>
<td>225280</td>
<td>0</td>
<td>0</td>
<td>208896</td>
</tr>
<tr>
<td>vrrp</td>
<td>335872</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

### Table 4-2. Descriptions of show processes memory output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Total system memory available</td>
</tr>
<tr>
<td>MaxUsed</td>
<td>Total maximum memory used ever (history indicated with time stamp)</td>
</tr>
<tr>
<td>CurrentUsed</td>
<td>Total memory currently in use</td>
</tr>
<tr>
<td>CurrentFree</td>
<td>Total system memory available</td>
</tr>
<tr>
<td>SharedUsed</td>
<td>Total used shared memory</td>
</tr>
<tr>
<td>SharedFree</td>
<td>Total free shared memory</td>
</tr>
</tbody>
</table>
show software ifm

Display interface management (IFM) data.

**Syntax**

```plaintext
show software ifm {clients [summary] | ifagt number | ifcb interface | stack-unit unit-ID | trace-flags}
```

**Parameters**

- `clients` Enter the keyword `clients` to display IFM client information.
- `summary` (OPTIONAL) Enter the keyword `summary` to display brief information about IFM clients.
- `ifagt number` Enter the keyword `ifagt` followed by the number of an interface agent to display software pipe and IPC statistics.
- `ifcb interface` Enter the keyword `ifcb` followed by one of the following interface IDs followed by the slot/port information to display interface control block information for that interface:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  - For a 10G Ethernet interface, enter the keyword `TenGigabitEthernet`.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
- `stack-unit unit-ID` Enter the keyword `stack-unit` followed by the stack member number to display IFM information for that unit.
  Range: 0-5
- `trace-flags` Enter the keyword `trace-flags` to display IFM information for internal trace flags.

**Defaults**

None

**Command Mode**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
show system

Display the current status of all stack members or a specific member.

**Syntax**

```
show system [brief | stack-unit unit-id]
```

**Parameters**

- `brief`  
  (OPTIONAL) Enter the keyword `brief` to view an abbreviated list of system information.

- `stack-unit unit-id`  
  (OPTIONAL) Enter the keyword `stack-unit` followed by the stack member ID for information on that stack member. Range: 0 to 5.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage**

- Figure 4-28 shows the output from the `show system brief` command.
- Figure 4-29 shows the output from the `show system stack-unit` command.
Example Figure 4-28. show system brief Command Example

FTOS#show system brief
Stack MAC : 00:1e:c9:f1:03:1a
Reload Type : normal-reload [Next boot : normal-reload]

-- Stack Info --
Unit   UnitType     Status         ReqTyp          CurTyp          Version     Ports
--------------------------------------------------------------------------------
----
0   Member       not present
1   Management   online         MXL-10/40GbE    MXL-10/40GbE    9-1-0-917   56
2   Member       not present
3   Member       not present
4   Member       not present
5   Member       not present

FTOS#

Example Figure 4-29. show system stack-unit Command Example

FTOS#show system stack-unit 0

-- Unit 0 --
Unit Type       : Management Unit
Status          : online
Next Boot       : online
Required Type   : MXL-10/40GbE - 34-port GE/TE/FG (XL)
Current Type    : MXL-10/40GbE - 34-port GE/TE/FG (XL)
Master priority : 0
Hardware Rev    : X01
Num Ports       : 56
Up Time         : 3 hr, 35 min
FTOS Version    : 8-3-16-160
Jumbo Capable   : yes
POE Capable     : no
Boot Flash      : A: 4.0.1.0bt1  B: 4.0.1.0bt1 [booted]
Boot Selector   : 4.0.0.0bt1
Memory Size     : 2147483648 bytes
Temperature     : 44C
Voltage         : ok
Switch Power    : GOOD
Product Name    : Force10 MXL 10/40GbE
Mfg By          : DELL
Mfg Date        : 2012-01-05
Serial Number   : DELL123456
Part Number     : 0NVH81X01
Piece Part ID   : N/A
PPID Revision   : N/A
Service Tag     : N/A
Expr Svc Code   : N/A
Chassis Svce Tag: RTWB200
Fabric Id       : C2
Asset tag       : test
PSOC FW Rev     : 0xb
ICT Test Date   : 0-0-0
ICT Test Info   : 0x0
Max Power Req   : 31488
Fabric Type     : 0x3
Fabric Maj Ver  : 0x1
Fabric Min Ver  : 0x0
SW Manageability: 0x4
HW Manageability: 0x1
Max Boot Time   : 6 minutes
Link Tuning     : unsupported
Auto Reboot     : enabled
Burned In MAC   : 00:01:e8:43:de:e1
No Of MACs      : 3
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset-tag</td>
<td>Assign and store unique asset-tag to the stack member.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the FTOS version.</td>
</tr>
<tr>
<td>show processes memory</td>
<td>Displays the memory usage based on the running processes.</td>
</tr>
<tr>
<td>show system stack-ports</td>
<td>Displays information about the stack ports on all switches in the stack.</td>
</tr>
<tr>
<td>show hardware stack-unit</td>
<td>Displays the data plane and management plane input and output statistics of a particular stack member.</td>
</tr>
<tr>
<td>stack-unit priority</td>
<td>Configures the ability of the switch to become the management unit of a stack.</td>
</tr>
</tbody>
</table>

**show tech-support**

Display a collection of data from other show commands, necessary for Dell Networking technical support to perform troubleshooting on MXL switches.

**Syntax**

```
show tech-support [stack-unit unit-id | page]
```

**Parameters**

- **stack-unit** (OPTIONAL) Enter the keyword `stack-unit` to view CPU memory usage for the stack member designated by `unit-id`. Range: 0 to 5
- **page** (OPTIONAL) Enter the keyword `page` to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press the ENTER key to view the next line of text.

When using the pipe command ( | ), enter one of these keywords to filter command output. Refer to Chapter 2, CLI Basics for details on filtering commands.

- **save** Enter the `save` keyword to save the command output.
- **flash:** Save to local flash drive (flash://filename (max 20 chars))

**Command Modes**

- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Examples Figure 4-30. show tech-support save Command Example (Partial)

```
FTOS#show tech-support ?
page                  Page through output
stack-unit            Unit Number
<cr>
FTOS#show tech-support stack-unit 1 ?
page                  Page through output
<cr>
FTOS#show tech-support stack-unit 1 | ?
except                Show only text that does not match a pattern
find                  Search for the first occurrence of a pattern
grep                  Show only text that matches a pattern
no-more                Don't paginate output
save                  Save output to a file

FTOS#show tech-support stack-unit 1 | save ?
flash:                Save to local file system (flash://filename (max 20 chars) )

FTOS#show tech-support stack-unit 1 | save flash://LauraSave
Start saving show command report .......
FTOS#

FTOS#dir
Directory of flash:

Directory of flash:

1 drwx 4096 Jan 01 1980 01:00:00 +01:00 .
2 drwx 2048 May 16 2012 10:49:01 +01:00 ..
3 drwx 4096 Jan 24 2012 19:38:32 +01:00 TRACE_LOG_DIR
4 drwx 4096 Jan 24 2012 19:38:32 +01:00 CORE_DUMP_DIR
5 d--- 4096 Jan 24 2012 19:38:34 +01:00 ADMIN_DIR
6 -rwx 10303 Mar 15 2012 18:37:20 +01:00 startup-config.bak
7 -rwx 7366 Apr 20 2012 10:57:02 +01:00 dhcpBindConflict
8 -rwx 4096 Feb 18 2012 07:05:02 +01:00 startup-config.backup
9 -rwx 12829 Feb 18 2012 02:24:14 +01:00 WJ_running-config
10 drwx 4096 Mar 08 2012 22:58:54 +01:00 WJ_running-config
11 -rwx 7689 Feb 21 2012 04:45:40 +01:00 stBkup

flash: 2143281152 bytes total (2131476480 bytes free)

FTOS#```
**Figure 4-31. show tech-support Command Example (Partial)**

```
FTOS#show tech-support stack-unit 0
Required Type : -
-- Unit 5 --
Unit Type : Member Unit
Status : not present
Required Type : -

----------------------------------- show environment -------------------
-- Unit Environment Status --
Unit Status        Temp   Voltage
---------------------------------------------------------------------------
* 1   online        41C    ok
* Management Unit
-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1
----------------------------------- show ip traffic -------------------
IP statistics:
Rcvd: 894390 total, 415557 local destination
  0 format errors, 0 checksum errors, 0 bad hop count
  0 unknown protocol, 0 not a gateway
  15 security failures, 0 bad options
Frags: 0 reassembled, 0 timeouts, 0 too big
  0 fragmented, 0 couldn't fragment
Bcast: 402 received, 0 sent; Mcast: 37 received, 0 sent
Sent: 468133 generated, 0 forwarded
  42 encapsulation failed, 0 no route

ICMP statistics:
Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 2 unreachable
  0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
  0 parameter, 0 timestamp, 0 info request, 0 other
Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
  0 mask requests, 0 mask replies, 0 quench, 0 timestamp
  0 info reply, 0 time exceeded, 0 parameter problem

UDP statistics:
Rcvd: 396516 total, 0 checksum errors, 0 no port
  0 short packets, 0 bad length, 28746 no port broadcasts, 0 socket full
Sent: 16460 total, 28746 forwarded broadcasts

TCP statistics:
Rcvd: 4618 total, 0 checksum errors, 0 no port
Sent: 5023 total

ARP statistics:
Rcvd: 43988 requests, 24518 replies, 10 wrong interface
Sent: 42 requests, 6 replies {0 proxy}
```

**Usage Information**

Without the page or stack-unit option, the command output is continuous, use Ctrl-z to interrupt the command output.

The save option works with other filtering commands. This allows you to save specific information of a show command. The save entry must always be the last option.

For example: `FTOS#show tech-support | grep regular-expression | except regular-expression | find regular-expression | save flash://result`
This display output is an accumulation of the same information that is displayed when you execute one of the following `show` commands:

- `show cam`
- `show clock`
- `show environment`
- `show file`
- `show interfaces`
- `show inventory`
- `show ip protocols`
- `show ip route summary`
- `show processes cpu`
- `show processes memory`
- `show redundancy`
- `show running-conf`
- `show version`

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show version</code></td>
<td>Displays the FTOS version.</td>
</tr>
<tr>
<td><code>show system</code></td>
<td>Displays the current switch status.</td>
</tr>
<tr>
<td><code>show environment</code></td>
<td>Displays system component status.</td>
</tr>
<tr>
<td><code>show processes memory</code></td>
<td>Displays memory usage based on the running processes.</td>
</tr>
</tbody>
</table>

### telnet

Connect through Telnet to a server. The Telnet client and server in FTOS supports IPv4 connections. You can establish a Telnet session directly to the router, or a connection can be initiated from the router.

#### Syntax

```
telnet {host | ip-address} [/source-interface]
```

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>host</code></td>
<td>Enter the name of a server.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>Enter the IPv4 address in dotted decimal format of the server.</td>
</tr>
<tr>
<td><code>source-interface</code></td>
<td>(OPTIONAL) Enter the keywords <code>source-interface</code> followed by the interface information to include the interface’s IP address. Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>- For a Loopback interface, enter the keyword <code>loopback</code> followed by a number from zero (0) to 16383.</td>
</tr>
<tr>
<td></td>
<td>- For the Null interface, enter the keyword <code>null</code> followed by 0.</td>
</tr>
<tr>
<td></td>
<td>- For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number: Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>- For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a VLAN interface, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>
Defaults
Not configured.

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
Telnet to link-local addresses is not supported.

terminal length
Configure the number of lines displayed on the terminal screen.

Syntax
terminal length screen-length
To return to the default values, use the terminal no length command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen-length</td>
<td>Enter a number of lines. Entering zero will cause the terminal to display without pausing. Range: 0 to 512. Default: 24 lines.</td>
</tr>
</tbody>
</table>

Defaults
24 lines

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

terminal xml
Enable XML mode in Telnet and SSH client sessions.

Syntax
terminal xml
To exit the XML mode, use the terminal no xml command.

Defaults
Disabled

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
tracert

View the packet path to a specific device.

Syntax

tracert {host | ip-address}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Enter the name of device.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the device in dotted decimal format.</td>
</tr>
</tbody>
</table>

Defaults

Timeout = 5 seconds; Probe count = 3; 30 hops max; 40 byte packet size; UDP port = 33434

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enter the tracert command without specifying an IP address (Extended Tracert), you are prompted for a target and source IP address, timeout in seconds (default is 5), a probe count (default is 3), minimum TTL (default is 1), maximum TTL (default is 30), and port number (default is 33434). To keep the default setting for those parameters, press the ENTER key.

Example

```
FTOS#tracert www.force10networks.com

Translating "www.force10networks.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.

-----------------------------------------------------
Tracing the route to www.force10networks.com (10.11.84.18), 30 hops max, 40 byte packets
-----------------------------------------------------

TTL Hostname        Probe1      Probe2      Probe3
1  10.11.199.190     001.000 ms  001.000 ms  002.000 ms
2  gwegress-sjc-02.force10networks.com (10.11.30.126) 005.000 ms  001.000 ms  001.000 ms
3  fw-sjc-01.force10networks.com (10.11.127.254) 000.000 ms  000.000 ms  000.000 ms
4  www.force10networks.com (10.11.84.18) 000.000 ms  000.000 ms  000.000 ms

FTOS#
```

Related Commands

- ping Tests the connectivity to a device.
**undebug all**

Disable all debug operations on the system.

**Syntax**

undebug all

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**virtual-ip**

Configure a virtual IP address for the active management interface. You can configure virtual addresses for IPv4 independently.

**Syntax**

virtual-ip \{ipv4-address\}

**Parameters**

\{ipv4-address\} Enter the IPv4 address (A.B.C.D) of the active management interface.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Each time this command is issued, it replaces the previously configured address of the same family. The no virtual-ip command now takes an address/prefix-length argument, so that the desired address only is removed. If you use the no virtual-ip command without any specified address, the IPv4 virtual addresses are removed.

**Example**

**Figure 4-33. virtual ip (IPv4) Command Example**

```
FTOS(virtual-ip) 10.11.197.99/16
```

**write**

Copy the current configuration to either the startup-configuration file or the terminal.

**Syntax**

write \{memory | terminal\}

**Parameters**

memory Enter the keyword memory to copy the current running configuration to the startup configuration file. This command is similar to the `copy running-config startup-config` command.

terminal Enter the keyword terminal to copy the current running configuration to the terminal. This command is similar to the `show running-config` command.
The `write memory` command saves the running-configuration to the file labeled `startup-configuration`. When using a LOCAL CONFIG FILE other than the startup-config not named “startup-configuration”, the running-config is not saved to that file; use the `copy` command to save any running-configuration changes to that local file.

**Command Modes**
EXEC Privilege

**Command History**

Version 8.3.16.1  Introduced on the MXL 10/40GbE Switch IO Module.
802.1X

The 802.1X Port Authentication commands are:

- debug dot1x
- dot1x auth-fail-vlan
- dot1x auth-server
- dot1x auth-type mab-only
- dot1x authentication (Configuration)
- dot1x authentication (Interface)
- dot1x guest-vlan
- dot1x host-mode
- dot1x mac-auth-bypass
- dot1x max-eap-req
- dot1x max-supplicants
- dot1x port-control
- dot1x quiet-period
- dot1x reauthentication
- dot1x reauth-max
- dot1x server-timeout
- dot1x supplicant-timeout
- dot1x tx-period
- show dot1x cos-mapping interface
- show dot1x interface

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only EAPOL (Extensible Authentication Protocol over LAN) traffic is allowed through the port to which a client is connected. Once authentication is successful, normal traffic passes through the port.

FTOS supports RADIUS and Active Directory environments using 802.1X Port Authentication.
Important Points to Remember

FTOS limits network access for certain users by using VLAN assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- 802.1X is supported on C-Series, E-Series, S-Series (S25/S50), S4810, S4820T, and E-Series Terascale.
- If no VLAN is supplied by the RADIUS server or if 802.1X authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1X authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If 802.1X authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If port security is enabled on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the force authorized, force unauthorized, or shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration will not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

**debug dot1x**

Display 802.1X debugging information.

**Syntax**

dump dot1x [all | auth-pae-fsm | backend-fsm | eapol-pdu] [interface interface]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable all 802.1X debug messages.</td>
</tr>
<tr>
<td>auth-pae-fsm</td>
<td>Enable authentication PAE FSM debug messages.</td>
</tr>
<tr>
<td>backend-fsm</td>
<td>Enable Backend FSM debug messages.</td>
</tr>
<tr>
<td>eapol-pdu</td>
<td>Enable EAPOL frame trace and related debug messages</td>
</tr>
<tr>
<td>interface</td>
<td>Restricts the debugging information to an interface.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled

**Command Modes**

EXEC Privilege
dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

Syntax

```
dot1x auth-fail-vlan vlan-id [max-attempts number]
```

To delete the authentication failure VLAN, use the `no dot1x auth-fail-vlan vlan-id [max-attempts number]` command.

Parameters

- `vlan-id` Enter the VLAN Identifier. Range: 1 to 4094
- `max-attempts number` (OPTIONAL) Enter the keyword `max-attempts` followed number of attempts desired before authentication fails. Range: 1 to 5 Default: 3

Defaults

3 attempts

Command Modes

CONFIGURATION (conf-if-interface-slot/port)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series and S-Series</td>
</tr>
</tbody>
</table>

Usage Information

If the host responds to 802.1X with an incorrect login/password, the login fails. The switch will attempt to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface is moved to the authentication failed VLAN.

Once the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication will occur at the next re-authentication interval (dot1x reauthentication).

Related Commands

- `dot1x port-control` Enable port control on an interface.
- `dot1x guest-vlan` Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.
- `show dot1x interface` Display the 802.1X configuration of an interface.
**dot1x auth-server**

Configure the authentication server to RADIUS.

**Syntax**

```
dot1x auth-server radius
```

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**dot1x auth-type mab-only**

Use only the host MAC address to authenticate a device with MAC authentication bypass (MAB).

**Syntax**

```
dot1x auth-type mab-only
```

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The prerequisites for enabling MAB-only authentication on a port are:

- 802.1X authentication must be enabled globally on the switch and on the port (**dot1x authentication** command).
- MAC authentication bypass must be enabled on the port (**dot1x mac-auth-bypass** command).

In MAB-only authentication mode, a port authenticates using the host MAC address even though 802.1x authentication is enabled. If the MAB-only authentication fails, the host is placed in the guest VLAN (if configured).

To disable MAB-only authentication on a port, enter the **no dot1x auth-type mab-only** command.
Related Commands

**dot1x mac-auth-bypass**  
Enable MAC authentication bypass.

**dot1x authentication (Configuration)**

Enable dot1x globally; dot1x must be enabled both globally and at the interface level.

**Syntax**

```
dot1x authentication
```

To disable dot1x on an globally, use the **no dot1x authentication** command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
<td></td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
<td></td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
<td></td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
<td></td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

- **dot1x authentication (Interface)**  
  Enable dot1x on an interface.

**dot1x authentication (Interface)**

Enable dot1x on an interface; dot1x must be enabled both globally and at the interface level.

**Syntax**

```
dot1x authentication
```

To disable dot1x on an interface, use the **no dot1x authentication** command.

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
<td></td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
<td></td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
<td></td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
<td></td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

- **dot1x authentication (Configuration)**  
  Enable dot1x globally.
**dot1x guest-vlan**

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

**Syntax**

```
dot1x guest-vlan vlan-id
```

To disable the guest VLAN, use the `no dot1x guest-vlan vlan-id` command.

**Parameters**

- `vlan-id` Enter the VLAN Identifier.
  Range: 1 to 4094

**Defaults**

Not configured

**Command Modes**

CONFIGURATION (conf-if-interface-slot/port)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

802.1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication, for the device, will occur at the next re-authentication interval (dot1x reauthentication).

If the host fails authentication for the designated amount of times, the authenticator places the port in authentication failed VLAN (dot1x auth-fail-vlan).

**Note:** Layer 3 portion of guest VLAN and authentication fail VLANs can be created regardless if the VLAN is assigned to an interface or not. Once an interface is assigned a guest VLAN (which has an IP address), then routing through the guest VLAN is the same as any other traffic. However, interface may join/leave a VLAN dynamically.

**Related Commands**

- `dot1x auth-fail-vlan` Configure an authentication failure VLAN.
- `dot1x reauthentication` Enable periodic re-authentication of the client.
- `dot1x reauth-max` Configure the maximum number of times to re-authenticate a port before it becomes unauthorized.

**dot1x host-mode**

Enable single-host or multi-host authentication.

**Syntax**

```
dot1x host-mode {single-host | multi-host | multi-auth}
```
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>single-host</td>
<td>Enable single-host authentication.</td>
</tr>
<tr>
<td>multi-host</td>
<td>Enable multi-host authentication.</td>
</tr>
<tr>
<td>multi-auth</td>
<td>Enable multi-supplicant authentication.</td>
</tr>
</tbody>
</table>

### Defaults

single-host

### Command Modes

INTERFACE

### Command History

- **Version 9.2(0.2)** Introduced on the MXL 10/40GbE Switch IO Module.
- **Version 8.3.19.0** Introduced on the S4820T.
- **Version 8.3.12.0** Introduced on the S4810.
- **Version 8.4.1.0** The multi-auth option was introduced on the C-Series and S-Series.
- **Version 8.3.2.0** The single-host and multi-host options were introduced on the C-Series, E-Series, and S-Series.

### Usage Information

- Single-host mode authenticates only one host per authenticator port, and drops all other traffic on the port.
- Multi-host mode authenticates the first host to respond to an Identity Request, and then permits all other traffic on the port.
- Multi-supplicant mode authenticates every device attempting to connect to the network on through the authenticator port.

---

### dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, FTOS attempts to authenticate the host based on its MAC address.

#### Syntax

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

#### Defaults

Disabled

#### Command Modes

INTERFACE

#### Command History

- **Version 9.2(0.2)** Introduced on the MXL 10/40GbE Switch IO Module.
- **Version 8.3.19.0** Introduced on the S4820T.
- **Version 8.3.12.0** Introduced on the S4810.
- **Version 8.4.1.0** Introduced on C-Series and S-Series

#### Usage Information

To disable MAC authentication bypass on a port, enter the `no dot1x mac-auth-bypass` command.
**dot1x max-eap-req**

Configure the maximum number of times an EAP (Extensive Authentication Protocol) request is transmitted before the session times out.

**Syntax**

```
dot1x max-eap-req number
```

To return to the default, use the `no dot1x max-eap-req` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the number of times an EAP request is transmitted before a session time-out. Range: 1 to 10 Default: 2</td>
</tr>
</tbody>
</table>

**Defaults**

2

**Command Modes**

INTERFACE

**Command History**

- Version 9.2(0.2) Introduced on the MXL 10/40GbE Switch IO Module.
- Version 8.3.19.0 Introduced on the S4820T.
- Version 8.3.12.0 Introduced on the S4810.
- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

**dot1x max-suppllicants**

Restrict the number of supplicants that can be authenticated and permitted to access the network through the port. This configuration is only takes effect in multi-auth mode.

**Syntax**

```
dot1x max-suppllicants number
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the number of supplicants that can be authenticated on a single port in multi-auth mode. Range: 1-128 Default: 128</td>
</tr>
</tbody>
</table>

**Defaults**

128 hosts can be authenticated on a single authenticator port.

**Command Modes**

INTERFACE

**Command History**

- Version 9.2(0.2) Introduced on the MXL 10/40GbE Switch IO Module.
- Version 8.3.19.0 Introduced on the S4820T.
- Version 8.3.12.0 Introduced on the S4810.
- Version 8.4.1.0 Introduced on C-Series and S-Series

**Related Commands**

- `dot1x host-mode` Enable single-host or multi-host authentication
**dot1x port-control**

Enable port control on an interface.

**Syntax**

```
dot1x port-control {force-authorized | auto | force-unauthorized}
```

**Parameters**

- `force-authorized`: Enter the keyword `force-authorized` to forcibly authorize a port.
- `auto`: Enter the keyword `auto` to authorize a port based on the 802.1X operation result.
- `force-unauthorized`: Enter the keyword `force-unauthorized` to forcibly de-authorize a port.

**Defaults**

No default behavior or values

**Command Modes**

Auto

**Command History**

- Version 9.2(0.2) Introduced on the MXL 10/40GbE Switch IO Module.
- Version 8.3.19.0 Introduced on the S4820T.
- Version 8.3.12.0 Introduced on the S4810.
- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

**Usage Information**

The authenticator performs authentication only when port-control is set to `auto`.

---

**dot1x quiet-period**

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

**Syntax**

```
dot1x quiet-period seconds
```

To disable quiet time, use the `no dot1x quiet-time` command.

**Parameters**

- `seconds`: Enter the number of seconds.  
  Range: 1 to 65535
  Default: 60

**Defaults**

60 seconds

**Command Modes**

INTERFACE

**Command History**

- Version 9.2(0.2) Introduced on the MXL 10/40GbE Switch IO Module.
- Version 8.3.19.0 Introduced on the S4820T.
- Version 8.3.12.0 Introduced on the S4810.
- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series
dot1x reauthentication

Enable periodic re-authentication of the client.

Syntax dot1x reauthentication [interval seconds]

To disable periodic re-authentication, use the no dot1x reauthentication command.

Parameters

- **interval seconds** (Optional) Enter the keyword interval followed by the interval time, in seconds, after which re-authentication will be initiated.
  Range: 1 to 31536000 (1 year)
  Default: 3600 (1 hour)

Defaults 3600 seconds (1 hour)

Command Modes INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

dot1x reauth-max

Configure the maximum number of times a port can re-authenticate before the port becomes unauthorized.

Syntax dot1x reauth-max number

To return to the default, use the no dot1x reauth-max command.

Parameters

- **number** Enter the permitted number of re-authentications.
  Range: 1 - 10
  Default: 2

Defaults 2

Command Modes INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
dot1x server-timeout

Configure the amount of time after which exchanges with the server time out.

Syntax

```
dot1x server-timeout seconds
```

To return to the default, use the `no dot1x server-timeout` command.

Parameters

- **seconds**: Enter a time-out value in seconds.
  
  Range: 1 to 300, where 300 is implementation dependant. Default: 30

Defaults

30 seconds

Command Modes

INTERFACE

Command History

- **Version 9.2(0.2)**: Introduced on the MXL 10/40GbE Switch IO Module.
- **Version 8.3.19.0**: Introduced on the S4820T.
- **Version 8.3.12.0**: Introduced on the S4810.
- **Version 7.6.1.0**: Introduced on C-Series and S-Series
- **Version 7.4.1.0**: Introduced on E-Series

Usage Information

When you configure the `dot1x server-timeout` value, you must take into account the communication medium used to communicate with an authentication server and the number of RADIUS servers configured. Ideally, the `dot1x server-timeout` value (in seconds) is based on the configured RADIUS-server timeout and retransmit values and calculated according to the following formula:

```
dot1x server-timeout seconds > (radius-server retransmit seconds + 1) * radius-server timeout seconds
```

Where the default values are as follows: `dot1x server-timeout` (30 seconds), `radius-server retransmit` (3 seconds), and `radius-server timeout` (5 seconds).

For example:

```
FTOS(conf)#radius-server host 10.11.197.105 timeout 6
FTOS(conf)#radius-server host 10.11.197.105 retransmit 4
FTOS(conf)#interface gigabitethernet 2/23
FTOS(conf-if-gi-2/23)#dot1x server-timeout 40
```

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time out.

Syntax

```
dot1x supplicant-timeout seconds
```

To return to the default, use the `no dot1x supplicant-timeout` command.

Parameters

- **seconds**: Enter a time-out value in seconds.
  
  Range: 1 to 300, where 300 is implementation dependant. Default: 30

Defaults

INTERFACE

Command History

- **Version 9.2(0.2)**: Introduced on the MXL 10/40GbE Switch IO Module.
- **Version 8.3.19.0**: Introduced on the S4820T.
- **Version 8.3.12.0**: Introduced on the S4810.
- **Version 7.6.1.0**: Introduced on C-Series and S-Series
- **Version 7.4.1.0**: Introduced on E-Series
**dot1x tx-period**

Configure the intervals at which EAPOL PDUs are transmitted by the Authenticator PAE.

**Syntax**

```
dot1x tx-period seconds
```

To return to the default, use the **no dot1x tx-period** command.

**Parameters**

- **seconds**
  - Enter the interval time, in seconds, that EAPOL PDUs are transmitted.
  - Range: 1 to 65535
  - Default: 30

**Defaults**

30 seconds

**Command Modes**

INTERFACE

**Command History**

- Version 9.2(0.2) Introduced on the MXL 10/40GbE Switch IO Module.
- Version 8.3.19.0 Introduced on the S4820T.
- Version 8.3.12.0 Introduced on the S4810.
- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

**show dot1x cos-mapping interface**

Display the CoS priority-mapping table provided by the RADIUS server and applied to authenticated supplicants on an 802.1X-enabled port.

**Syntax**

```
show dot1x cos-mapping interface interface [mac-address mac-address]
```
Parameters

- **interface**
  - Enter one of the following keywords and slot/port or number information:
    - For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
    - For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information.
    - For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

- **mac-address** (Optional) MAC address of an 802.1X-authenticated supplicant.

Defaults

No default values or behavior

Command Modes

- **EXEC**
  - EXEC privilege

Command History

- **Version 9.2(0.2)** Introduced on the MXL 10/40GbE Switch IO Module.
- **Version 8.3.19.0** Introduced on the S4820T.
- **Version 8.3.12.0** Introduced on the S4810.
- **Version 8.4.2.1** Introduced on the C-Series and S-Series

Usage Information

Enter a supplicant’s MAC address using the **mac-address** option to display CoS mapping information only for the specified supplicant.

You can display the CoS mapping information applied to traffic from authenticated supplicants on 802.1X-enabled ports that are in single-host, multi-host, and multi-suppliant authentication modes.

Example

```
FTOS#show dot1x cos-mapping interface gigabitethernet 2/21

802.1p CoS re-map table on Gi 2/21:
----------------------------------
     Dot1p    Remapped Dot1p
----------    -----------
        0          7
        1          6
        2          5
        3          4
        4          3
        5          2
        6          1
        7          0

FTOS#show dot1x cos-mapping int g 2/21 mac-address 00:00:01:00:07:00

802.1p CoS re-map table on Gi 2/21:
----------------------------------

802.1p CoS re-map table for Supplicant: 00:00:01:00:07:00
----------------------------------
     Dot1p    Remapped Dot1p
----------    -----------
        0          7
        1          6
        2          5
        3          4
        4          3
        5          2
```
show dot1x interface
Display the 802.1X configuration of an interface.

Syntax
show dot1x interface interface [mac-address mac-address]

Parameters
- **interface**: Enter one of the following keywords and slot/port or number information:
  - For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information.
  - For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
- **mac-address**: (Optional) MAC address of a supplicant.

Defaults
No default values or behavior

Command Modes
- EXEC
- EXEC privilege

Command History
- **Version 9.2(0.2)**: Introduced on the MXL 10/40GbE Switch IO Module.
- **Version 8.3.19.0**: Introduced on the S4820T.
- **Version 8.3.12.0**: Introduced on the S4810.
- **Version 8.4.2.1**: Introduced **mac-address** option on the C-Series and S-Series
- **Version 7.6.1.0**: Introduced on C-Series, E-Series, and S-Series

Usage
**C-Series and S-Series only**: Enter a supplicant’s MAC address using the **mac-address** option to display information only on the 802.1X-enabled port to which the supplicant is connected.

If 802.1X multi-supplicant authentication is enabled on a port, additional 802.1X configuration details (port authentication status, untagged VLAN ID, authentication PAE state, and backend state) are displayed for each supplicant as shown in the last example.

Example
```
FTOS#show dot1x int Gi 2/32

802.1x information on Gi 2/32:
-----------------------------
Dot1x Status:        Enable
Port Control:        AUTO
Port Auth Status:    UNAUTHORIZED
Re-Authentication:   Disable
Untagged VLAN id:    None
Guest VLAN:          Enable
Guest VLAN id:       10
Auth-Fail VLAN:      Enable
Auth-Fail VLAN id:  11
Auth-Fail Max-Attempts: 3
Tx Period:          30 seconds
```
Quiet Period: 60 seconds
ReAuth Max: 2
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req: 2
Auth Type: SINGLE_HOST

Auth PAE State: Initialize
Backend State: Initialize

FTOS#

Example
(show dot1x interface mac-address)

FTOS#show dot1x interface gig 2/21 mac-address 00:00:01:00:07:00

802.1x information on Gi 2/21:
----------------------------------
Dot1x Status: Enable
Port Control: AUTO
Re-Authentication: Disable
Guest VLAN: Disable
Guest VLAN id: NONE
Auth-Fail VLAN: Disable
Auth-Fail VLAN id: NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass: Enable
Mac-Auth-Bypass Only: Disable
Tx Period: 5 seconds
Quiet Period: 60 seconds
ReAuth Max: 1
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 60 seconds
Max-EAP-Req: 2
Host Mode: MULTI_AUTH
Max-Supplicants: 128

Port status and State info for Supplicant: 00:00:01:00:07:00

Port Auth Status: AUTHORIZED(MAC-AUTH-BYPASS)
Untagged VLAN id: 4094
Auth PAE State: Authenticated
Backend State: Idle

FTOS#

Example
(Multi-Supplicant Authentication enabled)

FTOS#show dot1x interface g 0/21

802.1x information on Gi 0/21:
----------------------------------
Dot1x Status: Enable
Port Control: AUTO
Re-Authentication: Disable
Guest VLAN: Enable
Guest VLAN id: 100
Auth-Fail VLAN: Disable
Auth-Fail VLAN id: NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass: Disable
Mac-Auth-Bypass Only: Disable
Tx Period: 30 seconds
Quiet Period: 60 seconds
ReAuth Max: 3
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 60 seconds
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max-EAP-Req:</td>
<td>2</td>
</tr>
<tr>
<td>Host Mode:</td>
<td>MULTI_AUTH</td>
</tr>
<tr>
<td>Max-Supplicants:</td>
<td>128</td>
</tr>
</tbody>
</table>

**Port status and State info for Supplicant: 00:00:00:00:00:10**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Auth Status:</td>
<td>AUTHORIZED</td>
</tr>
<tr>
<td>Untagged VLAN id:</td>
<td>400</td>
</tr>
<tr>
<td>Auth PAE State:</td>
<td>Authenticated</td>
</tr>
<tr>
<td>Backend State:</td>
<td>Idle</td>
</tr>
</tbody>
</table>

**Port status and State info for Supplicant: 00:00:00:00:00:11**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Auth Status:</td>
<td>AUTHORIZED</td>
</tr>
<tr>
<td>Untagged VLAN id:</td>
<td>300</td>
</tr>
<tr>
<td>Auth PAE State:</td>
<td>Authenticated</td>
</tr>
<tr>
<td>Backend State:</td>
<td>Idle</td>
</tr>
</tbody>
</table>

**Port status and State info for Supplicant: 00:00:00:00:00:15**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Auth Status:</td>
<td>AUTHORIZED(GUEST-VLAN)</td>
</tr>
<tr>
<td>Untagged VLAN id:</td>
<td>100</td>
</tr>
<tr>
<td>Auth PAE State:</td>
<td>Authenticated</td>
</tr>
<tr>
<td>Backend State:</td>
<td>Idle</td>
</tr>
</tbody>
</table>
Access Control Lists (ACL)

Overview

The Dell Networking operating software (FTOS) supports the following types of access control lists (ACLs), IP prefix lists, and route maps:

- Commands Common to all ACL Types
- Common IP ACL Commands
- Standard IP ACL Commands
- Extended IP ACL Commands
- Common MAC Access List Commands
- Standard MAC ACL Commands
- Extended MAC ACL Commands
- IP Prefix List Commands
- Route Map Commands

**Note:** For ACL commands used in the Trace function, refer to the Secure DHCP Commands section in the chapter Security.

Commands Common to all ACL Types

The following commands are available within each ACL mode and do not have mode-specific options. Some commands may use similar names, but require different options to support the different ACL types (for example, deny).

- description
- remark
- resequence access-list
- resequence prefix-list ipv4
- show config
**description**

configure a short text string describing the ACL.

**Syntax**

description text

**Parameters**

text Enter a text string up to 80 characters long.

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION-IP ACCESS-LIST-STANDARD
CONFIGURATION-IP ACCESS-LIST-EXTENDED
CONFIGURATION-MAC ACCESS LIST-STANDARD
CONFIGURATION-MAC ACCESS LIST-EXTENDED

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**remark**

Enter a description for an ACL entry.

**Syntax**

remark [remark-number] [description]

**Parameters**

remark-number Enter the remark number. Note that you can use the same sequence number for the remark and an ACL rule.

Range: 0 to 4294967290

description Enter a description of up to 80 characters.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION-IP ACCESS-LIST-STANDARD
CONFIGURATION-IP ACCESS-LIST-EXTENDED
CONFIGURATION-MAC ACCESS LIST-STANDARD
CONFIGURATION-MAC ACCESS LIST-EXTENDED

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The remark command is available in each ACL mode. You can configure up to 4294967290 remarks in a given ACL.

The following example shows the use of the remark command twice within CONFIGURATION-IP ACCESS-LIST-STANDARD mode. Here, the same sequence number was used for the remark and for an associated ACL rule. The remark precedes the rule in the running-config because it is assumed that the remark is for the rule with the same sequence number, or the group of rules, that follow the remark.
**resequence access-list**

Re-assign sequence numbers to entries of an existing access-list.

**Syntax**

```
resequence access-list {ipv4 | mac} {access-list-name StartingSeqNum Step-to-Increment}
```

**Parameters**

- **ipv4 | mac**
  - Enter the keyword ipv4 or mac to identify the access list type to resequence.

- **access-list-name**
  - Enter the name of a configured IP access list.

- **StartingSeqNum**
  - Enter the starting sequence number to resequence.
  - Range: 0 to 4294967290

- **Step-to-Increment**
  - Enter the step to increment the sequence number.
  - Range: 1 to 4294967290

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When all sequence numbers have been exhausted, this feature permits re-assigning of a new sequence number to entries of an existing access-list.

**Related Commands**

- `resequence prefix-list ipv4` - Resequences a prefix list

---

**Example**

```
FTOS(conf-std-nacl)#remark 10 Deny rest of the traffic
FTOS(conf-std-nacl)#remark 5 Permit traffic from XYZ Inc.
FTOS(conf-std-nacl)#show config
!
ip access-list standard test
remark 5 Permit traffic from XYZ Inc.
seq 5 permit 1.1.1.0/24
remark 10 Deny rest of the traffic
seq 10 Deny any
FTOS(conf-std-nacl)#
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>prefix-list-name</strong></td>
<td>Enter the name of configured prefix list, up to 140 characters long.</td>
</tr>
<tr>
<td><strong>StartingSeqNum</strong></td>
<td>Enter the starting sequence number to resequence. Range: 0 to 65535</td>
</tr>
<tr>
<td><strong>Step-to-Increment</strong></td>
<td>Enter the step to increment the sequence number. Range: 1 to 65535</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

EXEC
EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When all sequence numbers have been exhausted, this feature permits re-assigning new sequence numbers to entries of an existing prefix list.

**Related Commands**

- `seq` Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

---

### show config

Display the current ACL configuration.

**Syntax**

show config

**Command Modes**

CONFIGURATION-IP ACCESS-LIST-STANDARD
CONFIGURATION-IP ACCESS-LIST-EXTENDED
CONFIGURATION-MAC ACCESS LIST-STANDARD
CONFIGURATION-MAC ACCESS LIST-EXTENDED

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
Figure 6-2. show config Command Example

FTOS(conf-ext-nacl)#show conf
!
ip access-list extended patches
FTOS(conf-ext-nacl)#
```

---

### Common IP ACL Commands

The following commands are available within both IP ACL modes (Standard and Extended) and do not have mode-specific options. When an access-list (ACL) is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

The MXL 10/40GbE Switch IO Module platform supports both ingress and egress IP ACLs.
The following commands allow you to clear, display, and assign IP ACL configurations.

- `access-class`
- `clear counters ip access-group`
- `ip access-group`
- `show ip access-lists`
- `show ip accounting access-list`

**Note:** See also [Commands Common to all ACL Types](#).

### access-class

Apply a standard ACL to a terminal line.

**Syntax**

```plaintext
access-class access-list-name
```

**Parameters**

- `access-list-name` Enter the name of a configured Standard ACL, up to 140 characters.

**Defaults**

Not configured.

**Command Modes**

- `LINE`

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### clear counters ip access-group

Erase all counters maintained for access lists.

**Syntax**

```plaintext
clear counters ip access-group [access-list-name]
```

**Parameters**

- `access-list-name` (OPTIONAL) Enter the name of a configured access-list, up to 140 characters.

**Command Modes**

- `EXEC Privilege`

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### ip access-group

Assign an IP access list (IP ACL) to an interface.

**Syntax**

```plaintext
ip access-group access-list-name {in | out} [implicit-permit] [vlan vlan-id]
```

**Parameters**

- `access-list-name` Enter the name of a configured access list, up to 140 characters.
- `in` Enter the keyword `in` to apply the ACL to incoming traffic.
- `out` Enter the keyword `out` to apply the ACL to outgoing traffic.
<table>
<thead>
<tr>
<th>Command Modes</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command History</td>
<td>Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

Usage Information

You can assign one ACL (standard or extended ACL) to an interface.

**Note:** This command is not supported on the MXL Switch loopback interfaces.

When you apply an ACL that filters IGMP traffic, all IGMP traffic is redirected to the CPUs and soft-forwarded, if required, in the following scenarios:

- on a Layer 2 interface - if a Layer 3 ACL is applied to the interface.
- on a Layer 3 port or on a Layer 2/Layer 3 port

## Related Commands

- `ip access-list standard` Configures a standard ACL.
- `ip access-list extended` Configures an extended ACL.

## show ip access-lists

Display all of the IP ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/mismatches against each ACL entry displayed.

**Syntax**

```
show ip access-lists [access-list-name] [interface interface] [in]
```

**Parameters**

- `access-list-name` Enter the name of a configured MAC ACL, up to 140 characters.
- `interface interface` Enter the keyword `interface` followed by the one of the following keywords and slot/port or number information:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
- `in` Identify whether ACL is applied on ingress side.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
show ip accounting access-list

Display the IP access-lists created on the switch and the sequence of filters.

Syntax

```plaintext
show ip accounting {access-list access-list-name | cam_count} interface interface
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-name</td>
<td>Enter the name of the ACL to be displayed.</td>
</tr>
<tr>
<td>cam_count</td>
<td>List the count of the CAM rules for this ACL.</td>
</tr>
</tbody>
</table>
| interface interface | Enter the keyword interface followed by the interface type and slot/port or number information:  
  • For a Port Channel interface, enter the keyword port-channel followed by a number:  
    Range: 1-128  
  • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.  
  • For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information. |

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```plaintext
FTOS#show ip accounting access FILTER1 interface tengig 1/6
Extended IP access list FILTER1
  seq 5 deny ip any 191.1.0.0 /16 count (0x00 packets)
  seq 10 deny ip any 191.2.0.0 /16 order 4
  seq 15 deny ip any 191.3.0.0 /16
  seq 20 deny ip any 191.4.0.0 /16
  seq 25 deny ip any 191.5.0.0 /16
```

Table 6-1 defines the information in Figure 6-3.

Table 6-1. show ip accounting access-lists Command Example Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Extended IP...”</td>
<td>Displays the name of the IP ACL.</td>
</tr>
<tr>
<td>“seq 5...”</td>
<td>Displays the filter. If the keywords count or byte were configured in the filter, the number of packets or bytes processed by the filter is displayed at the end of the line.</td>
</tr>
<tr>
<td>“order 4”</td>
<td>Displays the QoS order of priority for the ACL entry.</td>
</tr>
</tbody>
</table>
Standard IP ACL Commands

When an ACL is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

The MXL 10/40GbE Switch IO Module platform supports both ingress and egress IP ACLs.

The commands needed to configure a Standard IP ACL are:

- deny
- ip access-list standard
- permit

Note: See also Commands Common to all ACL Types and Common IP ACL Commands.

deny

Configure a filter to drop packets with a certain IP address.

Syntax
deny {source [mask] | any | host ip-address} [count [byte]] [dscp value] [order] [fragments]

To remove this filter, you have two choices:
- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny {source [mask] | any | host ip-address} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Enter the IP address in dotted decimal format of the network from which the packet was sent.</td>
</tr>
<tr>
<td>mask</td>
<td>(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous (discontiguous).</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword host followed by the IP address to specify a host IP address only.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword count to count packets processed by the filter.</td>
</tr>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.</td>
</tr>
<tr>
<td>dscp</td>
<td>(OPTIONAL) Enter the keyword dscp to match to the IP DSCP values.</td>
</tr>
<tr>
<td>order</td>
<td>(OPTIONAL) Enter the keyword order to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the order keyword is not used, the ACLs have the lowest order by default (255).</td>
</tr>
<tr>
<td>fragments</td>
<td>Enter the keyword fragments to use ACLs to control packet fragments.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

CONFIGURATION-IP ACCESS-LIST-STANDARD
The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service (QoS) chapter of the FTOS Configuration Guide.

In the MXL Switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

### Related Commands

- `ip access-list standard` Configures a standard ACL.
- `permit` Configures a permit filter.

---

### ip access-list standard

Create a standard IP access list (IP ACL) to filter based on IP address.

#### Syntax

```
ip access-list standard access-list-name
```

#### Parameters

- `access-list-name` Enter a string up to 140 characters long as the ACL name.

#### Defaults

All IP access lists contain an implicit `deny any`, that is, if no match occurs, the packet is dropped.

#### Command Modes

- **CONFIGURATION**

#### Command History

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

#### Usage Information

FTOS supports one ingress and one egress IP ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your switch documentation.

#### Example

**Figure 6-4. ip access-list standard Command Example**

```
FTOS(conf)#ip access-list standard TestList
FTOS(conf-std-nacl)#
```

### Related Commands

- `ip access-list extended` Creates an extended access list.
- `resequence access-list` Displays the current configuration.

---

### permit

Configure a filter to permit packets from a specific source IP address to leave the switch.

#### Syntax

```
permit {source [mask] | any | host ip-address} [count [byte]] [dscp value] [order]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
Parameters

- Use the no permit {source [mask] | any | host ip-address} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Enter the IP address in dotted decimal format of the network from which the</td>
</tr>
<tr>
<td>mask</td>
<td>packet was sent. (OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword host followed by the IP address to specify a host IP address or hostname.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword count to count packets processed by the filter.</td>
</tr>
<tr>
<td>dscp</td>
<td>(OPTIONAL) Enter the keyword dscp to match to the IP DSCP values.</td>
</tr>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.</td>
</tr>
<tr>
<td>order</td>
<td>(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the order keyword is not used, the ACLs have the lowest order by default (255).</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

CONFIGURATION-IP ACCESS-LIST-STANDARD

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The order option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service (QoS) chapter of the FTOS Configuration Guide.

In the MXL Switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Assign an IP ACL filter to deny IP packets.</td>
</tr>
<tr>
<td>ip access-list standard</td>
<td>Create a standard ACL.</td>
</tr>
</tbody>
</table>

seq

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

Syntax

seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count [byte] [dscp value] [order] [fragments]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence-number</td>
<td>Enter a number from 0 to 4294967290. Range: 0 to 65534</td>
</tr>
<tr>
<td>deny</td>
<td>Enter the keyword deny to configure a filter to drop packets meeting this condition.</td>
</tr>
<tr>
<td>permit</td>
<td>Enter the keyword permit to configure a filter to forward packets meeting this criteria.</td>
</tr>
</tbody>
</table>
### Defaults

Not configured

### Command Modes

**CONFIGURATION-IP ACCESS-LIST-STANDARD**

### Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq sequence-number` is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via QoS policy framework.
- The `order` option takes precedence over the `seq sequence-number`.
- If `sequence-number` is not configured, then rules with the same order value are ordered according to their configuration order.
- If the `sequence-number` is configured, then the `sequence-number` is used as a tie breaker for rules with the same order.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Configures a filter to drop packets.</td>
</tr>
<tr>
<td>permit</td>
<td>Configures a filter to forward packets.</td>
</tr>
<tr>
<td>seq</td>
<td>Assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.</td>
</tr>
</tbody>
</table>
Extended IP ACL Commands

When an ACL is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

The following commands configure extended IP ACLs, which in addition to the IP address also examine the packet’s protocol type.

The MXL 10/40GbE Switch IO Module platform supports both ingress and egress IP ACLs.

- deny
- deny icmp
- deny tcp
- deny udp
- ip access-list extended
- permit
- permit icmp
- permit tcp
- permit udp
- seq

Note: See also Commands Common to all ACL Types and Common IP ACL Commands.

deny

Configure a filter that drops IP packets meeting the filter criteria.

Syntax

deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [byte]] [dscp value] [order] [fragments]

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Enter the keyword ip to configure a generic IP access list. The keyword ip</td>
</tr>
<tr>
<td></td>
<td>specifies that the access list will deny all IP protocols.</td>
</tr>
<tr>
<td>ip-protocol-number</td>
<td>Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.</td>
</tr>
<tr>
<td>source</td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword host followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td>destination</td>
<td>Enter the IP address of the network or host to which the packets are sent.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword count to count packets processed by the filter.</td>
</tr>
</tbody>
</table>
deny icmp

Configure a filter to drop all or specific ICMP messages.

Syntax

```
deny icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} [dscp] [message-type] [count [byte]] [order] [fragments]
```

Parameters

- **source**: Enter the IP address of the network or host from which the packets were sent.
- **mask**: Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- **any**: Enter the keyword any to specify that all routes are subject to the filter.
- **host ip-address**: Enter the keyword host followed by the IP address to specify a host IP address.
- **destination**: Enter the IP address of the network or host to which the packets are sent.
- **dscp**: Enter this keyword to deny a packet based on DSCP value. Range: 0-63
- **message-type**: Enter the ICMP packet type. For more information, refer to the documentation for the ICMP type you want to filter.
- **count**: (OPTIONAL) Enter the keyword count to count packets processed by the filter.
- **byte**: (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.
- **dscp**: (OPTIONAL) Enter the keyword dscp to match to the IP DSCP values.
- **order**: (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) 
  Default: If the order keyword is not used, the ACLs have the lowest order by default (255).
- **fragments**: Enter the keyword fragments to use ACLs to control packet fragments.

Related Commands

- **deny tcp**: Assigns a filter to deny TCP packets.
- **deny udp**: Assigns a filter to deny UDP packets.
- **ip access-list extended**: Creates an extended ACL.

Defaults

Not configured.

Command Modes

CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The order option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service (QoS) chapter of the FTOS Configuration Guide.

In the MXL Switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.
message-type (OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 6-2).
   Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code

count (OPTIONAL) Enter the keyword count to count packets processed by the filter.

byte (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.

order (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry.
   Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)
   Default: If the order keyword is not used, the ACLs have the lowest order by default (255).

fragments Enter the keyword fragments to use ACLs to control packet fragments.

Defaults
Not configured

Command Modes
CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
The order option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service (QoS) chapter of the FTOS Configuration Guide.

Table 6-2 lists the keywords displayed in the CLI help and their corresponding ICMP message type name.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>ICMP Message Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>administratively-prohibited</td>
<td>Administratively prohibited</td>
</tr>
<tr>
<td>alternate-address</td>
<td>Alternate host address</td>
</tr>
<tr>
<td>conversion-error</td>
<td>Datagram conversion error</td>
</tr>
<tr>
<td>dod-host-prohibited</td>
<td>Host prohibited</td>
</tr>
<tr>
<td>dod-net-prohibited</td>
<td>Net prohibited</td>
</tr>
<tr>
<td>echo</td>
<td>Echo</td>
</tr>
<tr>
<td>echo-reply</td>
<td>Echo reply</td>
</tr>
<tr>
<td>general-parameter-problem</td>
<td>Parameter problem</td>
</tr>
<tr>
<td>host-isolated</td>
<td>Host isolated</td>
</tr>
<tr>
<td>host-precedence-unreachable</td>
<td>Host unreachable for precedence</td>
</tr>
<tr>
<td>host-redirect</td>
<td>Host redirect</td>
</tr>
<tr>
<td>host-tos-prohibited</td>
<td>Host redirect for TOS</td>
</tr>
<tr>
<td>host-tos-unreachable</td>
<td>Host unreachable for TOS</td>
</tr>
<tr>
<td>host-unknown</td>
<td>Host unknown</td>
</tr>
<tr>
<td>host-unreachable</td>
<td>Host unreachable</td>
</tr>
<tr>
<td>information-reply</td>
<td>Information replies</td>
</tr>
<tr>
<td>information-request</td>
<td>Information requests</td>
</tr>
</tbody>
</table>
deny tcp

Configure a filter that drops TCP packets meeting the filter criteria.

**Syntax**

deny tcp {source mask | any | host ip-address} [bit] [operator port [port]] {destination mask | any | host ip-address} [bit] [operator port [port]] [count [byte]] [order] [fragments]

To remove this filter, you have two choices:

- Use the **no seq sequence-number** command if you know the filter’s sequence number.
- Use the **no deny tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}** command.
**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword host followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td>dscp</td>
<td>Enter this keyword to deny a packet based on DSCP value. Range: 0-63</td>
</tr>
<tr>
<td>bit</td>
<td>Enter a flag or combination of bits:</td>
</tr>
<tr>
<td></td>
<td>- ack: acknowledgement field</td>
</tr>
<tr>
<td></td>
<td>- fin: finish (no more data from the user)</td>
</tr>
<tr>
<td></td>
<td>- psh: push function</td>
</tr>
<tr>
<td></td>
<td>- rst: reset the connection</td>
</tr>
<tr>
<td></td>
<td>- syn: synchronize sequence numbers</td>
</tr>
<tr>
<td></td>
<td>- urg: urgent field</td>
</tr>
<tr>
<td>operator</td>
<td>(OPTIONAL) Enter one of the following logical operand:</td>
</tr>
<tr>
<td></td>
<td>- eq = equal to</td>
</tr>
<tr>
<td></td>
<td>- neq = not equal to</td>
</tr>
<tr>
<td></td>
<td>- gt = greater than</td>
</tr>
<tr>
<td></td>
<td>- lt = less than</td>
</tr>
<tr>
<td></td>
<td>- range = inclusive range of ports (you must specify two ports for the port command parameter.</td>
</tr>
<tr>
<td>port port</td>
<td>Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers:</td>
</tr>
<tr>
<td></td>
<td>- 23 = Telnet</td>
</tr>
<tr>
<td></td>
<td>- 20 and 21 = FTP</td>
</tr>
<tr>
<td></td>
<td>- 25 = SMTP</td>
</tr>
<tr>
<td></td>
<td>- 169 = SNMP</td>
</tr>
<tr>
<td>destination</td>
<td>Enter the IP address of the network or host to which the packets are sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword count to count packets processed by the filter.</td>
</tr>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.</td>
</tr>
<tr>
<td>order</td>
<td>(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the order keyword is not used, the ACLs have the lowest order by default (255).</td>
</tr>
<tr>
<td>fragments</td>
<td>Enter the keyword fragments to use ACLs to control packet fragments.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION-IP ACCESS-LIST-EXTENDED

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
The order option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service (QoS) chapter of the FTOS Configuration Guide.

In the MXL Switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (gt, lt, range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port range 4000 - 8000 uses eight entries in the CAM:

```
Rule#   Data             Mask       From  To    #Covered
1       0000111110100000 1111111110000000 4000  4031  32
2       0000111111000000 1111111111000000 4032  4095  64
3       0000100000000000 1111100000000000 4096  6143  2048
4       0001100000000000 1111110000000000 6144  7167  1024
5       0001110000000000 1111111000000000 7168  7679  512
6       0001111000000000 1111111100000000 7680  7935  256
7       0001111100000000 1111111110000000 7936  7999  64
8       0001111101000000 1111111111000000 8000  8000  1
```

Total Ports: 4001

But an ACL rule with TCP port lt 1023 takes only one entry in the CAM:

```
Rule#   Data             Mask       From  To    #Covered
1       0000000000000000 1111110000000000 0     1023  1024
```

Total Ports: 1024

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny udp</td>
<td>Assigns a filter to deny UDP traffic.</td>
</tr>
</tbody>
</table>

deny udp

Configure a filter to drop UDP packets meeting the filter criteria.

Syntax

deny udp {source mask | any | host ip-address} [operator port [port]] {destination mask | any | host ip-address} [dscp] [operator port [port]] [count [byte]] [order] [fragments]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
</tbody>
</table>
any
Enter the keyword any to specify that all routes are subject to the filter.

host ip-address
Enter the keyword host followed by the IP address to specify a host IP address.

dscp
Enter this keyword to deny a packet based on DSCP value.
Range: 0-63

operator
(Optional) Enter one of the following logical operand:
• eq = equal to
• neq = not equal to
• gt = greater than
• lt = less than
• range = inclusive range of ports

port port
(Optional) Enter the application layer port number. Enter two port numbers if using the range logical operand.
Range: 0 to 65535

destination
Enter the IP address of the network or host to which the packets are sent.

mask
Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

count
(Optional) Enter the keyword count to count packets processed by the filter.

byte
(Optional) Enter the keyword byte to count bytes processed by the filter.

order
(Optional) Enter the keyword order to specify the QoS priority for the ACL entry.
Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)
Default: If the order keyword is not used, the ACLs have the lowest order by default (255).

fragments
Enter the keyword fragments to use ACLs to control packet fragments.

Defaults
Not configured

Command Modes
CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
The order option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service (QoS) chapter of the FTOS Configuration Guide.

In the MXL Switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (gt, lt, range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.
For example, an ACL rule with TCP port range 4000 - 8000 will use eight entries in the CAM:

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000111111010000 1111111111000000</td>
<td>4000  4031</td>
<td></td>
<td></td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111100000 1111111111000000</td>
<td>4032  4095</td>
<td></td>
<td></td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000 1111100000000000</td>
<td>4096  6143</td>
<td></td>
<td></td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000 1111110000000000</td>
<td>6144  7167</td>
<td></td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000 1111111000000000</td>
<td>7168  7679</td>
<td></td>
<td></td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111000000000 1111111100000000</td>
<td>7680  7935</td>
<td></td>
<td></td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000 1111111111000000</td>
<td>7936  7999</td>
<td></td>
<td></td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111101000000 1111111111111111</td>
<td>8000  8000</td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Total Ports: 4001

But an ACL rule with TCP port lt 1023 takes only one entry in the CAM:

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000000000000000 1111110000000000</td>
<td>0     1023</td>
<td></td>
<td></td>
<td>1024</td>
</tr>
</tbody>
</table>

Total Ports: 1024

Related Commands
- `deny` Assigns a deny filter for IP traffic.
- `deny tcp` Assigns a deny filter for TCP traffic.

**ip access-list extended**

Name (or select) an extended IP access list (IP ACL) based on IP addresses or protocols.

**Syntax**

```
ip access-list extended access-list-name
```

To delete an access list, use the `no ip access-list extended access-list-name` command.

**Parameters**

- `access-list-name` Enter a string up to 140 characters long as the access list name.

**Defaults**

All access lists contain an implicit `deny any`; that is, if no match occurs, the packet is dropped.

**Command Modes**

CONFIGURATION

**Usage Information**

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your switch documentation.

**Example**

```
Figure 6-5.  ip access-list extended Command Example

FTOS(config)#ip access-list extended TESTListEXTEND
FTOS(config-ext-nacl)#
```

**Related Commands**

- `ip access-list standard` Configures a standard IP access list.
- `resequence access-list` Displays the current configuration.
Configuring an Access Control List (ACL)

**permit**

Configure a filter to pass IP packets meeting the filter criteria.

**Syntax**

```
permit {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [byte] [dscp value] [order] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Enter the keyword <code>ip</code> to configure a generic IP access list. The keyword <code>ip</code> specifies that the access list will permit all IP protocols.</td>
</tr>
<tr>
<td>ip-protocol-number</td>
<td>Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header. Range: 0 to 128</td>
</tr>
<tr>
<td>source</td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword <code>any</code> to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword <code>host</code> followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td>destination</td>
<td>Enter the IP address of the network or host to which the packets are sent.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.</td>
</tr>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.</td>
</tr>
<tr>
<td>dscp</td>
<td>(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.</td>
</tr>
<tr>
<td>order</td>
<td>(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS order of priority for the ACL entry.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)</td>
</tr>
<tr>
<td>fragments</td>
<td>Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION-IP ACCESS-LIST-EXTENDED

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service (QoS) chapter of the FTOS Configuration Guide.

In the MXL Switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.
permit icmp

Configure a filter to allow all or specific ICMP messages.

**Syntax**

```plaintext
permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} [dscp] [message-type] [count [byte]] [order] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} command.

**Parameters**

- `source` Enter the IP address of the network or host from which the packets were sent.
- `mask` Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- `any` Enter the keyword `any` to specify that all routes are subject to the filter.
- `host ip-address` Enter the keyword `host` followed by the IP address to specify a host IP address.
- `destination` Enter the IP address of the network or host to which the packets are sent.
- `dscp` Enter this keyword to deny a packet based on DSCP value.
  - Range: 0-63
- `message-type` (OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 6-2).
  - Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code
- `count` (OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
- `byte` (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
- `order` (OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry.
  - Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)
  - Default: If the order keyword is not used, the ACLs have the lowest order by default (255).
- `fragments` Enter the keyword `fragments` to use ACLs to control packet fragments.

**Defaults**

Not configured

**Command Modes**

- **CONFIGURATION-IP ACCESS-LIST-STANDARD**

**Command History**

- **Version 8.3.16.1**
  - Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

- The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *FTOS Configuration Guide*. 

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list extended</code></td>
<td>Creates an extended ACL.</td>
</tr>
<tr>
<td><code>permit tcp</code></td>
<td>Assigns a permit filter for TCP packets.</td>
</tr>
<tr>
<td><code>permit udp</code></td>
<td>Assigns a permit filter for UDP packets.</td>
</tr>
</tbody>
</table>
permit tcp

Configure a filter to pass TCP packets meeting the filter criteria.

Syntax

```plaintext
permit tcp {source mask | any | host ip-address} {bit [operator port [port]]} {destination mask | any | host ip-address} {bit} [dscp] [operator port [port]] [count [byte]] [order] [fragments]
```

To remove this filter, you have two choices:
- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no permit tcp {source mask | any | host ip-address} {destination mask | any | host ip-address} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword host followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td>bit</td>
<td>Enter a flag or combination of bits:</td>
</tr>
<tr>
<td></td>
<td>• ack: acknowledgement field</td>
</tr>
<tr>
<td></td>
<td>• fin: finish (no more data from the user)</td>
</tr>
<tr>
<td></td>
<td>• psh: push function</td>
</tr>
<tr>
<td></td>
<td>• rst: reset the connection</td>
</tr>
<tr>
<td></td>
<td>• syn: synchronize sequence numbers</td>
</tr>
<tr>
<td></td>
<td>• urg: urgent field</td>
</tr>
<tr>
<td>dscp</td>
<td>Enter this keyword to deny a packet based on DSCP value. Range: 0-63</td>
</tr>
<tr>
<td>operator</td>
<td>(OPTIONAL) Enter one of the following logical operands:</td>
</tr>
<tr>
<td></td>
<td>• eq = equal to</td>
</tr>
<tr>
<td></td>
<td>• neq = not equal to</td>
</tr>
<tr>
<td></td>
<td>• gt = greater than</td>
</tr>
<tr>
<td></td>
<td>• lt = less than</td>
</tr>
<tr>
<td></td>
<td>• range = inclusive range of ports (you must specify two port for the port parameter.)</td>
</tr>
<tr>
<td>port port</td>
<td>Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535.</td>
</tr>
<tr>
<td></td>
<td>The following list includes some common TCP port numbers:</td>
</tr>
<tr>
<td></td>
<td>• 23 = Telnet</td>
</tr>
<tr>
<td></td>
<td>• 20 and 21 = FTP</td>
</tr>
<tr>
<td></td>
<td>• 25 = SMTP</td>
</tr>
<tr>
<td></td>
<td>• 169 = SNMP</td>
</tr>
<tr>
<td>destination</td>
<td>Enter the IP address of the network or host to which the packets are sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword count to count packets processed by the filter.</td>
</tr>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.</td>
</tr>
</tbody>
</table>
order (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry.
Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)
Default: If the order keyword is not used, the ACLs have the lowest order by default (255).

fragments Enter the keyword fragments to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-IP ACCESS-LIST-EXTENDED

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The order option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the FTOS Configuration Guide.

The MXL 10/40GbE System IO Module cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (gt, lt, range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port range 4000 - 8000 uses eight entries in the CAM:

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000111110100000</td>
<td>1111111111000000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111000000</td>
<td>1111111111000000</td>
<td>4032</td>
<td>4095</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000</td>
<td>1111100000000000</td>
<td>4096</td>
<td>6143</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000</td>
<td>1111110000000000</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000</td>
<td>1111110000000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111100000000</td>
<td>1111111100000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111110000000</td>
<td>1111111111000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111111000000</td>
<td>1111111111110000</td>
<td>8000</td>
<td>8000</td>
<td>1</td>
</tr>
</tbody>
</table>

Total Ports: 4001

But an ACL rule with TCP port lt 1023 takes only one entry in the CAM:

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000000000000000</td>
<td>1111110000000000</td>
<td>0</td>
<td>1023</td>
<td>1024</td>
</tr>
</tbody>
</table>

Total Ports: 1024

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list extended</td>
<td>Creates an extended ACL.</td>
</tr>
<tr>
<td>permit</td>
<td>Assigns a permit filter for IP packets.</td>
</tr>
<tr>
<td>permit udp</td>
<td>Assigns a permit filter for UDP packets.</td>
</tr>
</tbody>
</table>

Access Control Lists (ACL) | 123
permit udp

Configure a filter to pass UDP packets meeting the filter criteria.

Syntax

```
permit udp {source mask | any | host ip-address} [operator port [port]] {destination mask | any | host ip-address} [dscp] [operator port [port]] [count [byte]] [order] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit udp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>source</code></td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Enter the keyword <code>any</code> to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td><code>host ip-address</code></td>
<td>Enter the keyword <code>host</code> followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td><code>dscp</code></td>
<td>Enter this keyword to deny a packet based on DSCP value. Range: 0-63</td>
</tr>
</tbody>
</table>
| `operator`     | (OPTIONAL) Enter one of the following logical operand:
|                | • `eq` = equal to
|                | • `neq` = not equal to
|                | • `gt` = greater than
|                | • `lt` = less than
|                | • `range` = inclusive range of ports (you must specify two ports for the `port` parameter.) |
| `port port`    | (OPTIONAL) Enter the application layer port number. Enter two port numbers if using the `range` logical operand. Range: 0 to 65535 |
| `destination`  | Enter the IP address of the network or host to which the packets are sent.   |
| `count`        | (OPTIONAL) Enter the keyword `count` to count packets processed by the filter. |
| `byte`         | (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.   |
| `order`        | (OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority).
|                | Default: If the order keyword is not used, the ACLs have the lowest order by default (255). |
| `fragments`    | Enter the keyword `fragments` to use ACLs to control packet fragments.        |

### Defaults

Not configured.

### Command Modes

`CONFIGURATION-IP ACCESS-LIST-EXTENDED`

### Command History

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

### Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *FTOS Configuration Guide*.  

---

124 | Access Control Lists (ACL)
In the MXL Switch, you can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (gt, lt, range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port range 4000 - 8000 uses eight entries in the CAM:

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000111110100000 0000000000000000</td>
<td>1111111111000000 1111111111111111</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111000000 0000000000000000</td>
<td>1111110000000000 1111111111111111</td>
<td>4032</td>
<td>4095</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0001100000000000 0000000000000000</td>
<td>1111100000000000 1111100000000000</td>
<td>4096</td>
<td>6143</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0000110000000000 1111110000000000 1111110000000000 1111110000000000</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000 1111110000000000 1111110000000000 1111110000000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0001111100000000 1111111000000000 1111111000000000 1111111000000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000 1111111111000000 1111111111000000 1111111111000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0001111110100000 1111111111111111 1111111111111111 1111111111111111</td>
<td>8000</td>
<td>8000</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Total Ports: 4001

But an ACL rule with TCP port lt 1023 takes only one entry in the CAM:

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000000000000000 0000000000000000</td>
<td>1111111111000000 1111111111111111</td>
<td>0</td>
<td>1023</td>
<td>1024</td>
</tr>
</tbody>
</table>

Total Ports: 1024

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list extended</td>
<td>Configures an extended ACL.</td>
</tr>
<tr>
<td>permit</td>
<td>Assigns a permit filter for IP packets.</td>
</tr>
<tr>
<td>permit tcp</td>
<td>Assigns a permit filter for TCP packets.</td>
</tr>
</tbody>
</table>

**seq**

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

**Syntax**

```
seq sequence-number {deny | permit} {ip-protocol-number | icmp | ip | tcp | udp} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator port [port]] [count [byte]] [dscp value] [order] [fragments]
```

**Parameters**

- `sequence-number`: Enter a number from 0 to 4294967290.
  Range: 1 to 65534
- `deny`: Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
- `permit`: Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
- `ip-protocol-number`: Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
- `icmp`: Enter the keyword `icmp` to configure an ICMP access list filter.
### ip
Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list will permit all IP protocols.

### tcp
Enter the keyword `tcp` to configure a TCP access list filter.

### udp
Enter the keyword `udp` to configure a UDP access list filter.

### source
Enter the IP address of the network or host from which the packets were sent.

### mask
Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

### any
Enter the keyword `any` to specify that all routes are subject to the filter.

### host ip-address
Enter the keyword `host` followed by the IP address to specify a host IP address.

### operator
(OPTIONAL) Enter one of the following logical operands:
- `eq` = equal to
- `neq` = not equal to
- `gt` = greater than
- `lt` = less than
- `range` = inclusive range of ports (you must specify two ports for the `port` parameter)

### port port
(Optional) Enter the application layer port number. Enter two port numbers if using the `range` logical operand.
Range: 0 to 65535
The following list includes some common TCP port numbers:
- 23 = Telnet
- 20 and 21 = FTP
- 25 = SMTP
- 169 = SNMP

### destination
Enter the IP address of the network or host to which the packets are sent.

### message-type
(Optional) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 6-2).
Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code

### count
(Optional) Enter the keyword `count` to count packets processed by the filter.

### byte
(Optional) Enter the keyword `byte` to count bytes processed by the filter.

### dscp
(Optional) Enter the keyword `dscp` to match to the IP DSCP values.

### order
(Optional) Enter the keyword `order` to specify the QoS priority for the ACL entry.
Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)
Default: If the `order` keyword is not used, the ACLs have the lowest order by default (255).

### fragments
Enter the keyword `fragments` to use ACLs to control packet fragments.

### Defaults
Not configured

### Command Modes
CONFIGURATION-IP ACCESS-LIST-EXTENDED

### Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq sequence-number` is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via QoS policy framework.
- The `order` option takes precedence over the `seq sequence-number`.
- If `sequence-number` is not configured, then rules with the same order value are ordered according to their configuration order.
- If the `sequence-number` is configured, then the `sequence-number` is used as a tie breaker for rules with the same order.

If the `sequence-number` is configured, then the `sequence-number` is used as a tie breaker for rules with the same order.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
</tr>
<tr>
<td>permit</td>
</tr>
</tbody>
</table>

### Common MAC Access List Commands

The following commands are available within both MAC ACL modes (Standard and Extended) and do not have mode-specific options.

The MXL 10/40GbE Switch IO Module platform supports both ingress and egress MAC ACLs. The following commands allow you to clear, display and assign MAC ACL configurations.

- clear counters mac access-group
- mac access-group
- show mac access-lists
- show mac accounting access-list

### clear counters mac access-group

Clear counters for all or a specific MAC ACL.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>clear counters mac access-group [mac-list-name]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>mac-list-name (OPTIONAL) Enter the name of a configured MAC access list.</td>
</tr>
<tr>
<td>Command Modes</td>
<td>EXEC Privilege</td>
</tr>
<tr>
<td>Command History</td>
<td>Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>
mac access-group

Apply a MAC ACL to traffic entering or exiting an interface.

Syntax

```
mac access-group access-list-name {in [vlan vlan-range] | out}
```

Parameters

- **access-list-name**: Enter the name of a configured MAC access list, up to 140 characters.
- **vlan vlan-range** (OPTIONAL): Enter the keyword `vlan` followed by a range of VLANs. Note that this option is available only with the `in` keyword option.
  - Range: 1 to 4094, 1-2094 for ExaScale (can used IDs 1-4094)
- **in**: Enter the keyword `in` to configure the ACL to filter incoming traffic.
- **out**: Enter the keyword `out` to configure the ACL to filter outgoing traffic.

Defaults

```
none
```

Command Modes

```
INTERFACE
```

Command History

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```

Usage Information

You can assign one ACL (standard or extended) to an interface.

Related Commands

- `mac access-list standard`: Configures a standard MAC ACL.
- `mac access-list extended`: Configures an extended MAC ACL.

show mac access-lists

Displays all of the Layer 2 ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/mismatches against each ACL entry.

Syntax

```
show mac access-lists [access-list-name] [interface interface] [in | out]
```

Parameters

- **access-list-name**: Enter the name of a configured MAC ACL, up to 140 characters.
- **interface interface**: Enter the keyword `interface` followed by the one of the following keywords and slot/port or number information:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
- **in | out**: Identify whether ACL is applied on ingress or egress side.

Command Modes

```
EXEC Privilege
```

Command History

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```
show mac accounting access-list

Display MAC access list configurations and counters (if configured).

**Syntax**

```
show mac accounting access-list access-list-name interface interface in | out
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-name</td>
<td>Enter the name of a configured MAC ACL, up to 140 characters.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enter the keyword <code>interface</code> followed by one of the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>- For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>- For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
<tr>
<td>in</td>
<td>out</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC
EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#show mac accounting access-list mac-ext interface po 1
Extended mac access-list mac-ext on TenGigabitEthernet 0/11
    seq 5 permit host 00:00:00:00:00:11 host 00:00:00:00:00:19 count (393794576 packets)
    seq 10 deny host 00:00:00:00:00:21 host 00:00:00:00:00:29 count (89076777 packets)
    seq 15 deny host 00:00:00:00:00:31 host 00:00:00:00:00:39 count (0 packets)
    seq 20 deny host 00:00:00:00:00:41 host 00:00:00:00:00:49 count (0 packets)
    seq 25 permit any any count (0 packets)

Extended mac access-list mac-ext on TenGigabitEthernet 0/12
    seq 5 permit host 00:00:00:00:00:11 host 00:00:00:00:00:19 count (57589834 packets)
    seq 10 deny host 00:00:00:00:00:21 host 00:00:00:00:00:29 count (39314307 packets)
    seq 15 deny host 00:00:00:00:00:31 host 00:00:00:00:00:39 count (0 packets)
    seq 20 deny host 00:00:00:00:00:41 host 00:00:00:00:00:49 count (0 packets)
    seq 25 permit any any count (0 packets)
FTOS#
```

**Usage Information**

The ACL hit counters in this command increment the counters for each matching rule, not just the first matching rule.
Standard MAC ACL Commands

When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit.

The MXL 10/40GbE Switch IO Module platform supports both ingress and egress MAC ACLs.

The following commands configure standard MAC ACLs:

- `deny`
- `mac access-list standard`
- `permit`
- `seq`

Note: See also Commands Common to all ACL Types and Common MAC Access List Commands.

**deny**

Configure a filter to drop packets with a the MAC address specified.

**Syntax**

```
deny {any | mac-source-address [mac-source-address-mask]} [count [byte]]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no deny {any | mac-source-address mac-source-address-mask}` command.

**Parameters**

- **any**: Enter the keyword any to specify that all traffic is subject to the filter.
- **mac-source-address**: Enter a MAC address in nn:nn:nn:nn:nn:nn format.
- **mac-source-address-mask** (OPTIONAL): Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
- **count** (OPTIONAL): Enter the keyword count to count packets processed by the filter.
- **byte** (OPTIONAL): Enter the keyword byte to count bytes processed by the filter.

**Defaults**

Not enabled.

**Command Modes**

- **CONFIGURATION-MAC ACCESS LIST-STANDARD**

**Command History**

- **Version 8.3.16.1**: Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `permit`: Configures a MAC address filter to pass packets.
- `seq`: Configures a MAC address filter with a specified sequence number.
mac access-list standard

Name a new or existing MAC access control list (MAC ACL) and enter the MAC ACCESS LIST mode to configure a standard MAC ACL. See Commands Common to all ACL Types and Common MAC Access List Commands.

Syntax

mac access-list standard  \textit{mac-list-name}

Parameters

\textit{mac-list-name} \hspace{2cm} Enter a text string as the name of the standard MAC access list (140 character maximum).

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

FTOS supports one ingress and one egress MAC ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your switch documentation.

The MXL Switch supports both ingress and egress ACLs.

Example

\textbf{Figure 6-7. mac access-list standard Command Example}

```
FTOS(conf)#mac access-list standard TestMAC
FTOS(conf-std-macl)#?
deny                    Specify packets to reject
description             List description
exit                    Exit from access-list configuration mode
no                      Negate a command or set its defaults
permit                  Specify packets to forward
remark                  Specify access-list entry remark
seq                     Sequence numbers
show                    Show Standard ACL configuration
```

permit

Configure a filter to forward packets from a specific source MAC address.

Syntax

permit \{any | mac-source-address [mac-source-address-mask]\} [count [byte]]

To remove this filter, you have two choices:

- Use the no seq \textit{sequence-number} command if you know the filter’s sequence number.
- Use the no permit \{any | mac-source-address mac-source-address-mask\} command.

Parameters

\begin{tabular}{|l|l|}
\hline
\textbf{any} & Enter the keyword any to forward all packets received with a MAC address. \\
\hline
\textbf{mac-source-address} & Enter a MAC address in \texttt{nn:nn:nn:nn:nn:nn} format. \\
\hline
\textbf{mac-source-address-mask} & (OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match). \\
\hline
\end{tabular}
### seq

Assign a sequence number to a deny or permit filter in a MAC access list while creating the filter.

**Syntax**
```
seq sequence-number {deny | permit} {any | mac-source-address [mac-source-address-mask]} [count [byte]]
```

**Parameters**
- **sequence-number**: Enter a number between 0 and 65535.
- **deny**: Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
- **permit**: Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
- **any**: Enter the keyword `any` to filter all packets.
- **mac-source-address**: Enter a MAC address in nn:nn:nn:nn:nn:nn format.
- **mac-source-address-mask** (OPTIONAL): Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
- **count** (OPTIONAL): Enter the keyword `count` to count packets processed by the filter.
- **byte** (OPTIONAL): Enter the keyword `byte` to count bytes processed by the filter.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION-MAC ACCESS LIST-STANDARD

**Command History**
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**
- **deny**: Configures a MAC ACL filter to drop packets.
- **permit**: Configures a MAC ACL filter to forward packets.
Extended MAC ACL Commands

When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit.

The MXL 10/40GbE Switch IO Module platform supports ingress and egress MAC ACLs.

The following commands configure Extended MAC ACLs.

- **deny**
- **mac access-list extended**
- **permit**
- **seq**

*Note:* See also **Commands Common to all ACL Types** and **Common MAC Access List Commands**.

deny

Configure a filter to drop packets that match the filter criteria.

**Syntax**

deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype-operator] [count [byte]]

To remove this filter, you have two choices:

- Use the **no seq sequence-number** command if you know the filter’s sequence number.
- Use the **no deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask}** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Enter the keyword <strong>any</strong> to drop all packets.</td>
</tr>
<tr>
<td>host mac-address</td>
<td>Enter the keyword <strong>host</strong> followed by a MAC address to drop packets with that host address.</td>
</tr>
<tr>
<td>mac-source-address</td>
<td>Enter the source MAC address in nn:nn:nn:nn:nn:nn format.</td>
</tr>
<tr>
<td>mac-source-address-mask</td>
<td>Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.</td>
</tr>
<tr>
<td>mac-destination-address</td>
<td>Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.</td>
</tr>
<tr>
<td>mac-destination-address-mask</td>
<td>Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.</td>
</tr>
</tbody>
</table>
**mac access-list extended**

Name a new or existing extended MAC access control list (extended MAC ACL).

**Syntax**

mac access-list extended **access-list-name**

**Parameters**

- **access-list-name** Enter a text string as the MAC access list name, up to 140 characters.

**Defaults**

No default configuration

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your switch documentation.
**Example**

```
FTOS(conf)#mac access-list extended TestMATExt
FTOS(conf-ext-macl)#remark 5 IPv4
FTOS(conf-ext-macl)#seq 10 permit any any ev2 eq 800 count bytes
FTOS(conf-ext-macl)#seq 20 permit any any ev2 eq 806 count bytes
FTOS(conf-ext-macl)#remark 15 ARP
FTOS(conf-ext-macl)#seq 30 permit any any ev2 eq 86dd count bytes
FTOS(conf-ext-macl)#seq 40 permit any any count bytes
FTOS(conf-ext-macl)#exit
FTOS(conf)#do show mac accounting access-list snickers interface tengig0/47 in
Extended mac access-list snickers on TenGigabitEthernet 0/47
 seq 10  permit any any ev2 eq 800  count bytes (559851886 packets 191402152148 bytes)
 seq 20  permit any any ev2 eq 806  count bytes (74481486 packets 5031686754 bytes)
 seq 30  permit any any ev2 eq 86dd  count bytes (7751519 packets 797843521 bytes)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac access-list standard</code></td>
<td>Configures a standard MAC access list.</td>
</tr>
<tr>
<td><code>show mac accounting access-list</code></td>
<td>Displays MAC access list configurations and counters (if configured).</td>
</tr>
</tbody>
</table>

**permit**

Configure a filter to pass packets matching the criteria specified.

**Syntax**

```
permit {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype operator] [count [byte]]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit {any | host mac-address | mac-source-address mac-source-address-mask} {any | mac-destination-address mac-destination-address-mask}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>any</code></td>
<td>Enter the keyword <code>any</code> to forward all packets.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Enter the keyword <code>host</code> followed by a MAC address to forward packets with that host address.</td>
</tr>
<tr>
<td><code>mac-source-address</code></td>
<td>Enter the source MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.</td>
</tr>
<tr>
<td><code>mac-source-address-mask</code></td>
<td>Specify which bits in the MAC address must be matched.</td>
</tr>
<tr>
<td></td>
<td>The MAC ACL supports an inverse mask, therefore, a mask of <code>ff:ff:ff:ff:ff</code> allows entries that do not match and a mask of <code>00:00:00:00:00:00</code> only allows entries that match exactly.</td>
</tr>
<tr>
<td><code>mac-destination-address</code></td>
<td>Enter the destination MAC address and mask in <code>nn:nn:nn:nn:nn:nn</code> format.</td>
</tr>
<tr>
<td><code>mac-destination-address-mask</code></td>
<td>Specify which bits in the MAC address must be matched.</td>
</tr>
<tr>
<td></td>
<td>The MAC ACL supports an inverse mask, therefore, a mask of <code>ff:ff:ff:ff:ff</code> allows entries that do not match and a mask of <code>00:00:00:00:00:00</code> only allows entries that match exactly.</td>
</tr>
</tbody>
</table>
**ethertype operator**

(Optional) To filter based on protocol type, enter one of the following Ethertypes:
- **ev2** - is the Ethernet II frame format.
- **llc** - is the IEEE 802.3 frame format.
- **snap** - is the IEEE 802.3 SNAP frame format.

**count**

(Optional) Enter the keyword `count` to count packets processed by the filter.

**byte**

(Optional) Enter the keyword `byte` to count bytes processed by the filter.

---

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION-MAC ACCESS LIST-EXTENDED

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `deny` - Configures a filter to drop traffic based on the MAC address.
- `seq` - Configures a filter with specific sequence numbers.

---

**seq**

Configure a filter with a specific sequence number.

**Syntax**

```
seq sequence-number {deny | permit} {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype operator] [count [byte]]
```

**Parameters**

- `sequence-number` Enter a number as the filter sequence number. Range: zero (0) to 65535.
- `deny` Enter the keyword `deny` to drop any traffic matching this filter.
- `permit` Enter the keyword `permit` to forward any traffic matching this filter.
- `any` Enter the keyword `any` to filter all packets.
- `host mac-address` Enter the keyword `host` followed by a MAC address to filter packets with that host address.
- `mac-source-address` Enter the source MAC address in nn:nn:nn:nn:nn:nn format. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
- `mac-source-address-mask` Specify which bits in the MAC address must be matched.
- `mac-destination-address` Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
- `mac-destination-address-mask` Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit.

Use these commands to configure or enable IP prefix lists.

- clear ip prefix-list
- deny
- ip prefix-list
- permit
- seq
- show config
- show ip prefix-list detail
- show ip prefix-list summary

**clear ip prefix-list**

Reset the number of times traffic met the conditions (“hit” counters) of the configured prefix lists.

**Syntax**

clear ip prefix-list [prefix-name]

**Parameters**

prefix-name (OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.

**Command Modes**

EXEC Privilege
deny

Configure a filter to drop packets meeting the criteria specified.

Syntax
deny ip-prefix [ge min-prefix-length] [le max-prefix-length]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-prefix</td>
<td>Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.</td>
</tr>
<tr>
<td>ge min-prefix-length</td>
<td>(OPTIONAL) Enter the keyword ge followed by the minimum prefix length, which is a number from zero (0) to 32.</td>
</tr>
<tr>
<td>le max-prefix-length</td>
<td>(OPTIONAL) Enter the keyword le followed by the maximum prefix length, which is a number from zero (0) to 32.</td>
</tr>
</tbody>
</table>

Defaults
Not configured.

Command Modes
PREFIX-LIST

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the options ge or le, only packets with an exact match to the prefix are filtered.

Related Commands
permit Configure a filter to pass packets.
seq Configures a drop or permit filter with a specified sequence number.

ip prefix-list

Enter PREFIX-LIST mode and configure a prefix list.

Syntax
ip prefix-list prefix-name

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-name</td>
<td>Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.</td>
</tr>
</tbody>
</table>

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### Usage Information
Prefix lists redistribute OSPF and RIP routes meeting specific criteria. For related RIP commands, refer to Chapter 40, Routing Information Protocol (RIP). For related OSPF commands supported, refer to *FTOS Command Line Reference Guide* Chapter 34, Open Shortest Path First (OSPF).

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip route list</code></td>
<td>Displays IP routes in an IP prefix list.</td>
</tr>
<tr>
<td><code>show ip prefix-list summary</code></td>
<td>Displays a summary of the configured prefix lists.</td>
</tr>
</tbody>
</table>

### permit
Configure a filter that passes packets meeting the criteria specified.

#### Syntax
`permit ip-prefix [ge min-prefix-length] [le max-prefix-length]`

#### Parameters
- `ip-prefix` Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
- `ge min-prefix-length` (OPTIONAL) Enter the keyword `ge` followed by the minimum prefix length, which is a number from zero (0) to 32.
- `le max-prefix-length` (OPTIONAL) Enter the keyword `le` followed by the maximum prefix length, which is a number from zero (0) to 32.

#### Command Modes
PREFIX-LIST

#### Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

#### Usage Information
Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the options `ge` or `le`, only packets with an exact match to the prefix are filtered.

#### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>deny</code></td>
<td>Configures a filter to drop packets.</td>
</tr>
<tr>
<td><code>seq</code></td>
<td>Configures a drop or permit filter with a specified sequence number.</td>
</tr>
</tbody>
</table>

### seq
Assign a sequence number to a deny or permit filter in a prefix list while configuring the filter.

#### Syntax
`seq sequence-number {deny | permit} {any} | [ip-prefix /nn {ge min-prefix-length} {le max-prefix-length}] | [bitmask number]`

#### Parameters
- `sequence-number` Enter a number. Range: 1 to 4294967294.
- `deny` Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
- `permit` Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
- `any` (OPTIONAL) Enter the keyword `any` to match any packets.
- `ip-prefix /nn` (OPTIONAL) Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
Defaults
Not configured.

Command Modes
PREFIX-LIST

Command History

Usage Information
If you do not use the options ge or le, only packets with an exact match to the prefix are filtered.

Related Commands
deny Configures a filter to drop packets.
permit Configures a filter to pass packets.

show config
Display the current PREFIX-LIST configurations.

Syntax
show config

Command Modes
PREFIX-LIST

Example
Figure 6-9. show config Command Example
FTOS(conf-nprefixl)#show config
!
ip prefix-list snickers
FTOS(conf-nprefixl)#

show ip prefix-list detail
Display details of the configured prefix lists.

Syntax
show ip prefix-list detail [prefix-name]

Parameters
prefix-name (OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes
EXEC
EXEC Privilege
**show ip prefix-list summary**

Display a summary of the configured prefix lists.

**Syntax**

`show ip prefix-list summary [prefix-name]`

**Parameters**

`prefix-name` *(OPTIONAL)* Enter a text string as the name of the prefix list, up to 140 characters long.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 6-11. show ip prefix-list summary Command Example**

```
FTOS#show ip prefix-list summary
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
count: 3, range entries: 1, sequences: 5 - 15
ip prefix-list test1:
count: 2, range entries: 2, sequences: 5 - 10
ip prefix-list test2:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test3:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test4:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test5:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test6:
count: 1, range entries: 1, sequences: 5 - 5
FTOS#
```
Route Map Commands

When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit.

The following commands allow you to configure route maps and their redistribution criteria.

- continue
- description
- match interface
- match ip address
- match ip next-hop
- match ip route-source
- match metric
- match route-type
- match tag
- route-map
- set automatic-tag
- set metric
- set metric-type
- set tag
- show config
- show route-map

continue

Configure a route-map to go to a route-map entry with a higher sequence number.

Syntax

```
continue [sequence-number]
```

Parameters

- **sequence-number**
  
  (OPTIONAL) Enter the route map sequence number.
  
  Range: 1 - 65535
  
  Default: no sequence number

Defaults

Not Configured

Command Modes

ROUTE-MAP

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The `continue` feature allows movement from one route-map entry to a specific route-map entry (the `sequence number`). If you do not specify the sequence number, the `continue` feature simply moves to the next sequence number (also known as an implied continue). If a match clause exists, the `continue` feature executes only after a successful match occurs. If there are no successful matches, `continue` is ignored.
Match clause with Continue clause

The continue feature can exist without a match clause. A continue clause without a match clause executes and jumps to the specified route-map entry.

With a match clause and a continue clause, the match clause executes first and the continue clause next in a specified route map entry. The continue clause launches only after a successful match. The behavior is:

- A successful match with a continue clause, the route map executes the set clauses and then goes to the specified route map entry upon execution of the continue clause.
- If the next route map entry contains a continue clause, the route map executes the continue clause if a successful match occurs.
- If the next route map entry does not contain a continue clause, the route map evaluates normally. If a match does not occur, the route map does not continue and falls through to the next sequence number, if one exists.

Set clause with continue clause

If the route-map entry contains sets with the continue clause, set actions are performed first followed by the continue clause jump to the specified route map entry.

- If a set action occurs in the first route map entry and the same set action occurs with a different value in a subsequent route map entry, the last set of actions overrides the previous set of actions with the same set command.
- If you configure the set community additive and set as-path prepend options, the communities and AS numbers are prepended.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set metric</td>
<td>Specifies a COMMUNITY attribute</td>
</tr>
<tr>
<td>set automatic-tag</td>
<td>Configures a filter to modify the AS path</td>
</tr>
</tbody>
</table>

### description

Add a description to this route map.

**Syntax**

description {description}

**Parameters**

- **description**
  - Enter a description to identify the route map (80 characters maximum).

**Defaults**

- none

**Command Modes**

- ROUTE-MAP

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Enables a route map.</td>
</tr>
</tbody>
</table>
match interface

Configure a filter to match routes whose next hop is on the interface specified.

Syntax

match interface interface

To remove a match, use the no match interface interface command.

Parameters

- **interface**: Enter the following keywords and slot/port or number information:
  - For the loopback interface, enter the keyword loopback followed by a number from zero (0) to 16383.
  - For a Port Channel interface, enter the keyword port-channel followed by a number: Range: 1-128
  - For a Ten Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

Defaults

Not configured

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- match ip address
- match ip next-hop
- match ip route-source
- match metric
- match route-type
- match tag

match ip address

Configure a filter to match routes based on IP addresses specified in an access list.

Syntax

match ip address prefix-list-name

Parameters

- **prefix-list-name**: Enter the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- match interface
- match ip next-hop
- match ip route-source
match ip next-hop

Configure a filter to match routes based on the next-hop IP addresses specified in an IP access list or IP prefix list.

**Syntax**

```
match ip next-hop {access-list | prefix-list prefix-list-name}
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-name</code></td>
<td>Enter the name of a configured IP access list, up to 140 characters.</td>
</tr>
<tr>
<td><code>prefix-list prefix-list-name</code></td>
<td>Enter the keywords <code>prefix-list</code> followed by the name of configured prefix list.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `match interface` Redistributes routes that match the next-hop interface.
- `match ip address` Redistributes routes that match an IP address.
- `match ip route-source` Redistributes routes that match routes advertised by other routers.
- `match metric` Redistributes routes that match a specific metric.
- `match route-type` Redistributes routes that match a route type.
- `match tag` Redistributes routes that match a specific tag.

match ip route-source

Configure a filter to match routes based on the routes advertised by routers specified in IP access lists or IP prefix lists.

**Syntax**

```
match ip route-source {access-list | prefix-list prefix-list-name}
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-name</code></td>
<td>Enter the name of a configured IP access list, up to 140 characters.</td>
</tr>
<tr>
<td><code>prefix-list prefix-list-name</code></td>
<td>Enter the keywords <code>prefix-list</code> followed by the name of configured prefix list, up to 140 characters.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module
## match metric

Configure a filter to match on a specified value.

### Syntax

```
match metric metric-value
```

### Parameters

- `metric-value` Enter a value to match.
  
  Range: zero (0) to 4294967295.

### Defaults

Not configured.

### Command Modes

ROUTE-MAP

### Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### Related Commands

- `match interface` Redistributes routes that match the next-hop interface.
- `match ip address` Redistributes routes that match an IP address.
- `match ip next-hop` Redistributes routes that match the next-hop IP address.
- `match metric` Redistributes routes that match a specific metric.
- `match route-type` Redistributes routes that match a route type.
- `match tag` Redistributes routes that match a specific tag.

## match route-type

Configure a filter to match routes based on the how the route is defined.

### Syntax

```
match route-type {external [type-1 | type-2] | internal | local}
```

### Parameters

- `external [type-1 | type-2]` Enter the keyword `external` followed by either `type-1` or `type-2` to match only on OSPF Type 1 routes or OSPF Type 2 routes.
- `internal` Enter the keyword `internal` to match only on routes generated within OSPF areas.
- `local` Enter the keyword `local` to match only on routes generated within the switch.

### Defaults

Not configured.

### Command Modes

ROUTE-MAP
**match tag**

Configure a filter to redistribute only routes that match a specified tag value.

**Syntax**

```
match tag tag-value
```

**Parameters**

- **tag-value**
  - Enter a value as the tag on which to match.
  - Range: zero (0) to 4294967295.

**Defaults**

Not configured

**Command Modes**

ROUTE-MAP

**Related Commands**

- **match interface** Redistributes routes that match the next-hop interface.
- **match ip address** Redistributes routes that match an IP address.
- **match ip next-hop** Redistributes routes that match the next-hop IP address.
- **match ip route-source** Redistributes routes that match routes advertised by other routers.
- **match metric** Redistributes routes that match a specific metric.
- **match route-type** Redistributes routes that match a route type.

**route-map**

Enable a route map statement and configure its action and sequence number. This command also places you in ROUTE-MAP mode.

**Syntax**

```
route-map map-name [permit | deny] [sequence-number]
```

**Parameters**

- **map-name**
  - Enter a text string of up to 140 characters to name the route map for easy identification.
- **permit**
  - (OPTIONAL) Enter the keyword permit to set the route map default as permit.
  - If no keyword is specified, the default is permit.
deny

(INTERNATIONAL) Enter the keyword deny to set the route map default as deny.

sequence-number

(INTERNATIONAL) Enter a number to identify the route map for editing and sequencing with other route maps. You are prompted for a sequence number if there are multiple instances of the route map.

Range: 1 to 65535.

Defaults

Not configured

If no keyword (permit or deny) is defined for the route map, the permit action is the default.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 6-12. route-map Command Example

FTOS(conf)#route-map dempsey
FTOS(conf-route-map)#

Usage Information

Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same map-name are deleted when you use no route-map map-name command.

Related Commands

show config Displays the current configuration.

set automatic-tag

Configure a filter to automatically compute the tag value of the route.

Syntax

set automatic-tag

To return to the default, enter no set automatic-tag.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

set metric Specifies the metric value assigned to redistributed routes.

set metric-type Specifies the metric type assigned to redistributed routes.

set tag Specifies the tag assigned to redistributed routes.
set metric

Configure a filter to assign a new metric to redistributed routes.

Syntax

```
set metric [+] [-] metric-value
```

Parameters

+ (OPTIONAL) Enter + to add a metric-value to the redistributed routes.
- (OPTIONAL) Enter - to subtract a metric-value from the redistributed routes.

**metric-value**
Enter a number as the new metric value.
Range: zero (0) to 4294967295

Defaults

Not configured

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set automatic-tag</td>
<td>Computes the tag value of the route.</td>
</tr>
<tr>
<td>set metric-type</td>
<td>Specifies the route type assigned to redistributed routes.</td>
</tr>
<tr>
<td>set tag</td>
<td>Specifies the tag assigned to redistributed routes.</td>
</tr>
</tbody>
</table>

set metric-type

Configure a filter to assign a new route type for routes redistributed to OSPF.

Syntax

```
set metric-type {internal | external | type-1 | type-2}
```

Parameters

**internal** Enter the keyword internal to assign the Interior Gateway Protocol metric of the next hop as the route’s BGP MULTI_EXIT DES (MED) value.

**external** Enter the keyword external to assign the IS-IS external metric.

**type-1** Enter the keyword type-1 to assign the OSPF Type 1 metric.

**type-2** Enter the keyword type-2 to assign the OSPF Type 2 metric.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set automatic-tag</td>
<td>Computes the tag value of the route.</td>
</tr>
<tr>
<td>set metric</td>
<td>Specifies the metric value assigned to redistributed routes.</td>
</tr>
<tr>
<td>set tag</td>
<td>Specifies the tag assigned to redistributed routes.</td>
</tr>
</tbody>
</table>
set tag

Configure a filter to specify a tag for redistributed routes.

Syntax

set tag tag-value

Parameters

tag-value

Enter a number as the tag.

Range: zero (0) to 4294967295.

Defaults

Not configured

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- set automatic-tag
  Computes the tag value of the route.

- set metric
  Specifies the metric value assigned to redistributed routes.

- set metric-type
  Specifies the route type assigned to redistributed routes.

show config

Display the current route map configuration.

Syntax

show config

Command Modes

ROUTE-MAP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 6-13. show config Command Example

```
FTOS(conf-route-map)#show config
!
route-map hopper permit 10
FTOS(conf-route-map)#
```
### Example

**Figure 6-14. show route-map Command Example**

```
FTOS#show route-map
route-map firpo, permit, sequence 10
  Match clauses:
  Set clauses:
    tag  34
FTOS#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Configures a route map.</td>
</tr>
</tbody>
</table>
Bidirectional Forwarding Detection (BFD)

Overview

Bidirectional Forwarding Detection (BFD) is a detection protocol that provides fast forwarding path failure detection. The FTOS implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03 and supports BFD on all Layer 3 physical interfaces including VLAN interfaces and port-channels.

Commands

- bfd all-neighbors
- bfd disable
- bfd enable (Configuration)
- bfd enable (Interface)
- bfd interval
- bfd neighbor
- bfd protocol-liveness
- ip route bfd
- ipv6 ospf bfd all-neighbors
- isis bfd all-neighbors
- neighbor bfd
- neighbor bfd disable
- show bfd neighbors
- vrrp bfd neighbor

**bfd all-neighbors**

Enable BFD sessions with all neighbors discovered by Layer 3 protocols IS-IS, OSPF, or BGP on router interfaces, and (optionally) reconfigure the default timer values.

**Syntax**

```
[vrrp] bfd all-neighbors [interval interval min_rx min_rx multiplier value role [active | passive]]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp</td>
<td>Enter the keyword vrrp in INTERFACE mode to enable BFD for VRRP.</td>
</tr>
<tr>
<td>interval</td>
<td>(OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval.</td>
</tr>
<tr>
<td>milliseconds</td>
<td>Range: 50 to 1000</td>
</tr>
<tr>
<td></td>
<td>Default: 100</td>
</tr>
</tbody>
</table>
**min_rx milliseconds**

Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system.

- **Range:** 50 to 100
- **Default:** 100

**multiplier value**

Enter this keyword to specify the number of packets that must be missed in order to declare a session down.

- **Range:** 3 to 50
- **Default:** 3

**role [active | passive]**

Enter the role that the local system assumes:

- **Active**—The active system initiates the BFD session. Both systems can be active for the same session.
- **Passive**—The passive system does not initiate a session. It only responds to a request for session initialization from the active system.

- **Default:** Active

---

**Defaults**

See Parameters

**Command Modes**

- ROUTER OSPF
- ROUTER OSPFv3
- ROUTER BGP
- ROUTER ISIS
- INTERFACE (BFD for VRRP only)

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information

All neighbors inherit the timer values configured with the bfd all-neighbors command except in the following cases:

- Timer values configured with the isis bfd all-neighbors command in INTERFACE mode override timer values configured with the bfd all-neighbors command. Likewise, using the no bfd all-neighbors command does not disable BFD on an interface if BFD is explicitly enabled using the command isis bfd all-neighbors.

- Neighbors that have been explicitly enabled or disabled for a BFD session with the bfd neighbor or neighbor bfd disable commands in ROUTER BGP mode do not inherit the global BFD enable/disable values configured with the bfd all-neighbors command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values (configured with the bfd all-neighbors command).

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show bfd neighbors</td>
<td>Display BFD neighbor information on all interfaces or a specified interface.</td>
</tr>
<tr>
<td>bfd neighbor</td>
<td>Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.</td>
</tr>
<tr>
<td>neighbor bfd disable</td>
<td>Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.</td>
</tr>
</tbody>
</table>

**bfd disable**

Disable BFD on an interface.

**Syntax**

`bfd disable`

Re-enable BFD using the command `no bfd disable`.

**Defaults**

BFD is disabled by default.

**Command Modes**

INTERFACE VRRP

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**bfd enable (Configuration)**

Enable BFD on all interfaces.

**Syntax**

`bfd enable`

Disable BFD using the `no bfd enable` command.

**Defaults**

BFD is disabled by default.

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**bfd enable (Interface)**

Enable BFD on an interface.

**Syntax**

`bfd enable`

**Defaults**

BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**bfd interval**

Specify non-default BFD session parameters beginning with the transmission interval.

**Syntax**

`bfd interval interval min_rx min_rx multiplier value role {active | passive}`

**Parameters**

- `interval milliseconds` Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval.
  Range: 50 to 1000
  Default: 100
- `min_rx milliseconds` Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system.
  Range: 50 to 100
  Default: 100
- `multiplier value` Enter this keyword to specify the number of packets that must be missed in order to declare a session down.
  Range: 3 to 50
  Default: 3
- `role [active | passive]` Enter the role that the local system assumes:
  - Active—The active system initiates the BFD session. Both systems can be active for the same session.
  - Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system.
  Default: Active

**Defaults**

See Parameters

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
FTOS(conf-if-gi-0/3)#bfd interval 250 min_rx 300 multiplier 4 role passive
FTOS(conf-if-gi-0/3)#
```
**bfd neighbor**

Establish a BFD session with a neighbor.

**Syntax**

```
bfd neighbor ip-address
```

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format (A.B.C.D).

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `show bfd neighbors` Display BFD neighbor information on all interfaces or a specified interface.

**bfd protocol-liveness**

Enable the BFD protocol liveness feature.

**Syntax**

```
bfd protocol-liveness
```

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Protocol Liveness is a feature that notifies the BFD Manager when a client protocol (e.g. OSPF, ISIS) is disabled. When a client is disabled, all BFD sessions for that protocol are torn down. Neighbors on the remote system receive an Admin Down control packet and are placed in the Down state. Peer routers might take corrective action by choosing alternative paths for the routes that originally pointed to this router.
ip route bfd

Enable BFD for all neighbors configured through static routes.

Syntax

ip route bfd [interval interval min_rx min_rx multiplier value role {active | passive}]

To disable BFD for all neighbors configured through static routes, use the no ip route bfd [interval interval min_rx min_rx multiplier value role {active | passive}] command.

Parameters

Parameter | Description |
--- | --- |
interval milliseconds | (OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range: 50 to 1000 Default: 100 |
interval milliseconds | (OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range: 50 to 1000 Default: 100 |
multiplier value | Enter this keyword to specify the number of packets that must be missed in order to declare a session down. Range: 3 to 50 Default: 3 |
role [active | passive] | Enter the role that the local system assumes:  
- Active—The active system initiates the BFD session. Both systems can be active for the same session.  
- Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system. Default: Active |

Defaults

See Parameters

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show bfd neighbors | Display BFD neighbor information on all interfaces or a specified interface.
ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

**Syntax**

```plaintext
ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]
```

To disable all BFD sessions on an OSPFv3 interface, use the `no ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]` command in interface mode.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>disable</strong></td>
<td>(OPTIONAL) Enter the keyword disable to disable BFD on this interface.</td>
</tr>
<tr>
<td><strong>interval milliseconds</strong></td>
<td>(OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range: 50 to 1000 Default: 100</td>
</tr>
<tr>
<td><strong>min_rx milliseconds</strong></td>
<td>Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system. Range: 50 to 100 Default: 100</td>
</tr>
<tr>
<td><strong>multiplier value</strong></td>
<td>Enter this keyword to specify the number of packets that must be missed in order to declare a session down. Range: 3 to 50 Default: 3</td>
</tr>
</tbody>
</table>
| **role [active | passive]** | Enter the role that the local system assumes:  
• Active—The active system initiates the BFD session. Both systems can be active for the same session.  
• Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system. Default: Active |

**Defaults**

See Parameters

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
isis bfd all-neighbors

Enable BFD on all IS-IS neighbors discovered on an interface.

Syntax

isis bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]

To remove all BFD sessions with IS-IS neighbors discovered on this interface, use the no isis bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]] command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>(OPTIONAL) Enter the keyword disable to disable BFD on this interface.</td>
</tr>
<tr>
<td>interval</td>
<td>(OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range: 50 to 1000 Default: 100</td>
</tr>
<tr>
<td>min_rx</td>
<td>Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system. Range: 50 to 100 Default: 100</td>
</tr>
<tr>
<td>multiplier</td>
<td>Enter this keyword to specify the number of packets that must be missed in order to declare a session down. Range: 3 to 50 Default: 3</td>
</tr>
<tr>
<td>role</td>
<td>Enter the role that the local system assumes:</td>
</tr>
<tr>
<td></td>
<td>• Active—The active system initiates the BFD session. Both systems can be active for the same session.</td>
</tr>
<tr>
<td></td>
<td>• Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system. Default: Active</td>
</tr>
</tbody>
</table>

Defaults

See Parameters

Command Modes

INTERFACE

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command provides the flexibility to fine tune the timer values based on individual interface needs when ISIS BFD is configured in CONFIGURATION mode. Any timer values specified with this command override timers set using the command bfd all-neighbors. Using the no form of this command will not disable BFD if BFD is configured in CONFIGURATION mode.

Use the keyword disable to disable BFD on a specific interface while BFD is configured in from CONFIGURATION mode.
neighbor bfd

Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.

Syntax
neighbor {ip-address | peer-group-name} bfd

Parameters

- `ip-address` Enter the IP address of the BGP neighbor that you want to explicitly enable for BFD sessions in dotted decimal format (A.B.C.D).
- `peer-group-name` Enter the name of the peer group that you want to explicitly enable for BFD sessions.

Defaults
None

Command Modes
ROUTER BGP

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you enable a BFD session with a specified BGP neighbor or peer group using the `bfd neighbor` command, the default BFD session parameters are used (interval: 100 milliseconds, min_rx: 100 milliseconds, multiplier: 3 packets, and role: active) if no parameters have been specified with the `bfd all-neighbors` command.

When you explicitly enable a BGP neighbor for a BFD session with the `bfd neighbor` command:

- The neighbor does not inherit the global BFD enable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

Related Commands

- `bfd all-neighbors` Enable BFD sessions with all neighbors discovered by Layer 3 protocols.
- `neighbor bfd disable` Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.
- `show bfd neighbors` Display BFD neighbor information on all interfaces or a specified interface.

neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

Syntax
neighbor {ip-address | peer-group-name} bfd disable

Parameters

- `ip-address` Enter the IP address of the BGP neighbor that you want to explicitly disable for BFD sessions in dotted decimal format (A.B.C.D).
- `peer-group-name` Enter the name of the peer group that you want to explicitly disable for BFD sessions.

Defaults
None
Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>ROUTER BGP</th>
</tr>
</thead>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

When you explicitly disable a BGP neighbor for a BFD session with the `neighbor bfd disable` command:

- The neighbor does not inherit the global BFD disable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

When you remove the disabled state of a BFD for BGP session with a specified neighbor by entering the `no neighbor bfd disable` command, the BGP link with the neighbor returns to normal operation and uses the BFD session parameters globally configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd all-neighbors</td>
<td>Enable BFD sessions with all neighbors discovered by Layer 3 protocols.</td>
</tr>
<tr>
<td>bfd neighbor</td>
<td>Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.</td>
</tr>
<tr>
<td>show bfd neighbors</td>
<td>Display BFD neighbor information on all interfaces or a specified interface.</td>
</tr>
</tbody>
</table>

show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

Syntax

```
show bfd neighbors interface [detail]
```

Parameters

- `interface` (required) Enter one of the following keywords and slot/port or number information:
  - For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number. The range is from 0 to 5.
  - For VLAN interfaces, enter the keyword `vlan` followed by a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1-2730 (VLAN IDs can be 0-4093).

- `detail` (OPTIONAL) Enter the keyword `detail` to view detailed information about BFD neighbors.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Example

**Figure 7-2. show bfd neighbors Command**

```
Force10#show bfd neighbors
  * - Active session role
Ad Dn - Admin Down
B - BGP
C - CLI
I - ISIS
O - OSPF
R - Static Route (RTM)

<table>
<thead>
<tr>
<th>LocalAddr</th>
<th>RemoteAddr</th>
<th>Interface</th>
<th>State</th>
<th>Rx-int</th>
<th>Tx-int</th>
<th>Mult</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.3.2</td>
<td>10.1.3.1</td>
<td>Gi 1/3</td>
<td>Up</td>
<td>300</td>
<td>250</td>
<td>3</td>
<td>C</td>
</tr>
</tbody>
</table>
```

Example

**Figure 7-3. show bfd neighbors detail Command Example**

```
Force10#show bfd neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: GigabitEthernet 1/3
State: Up
Configured parameters:
  TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
  TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
  TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
  Number of packets received from neighbor: 376
  Number of packets sent to neighbor: 314
  Number of state changes: 2
  Number of messages from IFA about port state change: 0
  Number of messages communicated b/w Manager and Agent: 6

Force10#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd neighbor</td>
<td>Establish a BFD session with a neighbor.</td>
</tr>
<tr>
<td>bfd all-neighbors</td>
<td>Establish BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.</td>
</tr>
</tbody>
</table>

**vrrp bfd neighbor**

Establish a VRRP BFD session with a neighbor.

**Syntax**

```
vrrp bfd neighbor ip-address
```

**Parameters**

- `neighbor ip-address` Enter the IP address of the BFD neighbor.

**Defaults**

None.

**Command Modes**

INTERFACE

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
Border Gateway Protocol IPv4 (BGPv4)

Overview

For detailed information on configuring BGP, refer to the BGP chapter in the FTOS Configuration Guide.

This chapter contains the following sections:

- BGPv4 Commands
- MBGP Commands
- BGP Extended Communities (RFC 4360)

BGP IPv6 Commands are listed in the following sections:

- IPv6 BGP Commands
- IPv6 MBGP Commands

BGPv4 Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP version 4 (BGPv4) supports Classless InterDomain Routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

The following commands enable you to configure and enable BGP:

- address-family
- aggregate-address
- bgp add-path
- bgp always-compare-med
- bgp asnotation
- bgp bestpath as-path ignore
- bgp bestpath as-path confed
- bgp bestpath med confed
- bgp bestpath med missing-as-best

Note: FTOS Version 7.7.1 supports 2-Byte (16-bit) and 4-Byte (32-bit) format for Autonomous System Numbers (ASNs), where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295.

Note: FTOS Version 8.3.1.0 supports Dotted format as well as the Traditional Plain format for AS Numbers. The dot format is displayed when using the show ip bgp commands. To determine the comparable dot format for an ASN from a traditional format, use ASN/65536. ASN%65536.

For more information about using the 2 or 4-Byte format, refer to the FTOS Configuration Guide.
• bgp bestpath router-id ignore
• bgp client-to-client reflection
• bgp cluster-id
• bgp confederation identifier
• bgp confederation peers
• bgp dampening
• bgp default local-preference
• bgp enforce-first-as
• bgp fast-external-fallover
• bgp four-octet-as-support
• bgp graceful-restart
• bgp non-deterministic-med
• bgp recursive-bgp-next-hop
• bgp regex-eval-optz-disable
• bgp router-id
• bgp soft-reconfig-backup
• capture bgp-pdu neighbor
• capture bgp-pdu max-buffer-size
• clear ip bgp
• clear ip bgp dampening
• clear ip bgp flap-statistics
• debug ip bgp
• debug ip bgp dampening
• debug ip bgp events
• debug ip bgp keepalives
• debug ip bgp notifications
• debug ip bgp soft-reconfiguration
• debug ip bgp updates
• default-metric
• description
• max-paths
• neighbor activate
• neighbor add-path
• neighbor advertisement-interval
• neighbor advertisement-start
• neighbor allowas-in
• neighbor default-originate
• neighbor description
• neighbor distribute-list
• neighbor ebgp-multihop
• neighbor fall-over
• neighbor local-as
• neighbor maximum-prefix
• neighbor password
• neighbor peer-group (assigning peers)
• neighbor peer-group (creating group)
address-family

Enable the IPv4 multicast or the IPv6 address family.

**Syntax**

```
address-family [ipv4 multicast| ipv6unicast]
```
aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

aggregate-address ip-address mask [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address mask</td>
<td>Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).</td>
</tr>
<tr>
<td>advertise-map</td>
<td>(OPTIONAL) Enter the keywords advertise-map followed by the name of a configured route map to set filters for advertising an aggregate route.</td>
</tr>
<tr>
<td>map-name</td>
<td>(OPTIONAL) Enter the name of a configured route map to set filters for advertising an aggregate route.</td>
</tr>
<tr>
<td>as-set</td>
<td>(OPTIONAL) Enter the keyword as-set to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.</td>
</tr>
<tr>
<td>attribute-map</td>
<td>(OPTIONAL) Enter the keywords attribute-map followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.</td>
</tr>
<tr>
<td>map-name</td>
<td>(OPTIONAL) Enter the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.</td>
</tr>
<tr>
<td>summary-only</td>
<td>(OPTIONAL) Enter the keyword summary-only to advertise only the aggregate address. Specific routes will not be advertised.</td>
</tr>
<tr>
<td>suppress-map</td>
<td>(OPTIONAL) Enter the keywords suppress-map followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.</td>
</tr>
<tr>
<td>map-name</td>
<td>(OPTIONAL) Enter the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

ROUTER BGP ADDRESS FAMILY

ROUTER BGP ADDRESS FAMILY IPv6

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

If routes within the aggregate are constantly changing, do not add the as-set parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the suppress-map parameter, routes meeting the deny clause are not suppress; in other words, they are allowed. The opposite is also true: routes meeting the permit clause are suppressed.
If the route is injected via the network command, that route still appears in the routing table if the summary-only parameter is configured in the aggregate-address command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.

In the show ip bgp command, aggregates contain an ‘a’ in the first column and routes suppressed by the aggregate contain an ‘s’ in the first column.

### Command History

*Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.*

---

**bgp add-path**

Allow the advertisement of multiple paths for the same address prefix without the new paths replacing any previous ones.

**Syntax**

```
bgp add-path [send | receive | both] path-count
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>send</td>
<td>Enter this keyword to indicate that the system will send multiple paths to peers.</td>
</tr>
<tr>
<td>receive</td>
<td>Enter this keyword to indicate that the system will accept multiple paths from peers.</td>
</tr>
<tr>
<td>both</td>
<td>Enter this keyword to indicate that the system will send and accept multiple paths from peers.</td>
</tr>
<tr>
<td>path-count</td>
<td>Enter the number of paths supported. Range: 2-64</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled

**Command Modes**

- ROUTER BGP
- ROUTER BGP-address-family

**Related Commands**

- `neighbor add-path` Specify that this neighbor/peer group can send/receive multiple path advertisements.

**Command History**

*Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.*

---

**bgp always-compare-med**

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

**Syntax**

```
bgp always-compare-med
```

To disable comparison of MED, enter `no bgp always-compare-med`.

**Defaults**

Disabled (that is, the software only compares MEDs from neighbors within the same AS).

**Command Modes**

- ROUTER BGP
**Usage Information**

Any update without a MED attribute is the least preferred route.

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**bgp asnotation**

Enables you to implement a method for AS Number representation in the CLI.

**Syntax**

`bgp asnotation [asplain | asdot+ | asdot]`

To disable a dot or dot+ representation and return to ASPLAIN, enter the `no bgp asnotation` command.

**Defaults**

asplain

**Command Modes**

ROUTER BGP

**Usage Information**

Before enabling this feature, enable the `enable bgp four-octet-as-support` command. If you disable the four-octect-support command after using dot or dot+ format, the AS numbers revert to asplain text.

When you apply an asnotation, it is reflected in the running-configuration. If you change the notation type, the running-config updates dynamically and the new notation shows.

**Example**

```plaintext
FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#bgp asnotation asdot
FTOS(conf-router_bgp)#ex
FTOS(conf)#do show run | grep bgp

router bgp 1
bgp four-octet-as-support
bgp asnotation asdot

FTOS(conf-router_bgp)#bgp asnotation asdot+
FTOS(conf-router_bgp)#ex
FTOS(conf)#do show run | grep bgp

router bgp 1
bgp four-octet-as-support
bgp asnotation asdot+

FTOS(conf-router_bgp)#bgp asnotation asplain
FTOS(conf-router_bgp)#ex
FTOS(conf)#do show run | grep bgp

router bgp 1
bgp four-octet-as-support
bgp asnotation asplain

FTOS(conf)#
```

**Related Commands**

`bgp four-octet-as-support` — Enable 4-byte support for the BGP process
**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40Gbe Switch IO Module.

---

**bgp bestpath as-path ignore**

Ignore the AS PATH in BGP best path calculations.

**Syntax**

bgp bestpath as-path ignore

To return to the default, enter no bgp bestpath as-path ignore.

**Defaults**

Disabled (that is, the software considers the AS_PATH when choosing a route as best).

**Command Modes**

- ROUTER BGP

**Usage Information**

If you enable this command, use the clear ip bgp * command to recompute the best path.

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40Gbe Switch IO Module.

---

**bgp bestpath as-path multipath-relax**

Include prefixes received from different AS paths during multipath calculation.

**Syntax**

bgp bestpath as-path multipath-relax

To return to the default BGP routing process, use the no bgp bestpath as-path multipath-relax command.

**Defaults**

Disabled

**Command Modes**

- ROUTER BGP

**Usage Information**

The bestpath router bgp configuration mode command changes the default bestpath selection algorithm. The multipath-relax option allows load-sharing across providers with different (but equal-length) autonomous system paths. Without this option, ECMP expects the AS paths to be identical for load-sharing.

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40Gbe Switch IO Module.

---

**bgp bestpath med confed**

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

**Syntax**

bgp bestpath med confed

To disable MED comparison on BGP confederation paths, enter the no bgp bestpath med confed command.
Defaults: Disabled

Command Modes: ROUTER BGP

Usage Information: The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the `clear ip bgp *` command to recompute the best path.

Command History: Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**bgp bestpath med missing-as-best**

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

**Syntax**

```
bgp bestpath med missing-as-best
```

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults: Disabled

Command Modes: ROUTER BGP

Usage Information: The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.

Command History: Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**bgp bestpath router-id ignore**

Do not compare router-id information for external paths during best path selection.

**Syntax**

```
bgp bestpath router-id ignore
```

To return to the default selection, use the `no bgp bestpath router-id ignore` command.

Defaults: Disabled

Command Modes: ROUTER BGP

Usage Information: Configuring this option will retain the current best-path. When sessions are subsequently reset, the oldest received path will be chosen as the best-path.

Command History: Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**bgp client-to-client reflection**

Enables you to enable route reflection between clients in a cluster.

**Syntax**

```
bgp client-to-client reflection
```

To disable client-to-client reflection, enter `no bgp client-to-client reflection`.

**Defaults**

Enabled when a route reflector is configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Route reflection to clients is not necessary if all client routers are fully meshed.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp cluster-id</code></td>
<td>Assign ID to a BGP cluster with two or more route reflectors.</td>
</tr>
<tr>
<td><code>neighbor route-reflector-client</code></td>
<td>Configure a route reflector and clients.</td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**bgp cluster-id**

Assign a cluster ID to a BGP cluster with more than one route reflector.

**Syntax**

```
bgp cluster-id {ip-address | number}
```

To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

**Parameters**

- `ip-address` Enter an IP address as the route reflector cluster ID.
- `number` Enter a route reflector cluster ID as a number from 1 to 4294967295.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

When a BGP cluster contains only one route reflector, the cluster ID is the route reflector’s router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it will be displayed as an integer.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp client-to-client reflection</code></td>
<td>Enable route reflection between route reflector and clients.</td>
</tr>
<tr>
<td><code>neighbor route-reflector-client</code></td>
<td>Configure a route reflector and clients.</td>
</tr>
<tr>
<td><code>show ip bgp cluster-list</code></td>
<td>View paths with a cluster ID.</td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**bgp confederation identifier**

Configure an identifier for a BGP confederation.

**Syntax**

```
bgp confederation identifier as-number
```

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

**Parameters**

- `as-number` Enter the AS number.
  - Range: `0-65535` (2-Byte) or
  - `1-4294967295` (4-Byte) or
  - `0.1-65535.65535` (Dotted format)

**Defaults**

Not configured.

**Command Modes**

ROUTERS BGP

**Usage Information**

To accept 4-byte formats before entering a 4-byte AS number, configure your system. All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

FTOS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

**Related Commands**

- `bgp four-octet-as-support` — Enable 4-Byte support for the BGP process.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**bgp confederation peers**

Specify the Autonomous Systems (ASs) that belong to the BGP confederation.

**Syntax**

```
bgp confederation peers as-number [...as-number]
```

To return to the default, enter `no bgp confederation peers`.

**Parameters**

- `as-number` Enter the AS number.
  - Range: `0-65535` (2-Byte) or
  - `1-4294967295` (4-Byte) or
  - `0.1-65535.65535` (Dotted format)

- `...as-number` (OPTIONAL) Enter up to 16 confederation numbers.
  - Range: `0-65535` (2-Byte) or
  - `1-4294967295` (4-Byte) or
  - `0.1-65535.65535` (Dotted format)

**Defaults**

Not configured.
### Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>ROUTER BGP</th>
</tr>
</thead>
</table>

### Usage Information

All the routers in the Confederation must be 4 or 2 byte identified routers. You cannot mix them.

The Autonomous Systems configured in this command are visible to the EBGP neighbors. Each Autonomous System is fully meshed and contains a few connections to other Autonomous Systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp confederation identifier</td>
<td>Configure a confederation ID.</td>
</tr>
<tr>
<td>bgp four-octet-as-support</td>
<td>Enable 4-byte support for the BGP process.</td>
</tr>
</tbody>
</table>

### Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

### bgp dampening

Enable BGP route dampening and configure the dampening parameters.

**Syntax**

```
bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]
```

To disable route dampening, use the no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name] command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>half-life (OPTIONAL)</td>
<td>Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. Range: 1 to 45. Default: 15 minutes</td>
</tr>
<tr>
<td>reuse (OPTIONAL)</td>
<td>Enter a number as the reuse value, which is compared to the flapping route’s Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). Range: 1 to 20000. Default: 750</td>
</tr>
<tr>
<td>suppress (OPTIONAL)</td>
<td>Enter a number as the suppress value, which is compared to the flapping route’s Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). Range: 1 to 20000. Default: 750</td>
</tr>
<tr>
<td>max-suppress-time (OPTIONAL)</td>
<td>Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. Range: 1 to 255. Default: 60 minutes.</td>
</tr>
<tr>
<td>route-map map-name (OPTIONAL)</td>
<td>Enter the keyword route-map followed by the name of a configured route map. Only match commands in the configured route map are supported.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled.
### bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

**Syntax**
```
bgp default local-preference value
```

**Parameters**
- **value**
  - Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred.
  - Range: 0 to 4294967295
  - Default: 100

**Defaults**
100

**Command Modes**
- ROUTER BGP

**Usage Information**
The `bgp default local-preference` command setting is applied by all routers within the AS. To set the local preference for a specific route, use the `set metric` command in the ROUTE-MAP mode.

**Related Commands**
- `show ip bgp dampened-paths` View the BGP paths
- `set metric` Assign a local preference value for a specific route.

**Command History**
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

**Syntax**
```
bgp enforce-first-as
```

**Defaults**
Enabled

**Command Modes**
- ROUTER BGP

**Usage Information**
- To turn off the default, use the `no bgp enforce-first-as` command.
This command is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. Use the `show ip bgp neighbors` command to view the “failed enforce-first-as check” counter.

If you disable the `enforce-first-as` command, it can be viewed using the `show ip protocols` command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip bgp neighbors</code></td>
<td>View the information exchanged by BGP neighbors</td>
</tr>
<tr>
<td><code>show ip protocols</code></td>
<td>View Information on routing protocols</td>
</tr>
</tbody>
</table>

### Command History

```
Version 9.2(0.0)  Introduced on the MXL 10/40GbE Switch IO Module.
```

## bgp fast-external-fallover

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

### Syntax

```
bgp fast-external-fallover
```

To disable fast external fallover, enter `no bgp fast-external-fallover`.

### Defaults

Enabled.

### Command Modes

ROUTER BGP

### Usage Information

The `bgp fast-external-fallover` command appears in the `show config` command output.

### Command History

```
Version 9.2(0.0)  Introduced on the MXL 10/40GbE Switch IO Module.
```

## bgp four-octet-as-support

Enable 4-byte support for the BGP process.

### Syntax

```
bgp four-octet-as-support
```

To disable fast external fallover, enter the `no bgp four-octet-as-support` command.

### Defaults

Disabled (supports 2-Byte format)

### Command Modes

ROUTER BGP

### Usage Information

Routers supporting 4-Byte ASNs advertise that function in the OPEN message. The behavior of a 4-Byte router will be slightly different depending on whether it is speaking to a 2-Byte router or a 4-Byte router.

When creating Confederations, all the routers in the Confederation must be 4 or 2 byte identified routers. You cannot mix them.
Where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295. Both formats are accepted, and the advertisements will reflect the entered format.

For more information about using the 2 or 4-Byte format, refer to the FTOS Configuration Guide.

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

bgp graceful-restart
Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

Syntax
bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]

Parameters
- **restart-time seconds**: Enter the keyword restart-time followed by the maximum number of seconds needed to restart and bring-up all the peers.
  - Range: 1 to 3600 seconds
  - Default: 120 seconds

- **stale-path-time seconds**: Enter the keyword stale-path-time followed by the maximum number of seconds to wait before restarting a peer’s stale paths.
  - Default: 360 seconds.

- **role receiver-only**: Enter the keyword role receiver-only to designate the local router to support graceful restart as a receiver only.

Defaults
as above

Command Modes
ROUTER-BGP

Usage Information
This feature is advertised to BGP neighbors through a capability advertisement. In receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

bgp non-deterministic-med
Compare MEDs of paths from different Autonomous Systems.

Syntax
bgp non-deterministic-med

Defaults
Disabled (that is, paths/routes for the same destination but from different ASs will not have their MEDs compared).

To return to the default, enter the no bgp non-deterministic-med command.
In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to FTOS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors since MED may or may not get compared between adjacent paths. In deterministic mode (no bgp non-deterministic-med), FTOS compares MED between adjacent paths within an AS group since all paths in the AS group are from the same AS.

When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter the clear ip bgp command to clear existing paths.

**bgp recursive-bgp-next-hop**

Enable next-hop resolution through other routes learned by BGP.

**Syntax**

```
bgp recursive-bgp-next-hop
```

To disable next-hop resolution, use the no bgp recursive-bgp-next-hop command.

**Defaults**

Enabled

**Command Modes**

ROUTER BGP

**Usage Information**

This command is a knob to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route’s protocol source and is checked if the route is learned from BGP or not.

The clear ip bgp command is required for this command to take effect and to keep the BGP database consistent. Execute the clear ip bgp command right after executing this command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**bgp regex-eval-optz-disable**

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

**Syntax**

```
bgp regex-eval-optz-disable
```

To re-enable optimization engine, use the no bgp regex-eval-optz-disable command.

**Defaults**

Enabled.

**Command Modes**

ROUTER BGP (conf-router_bgp)
BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the show bgp commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.

**Example**

**Figure 8-2. Command Example: no bgp regex-eval-optz-disable**

```
FTOS(conf-router_bgp)#no bgp regex-eval-optz-disable
FTOS(conf-router_bgp)#do show ip protocols
Routing Protocol is "ospf 22222"
   Router ID is 2.2.2.2
   Area             Routing for Networks
   51               10.10.10.0/00
Routing Protocol is "bgp 1"
   Cluster Id is set to 10.10.10.0
   Router Id is set to 10.10.10.0
   Fast-external-fallover enabled
   Regular expression evaluation optimization enabled
   Capable of ROUTE_REFRESH
   For Address Family IPv4 Unicast
     BGP table version is 0, main routing table version 0
     Distance: external 20 internal 200 local 200
FTOS(conf-router_bgp)#
```

**Related Commands**

- `show ip protocols` View information on all routing protocols enabled and active.

**bgp router-id**

Assign a user-given ID to a BGP router.

**Syntax**

```
bgp router-id ip-address
```

To delete a user-assigned IP address, enter the `no bgp router-id` command.

**Parameters**

- `ip-address` Enter an IP address in dotted decimal format to reset only that BGP neighbor.

**Defaults**

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

**Command Modes**

ROUTER BGP

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Peering sessions are reset when you change the router ID of a BGP router.

**bgp soft-reconfig-backup**

Use this command *only* when route-refresh is *not* negotiated to avoid the peer from resending messages.

**Syntax**

```
bgp soft-reconfig-backup
```

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

**Defaults**

Off

**Command Modes**

ROUTER BGP

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer’s updates.

**Related Commands**

- `capture bgp-pdu neighbor` — Enable capture of an IPv4 BGP neighbor packet.
- `clear ip bgp soft in` — Activate inbound policies without resetting the BGP TCP session.

**capture bgp-pdu neighbor**

Enable capture of an IPv4 BGP neighbor packet.

**Syntax**

```
capture bgp-pdu neighbor ipv4-address direction {both | rx | tx}
```

To disable capture of the IPv4 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv4-address` command.

**Parameters**

- `ipv4-address` — Enter the IPv4 address of the target BGP neighbor.
- `direction {both | rx | tx}` — Enter the keyword `direction` and a direction— either `rx` for inbound, `tx` for outbound, or `both`.

**Defaults**

Not configured.

**Command Modes**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `capture bgp-pdu max-buffer-size` — Specify a size for the capture buffer.
- `show capture bgp-pdu neighbor` — Display BGP packet capture information.
capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Syntax

capture bgp-pdu max-buffer-size 100-102400000

Parameters

100-102400000 Enter a size for the capture buffer.

Defaults

40960000 bytes.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

capture bgp-pdu neighbor Enable capture of an IPv4 BGP neighbor packet.
capture bgp-pdu neighbor (ipv6) Enable capture of an IPv6 BGP neighbor packet.
show capture bgp-pdu neighbor Display BGP packet capture information for an IPv6 address.

clear ip bgp

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax

clear ip bgp * | as-number | ip-address [flap-statistics | soft [in | out]]

Parameters

* Enter an asterisk (*) to reset all BGP sessions.
as-number Enter the AS number to reset all neighbors belonging to that AS.
  Range: 0 to 65535 (2-Byte) or 1 to 4294967295 (4-Byte) or 0.1 to 65535.65535 (Dotted format)

ip-address Enter an IP address in dotted decimal format to reset all prefixes from that neighbor.

flap-statistics (OPTIONAL) Enter the keyword flap-statistics to reset the flap statistics on all prefixes from that neighbor.

soft (OPTIONAL) Enter the keyword soft to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
  Note: If you enter clear ip bgp ip-address soft, both inbound and outbound policies are reset.
in (OPTIONAL) Enter the keyword in to activate only inbound policies.
out (OPTIONAL) Enter the keyword out to activate only outbound policies.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
clear ip bgp dampening
Clear information on route dampening and return suppressed route to active state.

Syntax
```
clear ip bgp dampening [ip-address mask]
```

Parameters
- **ip-address mask**: (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.

Command Modes
- EXEC Privilege

Usage Information
After you enter this command, the software deletes history routes and returns suppressed routes to active state.

Command History
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

clear ip bgp flap-statistics
Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax
```
clear ip bgp flap-statistics [ip-address mask | filter-list as-path-name | regexp regular-expression]
```

Parameters
- **ip-address mask**: (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.
- **filter-list as-path-name**: (OPTIONAL) Enter the keyword filter-list followed by the name of a configured AS-PATH list.
- **regexp regular-expression**: (OPTIONAL) Enter the keyword regexp followed by regular expressions. Use one or a combination of the following:
  - . = (period) any single character (including a white space)
  - * = (asterisk) the sequences in a pattern (0 or more sequences)
  - + = (plus) the sequences in a pattern (1 or more sequences)
  - ? = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
  - [ ] = (brackets) a range of single-character patterns.
  - () = (parenthesis) groups a series of pattern elements to a single element
  - {} = (braces) minimum and the maximum match count
  - ^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - $ = (dollar sign) the end of the output string.

Command Modes
- EXEC Privilege

Usage Information
If you enter the clear ip bgp flap-statistics command without any parameters, all statistics are cleared.

Related Commands
- **show debugging**: View enabled debugging operations.
- **show ip bgp flap-statistics**: View BGP flap statistics.
- **undebug all**: Disable all debugging operations.
clear ip bgp peer-group

Reset a peer group’s BGP sessions.

Syntax

```
clear ip bgp peer-group peer-group-name
```

Parameters

- `peer-group peer-group-name`
  Enter the keyword `peer-group` followed by the name of the peer group.

Command Modes

EXEC Privilege

Related Commands

- **debug ip bgp**
  Display all information on BGP, including BGP events, keepalives, notifications, and updates.

Syntax

```
debug ip bgp [ip-address | peer-group peer-group-name] [in | out]
```

Parameters

- `ip-address`
  Enter the IP address of the neighbor in dotted decimal format.

- `peer-group peer-group-name`
  Enter the keyword `peer-group` followed by the name of the peer group.

- `in`
  (OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.

- `out`
  (OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

Command Modes

EXEC Privilege

Usage Information

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the debugging command. The `in` and `out` parameters cancel each other; for example, if you enter `debug ip bgp in` and then enter `debug ip bgp out`, you will not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

- **debug ip bgp events**
  View information about BGP events.

- **debug ip bgp keepalives**
  View information about BGP keepalives.

- **debug ip bgp notifications**
  View information about BGP notifications.

- **debug ip bgp updates**
  View information about BGP updates.

- **show debugging**
  View enabled debugging operations.
debug ip bgp dampening

Display information on routes being dampened.

Syntax

d ebug ip bgp dampening [in | out]

To disable debugging, enter no debug ip bgp dampening.

Parameters

- **in** (OPTIONAL) Enter the keyword in to view only inbound dampened routes.
- **out** (OPTIONAL) Enter the keyword out to view only outbound dampened routes.

Command Modes

EXEC Privilege

Usage Information

Enter no debug ip bgp command to remove all configured debug commands for BGP.

Related Commands

- **show debugging** View enabled debugging operations.
- **show ip bgp dampened-paths** View BGP dampened routes.

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

debug ip bgp events

Display information on local BGP state changes and other BGP events.

Syntax

d ebug ip bgp [ip-address | peer-group peer-group-name] events [in | out]

To disable debugging, use the no debug ip bgp [ip-address | peer-group peer-group-name] events command.

Parameters

- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group peer-group-name** (OPTIONAL) Enter the keyword peer-group followed by the name of the peer group.
- **in** (OPTIONAL) Enter the keyword in to view only events on inbound BGP messages.
- **out** (OPTIONAL) Enter the keyword out to view only events on outbound BGP messages.

Command Modes

EXEC Privilege

Usage Information

Enter no debug ip bgp command to remove all configured debug commands for BGP.

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
debug ip bgp keepalives

Display information about BGP keepalive messages.

**Syntax**

```
debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

**Parameters**

- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group peer-group-name** (OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
- **in** (OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
- **out** (OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

**Command Modes**

EXEC Privilege

**Usage Information**

Enter `no debug ip bgp` command to remove all configured debug commands for BGP.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

debug ip bgp notifications

Enables you to view information about BGP notifications received from neighbors.

**Syntax**

```
debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

**Parameters**

- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group peer-group-name** (OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
- **in** (OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.
- **out** (OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors.

**Command Modes**

EXEC Privilege

**Usage Information**

Enter `no debug ip bgp` command to remove all configured debug commands for BGP.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
debug ip bgp soft-reconfiguration
Enable soft-reconfiguration debug.

Syntax
ddebug ip bgp {ip-address | peer-group-name} soft-reconfiguration

To disable, use the no debug ip bgp {ip-address | peer-group-name} soft-reconfiguration command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.</td>
</tr>
</tbody>
</table>

Defaults
Disabled

Command Modes
EXEC Privilege

Usage Information
This command turns on BGP soft-reconfiguration inbound debugging. If no neighbor is specified, debug is turned on for all neighbors.

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

debug ip bgp updates
Enables you to view information about BGP updates.

Syntax
ddebug ip bgp updates [in | out | prefix-list prefix-list-name]

To disable debugging, use the no debug ip bgp [ip-address | peer-group peer-group-name] updates [in | out] command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword in to view only BGP updates received from neighbors.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword out to view only BGP updates sent to neighbors.</td>
</tr>
<tr>
<td>prefix-list</td>
<td>(OPTIONAL) Enter the keyword prefix-list followed by the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).</td>
</tr>
<tr>
<td>prefix-list-name</td>
<td>(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.</td>
</tr>
</tbody>
</table>

Command Modes
EXEC Privilege

Usage Information
Enter no debug ip bgp command to remove all configured debug commands for BGP.

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**default-metric**

Enables you to change the metrics of redistributed routes to locally originated routes. Use this command with the redistribute command.

**Syntax**

```
default-metric number
```

To return to the default setting, enter the `no default-metric` command.

**Parameters**

- `number`: Enter a number as the metric to be assigned to routes from other protocols. Range: 1 to 4294967295.

**Defaults**

0

**Command Modes**

ROUTER BGP

**Usage Information**

The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

**Related Commands**

- `bgp always-compare-med`: Enable comparison of all BGP MED attributes.
- `redistribute`: Redistribute routes from other routing protocols into BGP.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**description**

Enter a description of the BGP routing protocol

**Syntax**

```
description \{description\}
```

To remove the description, use the `no description \{description\}` command.

**Parameters**

- `description`: Enter a description to identify the BGP protocol (80 characters maximum).

**Defaults**

No default behavior or values

**Command Modes**

ROUTER BGP

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `router bgp`: Enter ROUTER mode on the switch.

---

**max-paths**

Configure the maximum number of parallel routes (multipath support) BGP supports.

**Syntax**

```
max-paths \{ebgp | ibgp\} number
```

**Parameters**

- `ebgp`, `ibgp`: Specify whether to configure EBGP or IBGP
- `number`: Enter a number as the metric to be assigned to routes from other protocols. Range: 1 to 4294967295.

**Defaults**

No default behavior or values

**Command Modes**

ROUTER BGP

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
To return to the default values, enter no maximum-paths.

**Parameters**

- **ebgp**
  Enter the keyword `ebgp` to enable multipath support for External BGP routes.

- **ibgp**
  Enter the keyword `ibgp` to enable multipath support for Internal BGP routes.

- **number**
  Enter a number as the maximum number of parallel paths.
  Range: 2 to 64

**Defaults**

none

**Command Modes**

ROUTER BGP

**Usage Information**

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier).

**Syntax**

```plaintext
neighbor [ip-address | peer-group-name] activate
```

To disable, use the `no neighbor [ip-address | peer-group-name] activate` command.

**Parameters**

- **ip-address**
  (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.

- **peer-group-name**
  (OPTIONAL) Enter the name of the peer group

- **activate**
  Enter the keyword `activate` to enable the neighbor/peer group in the new AFI/SAFI.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

**Usage Information**

By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv4/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

**Syntax**

```plaintext
neighbor [ip-address | peer-group-name] add-path [send | receive | both] count
```

**Parameters**

- **ip-address**
  (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.

- **peer-group-name**
  (OPTIONAL) Enter the name of the peer group

- **count**
  Enter a number as the maximum number of parallel paths.
  Range: 2 to 64
### neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

**Syntax**
```
neighbor {ip-address | peer-group-name} advertisement-interval seconds
```

To return to the default value, use the no neighbor {ip-address | peer-group-name} advertisement-interval command.

**Parameters**
- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name** (OPTIONAL) Enter the name of the peer group.
- **seconds** Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

**Defaults**
- **seconds** = 5 seconds (internal peers); **seconds** = 30 seconds (external peers)

**Command Modes**
- ROUTER BGP

**Command History**
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

### neighbor advertisement-start

Set the minimum interval before starting to send BGP routing updates.

**Syntax**
```
neighbor {ip-address | peer-group-name} advertisement-start seconds
```

**Parameters**
- **ip-address** Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name** Enter the name of the peer group.
- **seconds** Enter a number as the time interval, in seconds, before starting to send BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

**Defaults**
- **seconds** = 5 seconds (internal peers); **seconds** = 30 seconds (external peers)

**Command Modes**
- ROUTER BGP

**Command History**
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
To return to the default value, use the `no neighbor {ip-address} advertisement-start` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>Enter a number as the time interval, in seconds, before BGP route updates are sent. Range: 0 to 3600 seconds.</td>
</tr>
</tbody>
</table>

**Defaults**

`none`

**Command Modes**

ROUTER BGP

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**neighbor allowas-in**

Set the number of times an AS number can occur in the AS path.

**Syntax**

`neighbor {ip-address | peer-group-name} allowas-in number`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Enter the name of the peer group to set the advertisement interval for all routers in the peer group.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>Enter a number of times to allow this neighbor ID to use the AS path. Range: 1 to 10.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp four-octet-as-support</code></td>
<td>Enable 4-Byte support for the BGP process.</td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**neighbor default-originate**

Inject the default route to a BGP peer or neighbor.

**Syntax**

`neighbor {ip-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Enter the name of the peer group to set the advertisement interval for all routers in the peer group.</td>
</tr>
<tr>
<td><code>route-map map-name</code></td>
<td>Enter the name of the route map.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp four-octet-as-support</code></td>
<td>Enable 4-Byte support for the BGP process.</td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
 neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

**Syntax**

`neighbor {ip-address | peer-group-name} description text`

To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group.
- `text` Enter a continuous text string up to 80 characters.

**Defaults**
Not configured.

**Command Modes**
ROUTER BGP

**Command History**
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

 neighbor distribute-list

Distribute BGP information via an established prefix list.

**Syntax**

`neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group.
- `prefix-list-name` Enter the name of an established prefix list.
  - If the prefix list is not configured, the default is permit (to allow all routes).

**Defaults**
Not configured.

**Command Modes**
ROUTER BGP

**Command History**
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Defaults
Not configured.

Command Modes
ROUTER BGP

Usage Information
Other BGP filtering commands include: neighbor filter-list, ip as-path access-list, and neighbor route-map.

Related Commands
neighbor route-map Assign a route map to a neighbor or peer group.

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

neighbor ebgp-multihop
Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax
neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]

To disallow and disconnect connections, use the no neighbor {ip-address | peer-group-name} ebgp-multihop command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group.</td>
</tr>
<tr>
<td>ttl</td>
<td>(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. Range: 1 to 255. Default: 255</td>
</tr>
</tbody>
</table>

Defaults
Disabled.

Command Modes
ROUTER BGP

Usage Information
To prevent loops, the neighbor ebgp-multihop command does not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

neighbor fall-over
Enable or disable fast fall-over for BGP neighbors.

Syntax
neighbor {ipv4-address | peer-group-name} fall-over

To disable, use the no neighbor {ipv4-address | peer-group-name} fall-over command.
neighbor graceful-restart

Enable graceful restart on a BGP neighbor.

Syntax
neighbor \{ip-address | peer-group-name\} graceful-restart \[restart-time seconds\] \[stale-path-time seconds\] \[role receiver-only\]

Parameters

- **ip-address**: Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name**: Enter the name of the peer group to apply the filter to all routers in the peer group.
- **restart-time seconds**: Enter the keyword **restart-time** then the maximum number of seconds to restart and bring-up all the peers. The range is from 1 to 3600 seconds. The default is 120 seconds.
- **stale-path-time seconds**: Enter the keyword **stale-path-time** then the maximum number of seconds to wait before restarting a peer’s stale paths. The default is 360 seconds.
- **role receiver-only**: Enter the keyword **role receiver-only** to designate the local router to support graceful restart as a receiver only.

Command Modes
- ROUTER BGP

Command History
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
This feature advertises to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.
neighbor local-as

Configure Internal BGP (IBGP) routers to accept external routes from neighbors with a local AS number in the AS number path.

**Syntax**

```
neighbor {ip-address | peer-group-name} local-as as-number [no-prepend]
```

To return to the default value, use the `no neighbor {ip-address | peer-group-name} local-as` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group.</td>
</tr>
<tr>
<td>as-number</td>
<td>Enter the AS number to reset all neighbors belonging to that AS.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)</td>
</tr>
<tr>
<td>no prepend</td>
<td>Specifies that local AS values are not prepended to announcements from the neighbor.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Related Commands**

- `bgp four-octet-as-support`: Enable 4-Byte support for the BGP process.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

neighbor maximum-prefix

Control the number of network prefixes received.

**Syntax**

```
neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]
```

To return to the default values, use the `no neighbor {ip-address | peer-group-name} maximum-prefix maximum` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group.</td>
</tr>
<tr>
<td>maximum</td>
<td>Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.</td>
</tr>
</tbody>
</table>
neighbor password

Enable Message Digest 5 (MD5) authentication on the TCP connection between two neighbors.

**Syntax**

```
neighbor {ip-address | peer-group-name} password [encryption-type] password
```

To delete a password, use the no neighbor {ip-address | peer-group-name} password command.

**Parameters**

- **ip-address**: Enter the IP address of the router to be included in the peer group.
- **peer-group-name**: Enter the name of a configured peer group.
- **encryption-type** (OPTIONAL): Enter 7 as the encryption type for the `password` entered. 7 means that the password is encrypted and hidden.
- **password**: Enter a text string up to 80 characters long. The first character of the `password` must be a letter. You cannot use spaces in the password.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.
If you specify a BGP peer group by using the `peer-group-name` parameter, all the members of the peer group will inherit the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```
%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address]:179 to [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```
%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from [peer's IP address]:11502 to [local router's IP address]:179
```

### Command History

| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |

### neighbor peer-group (assigning peers)

Enables you to assign one peer to a existing peer group.

**Syntax**

```
neighbor ip-address peer-group peer-group-name
```

To delete a peer from a peer group, use the `no neighbor ip-address peer-group peer-group-name` command.

**Parameters**

<table>
<thead>
<tr>
<th>ip-address</th>
<th>Enter the IP address of the router to be included in the peer group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>Enter the name of a configured peer group.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTE BGP

**Usage Information**

You can assign up to 256 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group’s configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- `neighbor advertisement-interval`
- `neighbor distribute-list out`
- `neighbor route-map out`
- `neighbor route-reflector-client`
- `neighbor shutdown`

A neighbor may keep its configuration after it was added to a peer group if the neighbor’s configuration is more specific than the peer group’s, and the neighbor’s configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).
neighbor peer-group (creating group)

Enables you to create a peer group and assign it a name.

Syntax

```
neighbor peer-group-name peer-group
```

Parameters

- `peer-group-name` Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

When a peer group is created, it is disabled (shut mode).

Related Commands

- `clear ip bgp` Resets BGP sessions.
- `neighbor peer-group (creating group)` Create a peer group.
- `show ip bgp peer-group` View BGP peers.
- `show ip bgp neighbors` View BGP neighbors configurations.

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but will respond to one.

Syntax

```
neighbor peer-group-name peer-group passive [limit sessions]
```

Parameters

- `peer-group-name` Enter a text string up to 16 characters long as the name of the peer group.
- `limit` (Optional) Enter the keyword limit to constrain the numbers of sessions for this peer-group.
  - Range: 2-256
  - Default: 256

To delete a passive peer-group, use the no `neighbor peer-group-name peer-group passive` command.

Related Commands

- `neighbor peer-group (assigning peers)` Assign routers to a peer group.
- `neighbor remote-as` Assign a indirectly connected AS to a neighbor or peer group.
- `neighbor shutdown` Disable a peer or peer group.

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Defaults
Not Configured

Command Modes
ROUTER BGP

Usage Information
After you configure a peer group as passive, you must assign it a subnet using the neighbor soft-reconfiguration inbound command.

For passive eBGP limits, the Remote AS must be different from the AS for this neighbor.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor soft-reconfiguration inbound</td>
<td>Assign a subnet to a dynamically-configured BGP neighbor.</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Create and specify the remote peer to the BGP neighbor.</td>
</tr>
</tbody>
</table>

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

neighbor remote-as
Create and specify the remote peer to the BGP neighbor.

Syntax
neighbor \{ip-address | peer-group-name\} remote-as number

To delete a remote AS entry, use the no neighbor \{ip-address | peer-group-name\} remote-as number command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor to enter the remote AS in its routing table.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.</td>
</tr>
<tr>
<td>number</td>
<td>Enter a number of the AS. Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte)</td>
</tr>
</tbody>
</table>

Defaults
Not configured.

Command Modes
ROUTER BGP

Usage Information
You must configure your system to accept 4-Byte formats before entering a 4-Byte AS Number. If the number parameter is the same as the AS number used in the router bgp command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (shutdown).

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router bgp</td>
<td>Enter the ROUTER BGP mode and configure routes in an AS.</td>
</tr>
<tr>
<td>bgp four-octet-as-support</td>
<td>Enable 4-Byte support for the BGP process.</td>
</tr>
</tbody>
</table>

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax
neighbor {ip-address | peer-group-name} remove-private-as

To return to the default, use the no neighbor {ip-address | peer-group-name} remove-private-as command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor to remove the private AS numbers.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group to remove the private AS numbers.</td>
</tr>
</tbody>
</table>

Defaults
Disabled (that is, private AS number are not removed).

Command Modes
ROUTER BGP

Usage Information
Applies to EBGP neighbors only.

You must configure your system to accept 4-Byte formats before entering a 4-Byte AS Number.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535 (2-Byte).

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax
neighbor {ip-address | peer-group-name} route-map map-name {in | out}

To remove the route map, use the no neighbor {ip-address | peer-group-name} route-map map-name {in | out} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group.</td>
</tr>
<tr>
<td>map-name</td>
<td>Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).</td>
</tr>
<tr>
<td>in</td>
<td>Enter the keyword in to filter inbound routes.</td>
</tr>
<tr>
<td>out</td>
<td>Enter the keyword out to filter outbound routes.</td>
</tr>
</tbody>
</table>

Defaults
Not configured.

Command Modes
ROUTER BGP
When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure the router as a route reflector and the specified neighbors as members of the cluster.

Syntax

neighbor {ip-address | peer-group-name} route-reflector-client

To remove one or more neighbors from a cluster, use the no neighbor {ip-address | peer-group-name} route-reflector-client command. If you delete all members of a cluster, you also delete the route-reflector configuration on the router.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group.</td>
</tr>
<tr>
<td></td>
<td>All routers in the peer group receive routes from a route reflector.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

ROUTER BGP

A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need not be fully meshed. By default, when no route reflector is used, internal BGP (IBGP) speakers in the network must be fully meshed.

The first time you enter this command the router is configured as a route reflector and the specified BGP neighbors are configured as clients in the route-reflector cluster.

When you remove all clients of a route reflector using the no neighbor route-reflector-client command, the router no longer functions as a route reflector.

If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the no bgp client-to-client reflection command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp client-to-client reflection</td>
<td>Enable route reflection between route reflector and clients.</td>
</tr>
</tbody>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**neighbor shutdown**

Disable a BGP neighbor or peer group.

**Syntax**

```
neighbor {ip-address | peer-group-name} shutdown
```

To enable a disabled neighbor or peer group, use the `neighbor {ip-address | peer-group-name} no shutdown` command.

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group to disable or enable all routers within the peer group.

**Defaults**

Enabled (that is, BGP neighbors and peer groups are disabled.)

**Command Modes**

ROUTER BGP

**Usage Information**

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp summary` command to confirm its status.

**Related Commands**

- `show ip bgp summary` Displays the current BGP configuration.
- `show ip bgp neighbors` Displays the current BGP neighbors.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**neighbor soft-reconfiguration inbound**

Enable soft-reconfiguration for BGP.

**Syntax**

```
neighbor {ip-address | peer-group-name} soft-reconfiguration inbound
```

To disable, use the `no neighbor {ip-address | peer-group-name} soft-reconfiguration inbound` command.

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group to disable or enable all routers within the peer group.

**Defaults**

Disabled

**Command Modes**

ROUTER BGP
This command enables soft-reconfiguration for the BGP neighbor specified. BGP will store all the updates received by the neighbor but will not reset the peer-session.

**Caution:** Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.

**Note:** This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp neighbors</td>
<td>Display routes received by a neighbor</td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

**Syntax**

```
neighbor {ip-address | peer-group-name} timers keepalive holdtime
```

To return to the default values, use the `no neighbor {ip-address | peer-group-name} timers` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the peer router in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group to set the timers for all routers within the peer group.</td>
</tr>
</tbody>
</table>
| keepalive       | Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers.  
  Range: 1 to 65535  
  Default: 60 seconds |
| holdtime        | Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead.  
  Range: 3 to 65535  
  Default: 180 seconds |

**Defaults**

- `keepalive = 60` seconds; `holdtime = 180` seconds.

**Command Modes**

- **ROUTER BGP**

**Usage Information**

Timer values configured with the `neighbor timers` command override the timer values configured with the any other command.

When two neighbors, configured with different `keepalive` and `holdtime` values, negotiate for new values, the resulting values will be as follows:

- the lower of the `holdtime` values is the new `holdtime` value, and
- whichever is the lower value; one-third of the new `holdtime` value, or the configured `keepalive` value is the new `keepalive` value.
neighbor update-source
Enable the software to use Loopback interfaces for TCP connections for BGP sessions.

**Syntax**

```
neighbor {ip-address | peer-group-name} update-source interface
```

To use the closest interface, use the `no neighbor {ip-address | peer-group-name} update-source interface` command.

**Parameters**

- `ip-address` Enter the IP address of the peer router in dotted decimal format.
- `peer-group-name` Enter the name of the peer group to disable all routers within the peer group.
- `interface` Enter the keyword `loopback` followed by a number of the loopback interface. Range: 0 to 16383.

**Defaults**
Not configured.

**Command Modes**
ROUTER BGP

**Usage Information**
Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

neighbor weight
Assign a weight to the neighbor connection, which is used to determine the best path.

**Syntax**

```
neighbor {ip-address | peer-group-name} weight weight
```

To remove a weight value, use the `no neighbor {ip-address | peer-group-name} weight` command.

**Parameters**

- `ip-address` Enter the IP address of the peer router in dotted decimal format.
- `peer-group-name` Enter the name of the peer group to disable all routers within the peer group.
- `weight` Enter a number as the weight. Range: 0 to 65535

**Defaults**
0

**Command Modes**
ROUTER BGP
In the FTOS best path selection process, the path with the highest weight value is preferred.

**Note:** Reset the neighbor connection (clear ip bgp * command) to apply the weight to the connection and recompute the best path.

If the set weight command is configured in a route map applied to this neighbor, the weight set in that command overrides the weight set in the neighbor weight command.

### Command History

| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |

### network

Specify the networks for the BGP process and enter them in the BGP routing table.

**Syntax**

```
network ip-address mask [route-map map-name]
```

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

**Parameters**

- **ip-address**
  - Enter an IP address in dotted decimal format of the network.
- **mask**
  - Enter the mask of the IP address in the slash prefix length format (for example, /24).
  - The mask appears in command outputs in dotted decimal format (A.B.C.D).
- **route-map map-name** (OPTIONAL)
  - Enter the keyword `route-map` followed by the name of an established route map.
  - Only the following ROUTE-MAP mode commands are supported:
    - `match ip address`
    - `set metric`
    - `set metric`
    - `set metric`
    - `set metric`
    - `set tag`
  - If the route map is not configured, the default is deny (to drop all routes).

**Defaults**

Not configured.

**Command Modes**

- ROUTER BGP

**Usage Information**

FTOS software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

**Related Commands**

- `redistribute` — Redistribute routes into BGP.

**Command History**

| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |
**network backdoor**

Specify this IGP route as the preferred route.

**Syntax**

```
network ip-address mask backdoor
```

To remove a network, use the `no network ip-address mask backdoor` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Enter an IP address in dotted decimal format of the network.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Though FTOS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**redistribute**

Redistribute routes into BGP.

**Syntax**

```
redistribute {connected | static} [route-map map-name]
```

To disable redistribution, use the `no redistribute {connected | static} [route-map map-name]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>connected</code></td>
<td>Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.</td>
</tr>
<tr>
<td><code>route-map map-name</code></td>
<td>(OPTIONAL) Enter the keyword <code>route-map</code> followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported:</td>
</tr>
</tbody>
</table>

If the route map is not configured, the default is deny (to drop all routes).

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP
With FTOS version 8.3.1.0 and later, the redistribute command can be used to advertise the IGP cost as the MED on redistributed routes. When the route-map is set with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-group will have IGP cost set as MED.

If you do not configure default-metric command, in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0.0.0.0/0) configure the neighbor default-originate command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>neighbor default-originate</strong></td>
<td>Inject the default route.</td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**redistribute ospf**

Redistribute OSPF routes into BGP.

**Syntax**

redistribute ospf process-id [[match external {1 | 2}] [match internal]] [route-map map-name]

To stop redistribution of OSPF routes, use the no redistribute ospf process-id command.

**Parameters**

- **process-id**
  - Enter the number of the OSPF process.
  - Range: 1 to 65535
- **match external {1 | 2}**
  - (OPTIONAL) Enter the keywords match external to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
- **match internal**
  - (OPTIONAL) Enter the keywords match internal to redistribute OSPF internal routes only.
- **route-map map-name**
  - (OPTIONAL) Enter the keywords route-map followed by the name of a configured Route map.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

With FTOS version 8.3.1.0 and later, the redistribute command can be used to advertise the IGP cost as the MED on redistributed routes. When the route-map is set with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-group will have IGP cost set as MED.

When you enter redistribute isis process-id command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. This feature is not supported by an RFC.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
router bgp

Enter ROUTER BGP mode to configure and enable BGP.

**Syntax**

```
router bgp as-number
```

To disable BGP, use the no router bgp as-number command.

**Parameters**

- **as-number**: Enter the AS number.
  - Range: 1 to 65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION

**Example**

**Figure 8-3. Command Example: router bgp**

```
FTOS(conf)#router bgp 3
FTOS(conf-router_bgp)#
```

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

At least one interface must be in Layer 3 mode for the router bgp command to be accepted. If no interfaces are enabled for Layer 3, an error message appears: % Error: No router id configured.

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

**Syntax**

```
show capture bgp-pdu neighbor ipv4-address
```

**Parameters**

- **ipv4-address**: Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.

**Command Modes**

EXEC Privilege
Example Figure 8-4. Command Example: show capture bgp-pdu neighbor

```
FTOS(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using 680 bytes
PDU[1] : len 101, captured 00:34:51 ago
  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
  d41d8cd9 896a02b0 f87c700e 9ed1098c 9d5e2b0c
PDU[2] : len 19, captured 00:34:51 ago
  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
  00000000 00000000
PDU[3] : len 19, captured 00:34:51 ago
  00000000 00000000 00000000 00000000 00000000

Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 27 packet(s) captured using 562 bytes
PDU[1] : len 41, captured 00:34:52 ago
  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
  00000000 00000000 00000000
PDU[2] : len 19, captured 00:34:51 ago
  00000000 00000000 00000000 00000000 00000000 00000000
PDU[3] : len 19, captured 00:34:50 ago
  00000000 00000000 00000000

FTOS#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture bgp-pdu max-buffer-size</td>
<td>Specify a size for the capture buffer.</td>
</tr>
</tbody>
</table>

Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

```
show config
```

View the current ROUTER BGP configuration.

Syntax

```
show config
```

Command Modes

- **ROUTER BGP**

Example Figure 8-5. show config Command Example

```
FTOS(conf-router_bgp)#show confi
router bgp 45
neighbor suzanne peer-group
neighbor suzanne no shutdown
neighbor sara peer-group
neighbor sara shutdown
neighbor 13.14.15.20 peer-group suzanne
neighbor 13.14.15.20 shutdown
neighbor 123.34.55.123 peer-group suzanne
neighbor 123.34.55.123 shutdown
FTOS(conf-router_bgp)#
```

Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
show ip bgp

View the current BGP IPv4 routing table for the system.

Syntax

```bash
show ip bgp [ipv4 unicast] [network [network-mask] [longer-prefixes]]
```

Parameters

- `ipv4 unicast` (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to ipv4 unicast routes.
- `network` (OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
- `network-mask` (OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
- `longer-prefixes` (OPTIONAL) Enter the keyword `longer-prefixes` to view all routes with a common prefix.

Command Modes

- EXEC

EXEC Privilege

Usage Information

When you enable `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

Example

```
Figure 8-6. show ip bgp Command Example (Partial)
```
Table 8-1 defines the information displayed in Figure 8-6

**Table 8-1. show ip bgp Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router.</td>
</tr>
<tr>
<td></td>
<td>If 0.0.0.0 is listed in this column, then local routes exist in the routing</td>
</tr>
<tr>
<td></td>
<td>table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show ip bgp community` View BGP communities.
- `neighbor maximum-prefix` Control number of network prefixes received.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**show ip bgp cluster-list**

View BGP neighbors in a specific cluster.

**Syntax**

```
show ip bgp [ipv4 unicast] cluster-list [cluster-id]
```

**Parameters**

- `ipv4 unicast` (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to ipv4 unicast routes.
- `cluster-id` (OPTIONAL) Enter the cluster id in dotted decimal format.

**Command Modes**

- EXEC
- EXEC Privilege
FTOS#show ip bgp cluster-list
BGP table version is 6444463, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.10.10.1/32</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*&gt;I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>* 10.19.75.5/32</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt;I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* 10.30.1.0/24</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt;I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>

Table 8-2 defines the information displayed in Figure 8-7.

Table 8-2. show ip bgp cluster-list Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

Syntax

```
show ip bgp [ipv4 unicast] community [community-number] [local-as] [no-export] [no-advertise]
```
**Parameters**

- **ipv4 unicast**: (OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.

- **community-number**: Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.

- **local-AS**: Enter the keywords local-AS to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.

- **no-advertise**: Enter the keywords no-advertise to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.

- **no-export**: Enter the keywords no-export to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

**Command Modes**

- EXEC
- EXEC Privilege

**Usage Information**

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

**Example**

Figure 8-8. show ip bgp community Command Example (Partial)
The show ip bgp community command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the show ip bgp command output.

### Table 8-3. Command Example Fields: show ip bgp community

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### show ip bgp community-list

View routes that are affected by a specific community list.

**Syntax**

```
show ip bgp [ipv4 unicast] community-list community-list-name [exact-match]
```

**Parameters**

- `ipv4 unicast` (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to ipv4 unicast routes.
- `community-list-name` Enter the name of a configured IP community list. (max 16 chars)
- `exact-match` Enter the keyword for an exact match of the communities.

**Command Modes**

EXEC

EXEC Privilege

**Example**

**Figure 8-9. Command Example: show ip bgp community-list**

```
FTOS#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network       Next Hop        Metric   LocPrf  Weight  Path
FTOS#
```
The `show ip bgp community-list` command without any parameters lists BGP routes matching the Community List and the output is the same as for the `show ip bgp` command output.

### Table 8-4. show ip bgp community-list Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

**Syntax**

`show ip bgp [ipv4 unicast] dampened-paths`

**Command Modes**

- EXEC
- EXEC Privilege

**Example**

Figure 8-10. Command Example: show ip bgp dampened-paths

```
FTOS>show ip bgp damp
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
Network  From             Reuse     Path
---------  ----------------  --------  ----
---------  ----------------  --------  ----
FTOS>
```

Table 8-5 defines the information displayed in Figure 8-10.

### Table 8-5. show ip bgp dampened-paths Command Example

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the network ID to which the route is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>Displays the IP address of the neighbor advertising the dampened route.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Displays the hour:minutes:seconds until the dampened route is available.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the dampened route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>
show ip bgp detail

Display BGP internal information for IPv4 Unicast address family.

Syntax
show ip bgp [ipv4 unicast] detail

Defaults
none

Command Modes
EXEC
EXEC Privilege

Example

Figure 8-11. Sample partial output: show ip bgp detail

FTOS#show ip bgp detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPFPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedMissVal -1 :
NdIngnr11Id 0 : NdRCRC2 1 : NdClstId 3368273 : NdPaTblP 0x41a19088
NdASPfP 0x41a19050 : NdCommTblP 0x41a19098 : NdOptTransTblP 0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPtXP 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRC1P 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNhNP : NdOrigPAP 0
NdOrgNhNP 0 : NdModPathP 0x419efc60 : NdModASPAP 0x41a4c000 : NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNhNP : NdComSortBufP 0x41a19110 : NdComSortHdp
0x41a19d04 : NdUpdAFMsk 0 : AFRstSet 0x41a1a298 : NHopDfrdHdp 0x41a1a3e0 :
NumNhDfrd 0 : CfgHdrrAffmsk 1
APChNetTmrP 0x41ee705c 0x41ee705c : AFRtDamp 0 : AlwaysCmpMed 0 : LocRld 10 : LocRm 10 :
softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : Fails 0 : ConnExps 0 : HldExps 0 : KeepExps 0
RxOpens 0 : RrKeeps 0 : RxUpdps 0 : RxNotifs 0 : TxUpdps 0 : TxNotifs 0
BadEvtS 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP 0x41a1b6d8 : RxOpCodeP
0x41a1b64d
RxUpdCodeP 0x41a1b714 : TxCodeP 0x41a1b714 : TxHdrcodeP 0x41a1b750 : TxOpCodeP
0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP 0x41a1b7b8 : LogNbrChgs 1
RecrsiveNHNN 1 : PrcfgId 0 : KeepAlive 0 : HldTime 0 : BioHld 0 : AggrValTmrP
0x41e77024
UpdNetTmrP 0 : RedistTmrP 0x41e77094 : PeerChqTmrP 0 : CleanRibTmrP 0x41e77104
PeerUpdTmrP 0x41e7770c : DfrdNhTmrP 0x41e77174 : DfrdRcstlTmrP 0x41e7713c :
FastExtFallover 1 : FastIntFallover 0 : Enforce1stAs 1
Peer1dtsP 0x41967120 : soOutSz 16 : RibUpdCtxtCBP 0
UpdPeerCtxtCBP 0 : UpdPeerCtxtAFI 0 : TcpioCtxCB 0 : RedistBlk 1
NextCBFurg 0x11119536 : NumPeerToFurge 0 : PeerIBGPcnt 0 : NonDet 0 : DfrdPathSel 0
BGPRat 0 : NumGrCfg 1 : DfrdTmeestmp 0 : SmpTrps 0 : IgIdxBestPathASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalg 7 : RstInt 120 : MxoeExtInt 361
FixedPartCrt 1 : VarParrCrt 1
Packet Capture max allowed length 40960000 : current length 0
Peer Grp List
Nbr List
Conf Peer List
Address Family specific Information

Command
History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**show ip bgp extcommunity-list**

View information on all routes with Extended Community attributes.

**Syntax**

```
show ip bgp [ipv4 unicast] extcommunity-list [list name]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 unicast</td>
<td>(OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.</td>
</tr>
<tr>
<td>list name</td>
<td>Enter the extended community list name you wish to view.</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege

**Usage Information**

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**show ip bgp filter-list**

View the routes that match the filter lists.

**Syntax**

```
show ip bgp [ipv4 unicast] filter-list as-path-name
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 unicast</td>
<td>(OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.</td>
</tr>
<tr>
<td>as-path-name</td>
<td>Enter the name of an AS-PATH.</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege
Table 8-6 defines the information displayed in Figure 8-12.

Table 8-6. Command Example fields: show ip bgp filter-list

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path source codes</td>
<td>Lists the path sources shown to the right of the last AS number in the Path column:</td>
</tr>
<tr>
<td></td>
<td>• i = internal route entry</td>
</tr>
<tr>
<td></td>
<td>• a = aggregate route entry</td>
</tr>
<tr>
<td></td>
<td>• c = external confederation route entry</td>
</tr>
<tr>
<td></td>
<td>• n = network route entry</td>
</tr>
<tr>
<td></td>
<td>• r = redistributed route entry</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router.</td>
</tr>
<tr>
<td></td>
<td>If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
show ip bgp flap-statistics

View flap statistics on BGP routes.

**Syntax**
show ip bgp [ipv4 unicast] flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-expression]

**Parameters**
- **ipv4 unicast** (OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.
- **ip-address** (OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
- **mask** (OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
- **filter-list as-path-name** (OPTIONAL) Enter the keyword filter-list followed by the name of a configured AS-PATH ACL.
- **regexp regular-expression** Enter a regular expression then use one or a combination of the following characters to match:
  - . = (period) any single character (including a white space)
  - * = (asterisk) the sequences in a pattern (0 or more sequences)
  - + = (plus) the sequences in a pattern (1 or more sequences)
  - ? = (question mark) sequences in a pattern (either 0 or 1 sequences).
  - You must enter an escape sequence (CTRL+v) prior to entering the regular expression.
  - [ ] = (brackets) a range of single-character patterns.
  - ( ) = (parenthesis) groups a series of pattern elements to a single element
  - { } = (braces) minimum and the maximum match count
  - ^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - $ = (dollar sign) the end of the output string.

**Command Modes**
EXEC
EXEC Privilege

**Example**

Figure 8-13. Command Example: show ip bgp flap-statistics

```
FTOS>show ip bgp flap
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network From Flaps Duration Reuse Path

FTOS>
```
Table 8-7 defines the information displayed in Figure 8-13.

Table 8-7. show ip bgp flap-statistics Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the network ID to which the route is flapping.</td>
</tr>
<tr>
<td>From</td>
<td>Displays the IP address of the neighbor advertising the flapping route.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Displays the number of times the route flapped.</td>
</tr>
<tr>
<td>Duration</td>
<td>Displays the hours:minutes:seconds since the route first flapped.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Displays the hours:minutes:seconds until the flapped route is available.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the flapping route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp inconsistent-as

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax

show ip bgp [ipv4 unicast] inconsistent-as

Command Modes

EXEC

EXEC Privilege

Example

Figure 8-14. Command Example: show ip bgp inconsistent-as (Partial)
Table 8-8.  show ip bgp inconsistent-as Command Example Fields

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router.</td>
</tr>
<tr>
<td></td>
<td>If 0.0.0.0 is listed in this column, then local routes exist in the routing</td>
</tr>
<tr>
<td></td>
<td>table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight.</td>
</tr>
</tbody>
</table>
| Path                   | Lists all the ASs the route passed through to reach the destination network.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**show ip bgp neighbors**

Enables you to view the information exchanged by BGP neighbors.

**Syntax**

```
show ip bgp [ipv4 unicast] neighbors [ip-address [advertised-routes | dampened-routes | detail | flap-statistics | routes | {received-routes [network [network-mask]]} | {denied-routes [network [network-mask]]}]
```

**Parameters**

- **ipv4 unicast** (OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.
- **ip-address** (OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.
- **advertised-routes** (OPTIONAL) Enter the keywords advertised-routes to view only the routes the neighbor sent.
- **dampened-routes** (OPTIONAL) Enter the keyword dampened-routes to view information on dampened routes from the BGP neighbor.
- **detail** (OPTIONAL) Enter the keyword detail to view neighbor-specific internal information for the IPv4 Unicast address family.
- **flap-statistics** (OPTIONAL) Enter the keyword flap-statistics to view flap statistics on the neighbor’s routes.
- **routes** (OPTIONAL) Enter the keywords routes to view only the neighbor’s feasible routes.
- **received-routes [network [network-mask]]** (OPTIONAL) Enter the keywords received-routes followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. **Note:** neighbor soft-reconfiguration inbound must be configured prior to viewing all the information received from the neighbors.
- **denied-routes [network [network-mask]]** (OPTIONAL) Enter the keywords denied-routes followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.
Command Modes

EXEC
EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 8-15. Command Example: show ip bgp neighbors on the S4810(Partial)

```
FTOS#show ip bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 23456, external link
BGP version 4, remote router ID 10.10.10.1
BGP state ESTABLISHED, in this state for 00:00:35
...Capabilities received from neighbor for IPv4 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  4_OCTECT_AS(65)
  ADD_PATH (69)
  CISCO_ROUTE_REFRESH(128)
```

Example 1

Figure 8-16. Command Example: show ip bgp neighbors (Partial)

```
FTOS#show ip bgp neighbors
BGP neighbor is 100.10.10.2, remote AS 200, external link
BGP version 4, remote router ID 192.168.2.101
BGP state ESTABLISHED, in this state for 00:16:12
Last read 00:00:12, last write 00:00:03
Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
  3 opens, 1 notifications, 1394 updates
  6 keepalives, 0 route refresh requests
Sent 48 messages, 0 in queue
  3 opens, 2 notifications, 0 updates
  43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds
Capabilities received from neighbor for IPv4 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)
Capabilities advertised to neighbor for IPv4 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  ROUTE_REFRESH(2)
  GRACEFUL_RESTART(64)
  CISCO_ROUTE_REFRESH(128)
Route map for incoming advertisements is test
Maximum prefix set to 4 with threshold 75
For address family: IPv4 Unicast
BGP table version 34, neighbor version 34
5 accepted prefixes consume 20 bytes
Prefix advertised 0, denied 4, withdrawn 0
Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 2; dropped 1
Last reset 00:18:21, due to Maximum prefix limit reached
```
**Example 2**  
**Figure 8-17. Command Example: show ip bgp neighbors advertised-routes**

FTOS#show ip bgp neighbors 192.14.1.5 advertised-routes

BGP table version is 74103, local router ID is 33.33.33.33  
Status codes: s suppressed, S stale, d damped, h history, * valid, > best  
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network  
Origin codes: i - IGP, e - EGP, ? - incomplete  

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*r 1.10.1.0/24</td>
<td>0.0.0.0</td>
<td>5000</td>
<td>32768</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>*r 1.11.0.0/16</td>
<td>0.0.0.0</td>
<td>5000</td>
<td>32768</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>.........</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*I 223.94.249.0/24</td>
<td>223.100.4.249</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*I 223.94.250.0/24</td>
<td>223.100.4.250</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*I 223.100.0.0/16</td>
<td>223.100.255.254</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>

Total number of prefixes: 74102

**Example 3**  
**Figure 8-18. Command Example: show ip bgp neighbors received-routes**

FTOS#show ip bgp neighbors 100.10.10.2 received-routes

BGP table version is 13, local router ID is 120.10.10.1  
Status codes: s suppressed, S stale, d damped, h history, * valid, > best  
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network, D - denied, S - stale  
Origin codes: i - IGP, e - EGP, ? - incomplete  

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 70.70.21.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.22.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.23.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.24.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>* 70.70.25.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>* 70.70.26.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>* 70.70.27.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>* 70.70.28.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>* 70.70.29.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
</tbody>
</table>

**Example 4**  
**Figure 8-19. Command Example: show ip bgp neighbors denied-routes**

FTOS#show ip bgp neighbors 100.10.10.2 denied-routes

4 denied paths using 205 bytes of memory  
BGP table version is 34, local router ID is 100.10.10.2  
Status codes: s suppressed, S stale, d damped, h history, * valid, > best  
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network, D - denied, S - stale  
Origin codes: i - IGP, e - EGP, ? - incomplete  

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 70.70.21.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.22.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.23.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.24.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
</tbody>
</table>

**Table 8-9. Command Example fields: show ip bgp neighbors**

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version (always version 4) and the remote router ID.</td>
</tr>
</tbody>
</table>
### Table 8-9. Command Example fields: show ip bgp neighbors

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP state</td>
<td>Displays the neighbor’s BGP state and the amount of time in hours:minutes:seconds it has been in that state.</td>
</tr>
<tr>
<td>Last read</td>
<td>This line displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• last read is the time (hours:minutes:seconds) the router read a message from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• hold time is the number of seconds configured between messages from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.</td>
</tr>
<tr>
<td>Received messages</td>
<td>This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Sent messages</td>
<td>The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Received updates</td>
<td>This line displays the number of BGP updates received and sent.</td>
</tr>
<tr>
<td>Soft reconfiguration</td>
<td>This line indicates that soft reconfiguration inbound is configured.</td>
</tr>
<tr>
<td>Minimum time</td>
<td>Displays the minimum time, in seconds, between advertisements.</td>
</tr>
<tr>
<td>(list of inbound and outbound policies)</td>
<td>Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.</td>
</tr>
<tr>
<td>For address family:</td>
<td>Displays IPv4 Unicast as the address family.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the which version of the primary BGP routing table the router and the neighbor are using.</td>
</tr>
<tr>
<td>accepted prefixes</td>
<td>Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.</td>
</tr>
<tr>
<td>Prefix advertised</td>
<td>Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.</td>
</tr>
<tr>
<td>Local host:</td>
<td>Displays the peering address of the local router and the TCP port number.</td>
</tr>
<tr>
<td>Foreign host:</td>
<td>Displays the peering address of the neighbor and the TCP port number.</td>
</tr>
</tbody>
</table>

**Related Commands**

- **show ip bgp** View the current BGP routing table.
show ip bgp next-hop

View all next hops (via learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

**Syntax**

```
show ip bgp next-hop
```

**Command Modes**

- EXEC
- EXEC Privilege

**Example**

```
Figure 8-20. Command Example: show ip bgp next-hop
```

```
FTOS>show ip bgp next-hop
Next-hop          Via                        RefCount  Cost  Flaps Time Elapsed
63.114.8.33       63.114.8.33, Gi 12/22       240984     0      0 00:18:25
63.114.8.34       63.114.8.34, Gi 12/22       135152     0      0 00:18:13
63.114.8.35       63.114.8.35, Gi 12/22            1     0      0 00:18:07
63.114.8.60       63.114.8.60, Gi 12/22       135155     0      0 00:18:11
FTOS>
```

**Table 8-10. Command Example fields: show ip bgp next-hop**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-hop</td>
<td>Displays the next-hop IP address.</td>
</tr>
<tr>
<td>Via</td>
<td>Displays the IP address and interface used to reach the next hop.</td>
</tr>
<tr>
<td>RefCount</td>
<td>Displays the number of BGP routes using this next hop.</td>
</tr>
<tr>
<td>Cost</td>
<td>Displays the cost associated with using this next hop.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Displays the number of times the next hop has flapped.</td>
</tr>
<tr>
<td>Time Elapsed</td>
<td>Displays the time elapsed since the next hop was learned. If the route is down, then this field displays time elapsed since the route went down.</td>
</tr>
</tbody>
</table>

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp paths

View all the BGP path attributes in the BGP database.

**Syntax**

```
show ip bgp paths [regexp regular-expression]
```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| regexp regular-expression | Enter a regular expression then use one or a combination of the following characters to match: 
  - . = (period) any single character (including a white space)
  - * = (asterisk) the sequences in a pattern (0 or more sequences)
  - + = (plus) the sequences in a pattern (1 or more sequences)
  - ? = (question mark) sequences in a pattern (either 0 or 1 sequences). You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.
  - [ ] = (brackets) a range of single-character patterns.
  - ( ) = (parenthesis) groups a series of pattern elements to a single element
  - {} = (braces) minimum and the maximum match count
  - ^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - $ = (dollar sign) the end of the output string.

Command Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>EXEC Privilege</td>
</tr>
</tbody>
</table>

Example

**Figure 8-21. Command Example: show ip bgp paths (Partial)**

FTOS#show ip bgp path
Total 16 Paths
Address Hash Refcount Metric Path
0x1efe7e5c 15 10000 32 ?
0x1efe7e1c 71 10000 23 ?
0x1efe7d8c 127 10000 22 ?
0x1efe7d8c 183 10000 43 ?
0x1efe7d9c 239 10000 42 ?
0x1efe7c9c 283 6 (102 103) ?
0x1efe7d1c 287 33620000 ?
0x1efe7d1c 295 10000 13 ?
0x1efe7c5c 339 6 (92 93) ?
0x1efe7cdc 351 10000 12 ?
0x1efe7c1c 395 6 (82 83) ?
0x1efe7bdc 451 6 (72 73) ?
0x1efe7b5c 491 78 0 ?
0x1efe7adb 883 2 120 i
0x1efe7adc 983 10000 33 ?
0x1efe7b9c 1003 6 0 i
FTOS#

**Table 8-11. Command Example fields: show ip bgp paths**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Displays the total number of BGP path attributes.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using this path attribute.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the MED attribute for this path attribute.</td>
</tr>
<tr>
<td>Path</td>
<td>Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.</td>
</tr>
</tbody>
</table>
show ip bgp paths as-path

View all unique AS-PATHs in the BGP database

**Syntax**

show ip bgp paths as-path

**Command Modes**

EXEC

EXEC Privilege

**Example**

**Figure 8-22. Command Example: show ip bgp paths as-path (Partial)**

<table>
<thead>
<tr>
<th>Address</th>
<th>Hash</th>
<th>Refcount</th>
<th>AS-Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1ea3c1ec</td>
<td>251</td>
<td>1</td>
<td>42</td>
</tr>
<tr>
<td>0x1ea3c25c</td>
<td>251</td>
<td>1</td>
<td>22</td>
</tr>
<tr>
<td>0x1ea3c1b4</td>
<td>507</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>0x1ea3c304</td>
<td>507</td>
<td>1</td>
<td>33</td>
</tr>
<tr>
<td>0x1ea3c10c</td>
<td>763</td>
<td>1</td>
<td>(92 93)</td>
</tr>
<tr>
<td>0x1ea3c144</td>
<td>763</td>
<td>1</td>
<td>{102 103}</td>
</tr>
<tr>
<td>0x1ea3c17c</td>
<td>763</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>0x1ea3c22c</td>
<td>763</td>
<td>1</td>
<td>32</td>
</tr>
<tr>
<td>0x1ea3c09c</td>
<td>764</td>
<td>1</td>
<td>{72 73}</td>
</tr>
<tr>
<td>0x1ea3c0d4</td>
<td>766</td>
<td>1</td>
<td>{82 83}</td>
</tr>
<tr>
<td>0x1ea3c224</td>
<td>1019</td>
<td>1</td>
<td>43</td>
</tr>
<tr>
<td>0x1ea3c294</td>
<td>1019</td>
<td>1</td>
<td>23</td>
</tr>
<tr>
<td>0x1ea3c02c</td>
<td>1021</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

**Table 8-12. Command Example fields: show ip bgp paths community**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using these AS-Paths.</td>
</tr>
<tr>
<td>AS-Path</td>
<td>Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces { } are AS_SET information.</td>
</tr>
</tbody>
</table>

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

**Syntax**

show ip bgp paths community

**Command Modes**

EXEC

EXEC Privilege
show ip bgp peer-group

Enables you to view information on the BGP peers in a peer group.

Syntax

show ip bgp [ipv4 unicast] peer-group [peer-group-name [detail | summary]]

Parameters

- **ipv4 unicast** (OPTIONAL) Enter the **ipv4 unicast** keywords to view information only related to ipv4 unicast routes.
- **peer-group-name** (OPTIONAL) Enter the name of a peer group to view information about that peer group only.
- **detail** (OPTIONAL) Enter the keyword **detail** to view detailed status information of the peers in that peer group.
- **summary** (OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group.

The output is the same as that found in **show ip bgp summary** command.
Command Modes

EXEC
EXEC Privilege

Example

Figure 8-24. Command Example: show ip bgp peer-group on the S4810 (Partial)

FTOS#show ip bgp peer-group
Peer-group pg1
BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
BGP neighbor is pg1
Number of peers in this group 4
Update packing has 4_OCTECT_AS support enabled
Peer-group members (* - outbound optimized):
  1.1.1.5
  1.1.1.6
  10.10.10.2*
  20.20.20.100

Figure 8-25. Command Example: show ip bgp peer-group (Partial)

FTOS#show ip bgp peer-group
Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
  12.1.1.2*
  12.1.1.3*
  12.1.1.4*
  12.1.1.5*
  12.1.1.6*
  12.2.1.2*
  12.2.1.3*
  12.2.1.4*
  12.2.1.5*
  12.2.1.6*
  12.3.1.2*
  12.3.1.3*
  12.3.1.4*
  12.3.1.5*
  12.3.1.6*
  12.4.1.2*
  12.4.1.3*
  12.4.1.4*
  12.4.1.5*
  12.4.1.6*

Table 8-14. Command Example fields: show ip bgp peer-group

<table>
<thead>
<tr>
<th>Line beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer-group</td>
<td>Displays the peer group’s name.</td>
</tr>
<tr>
<td>Administratively shut</td>
<td>Displays the peer group’s status if the peer group is not enabled. If the peer group is enabled, this line is not displayed.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version supported.</td>
</tr>
<tr>
<td>Minimum time</td>
<td>Displays the time interval between BGP advertisements.</td>
</tr>
<tr>
<td>For address family</td>
<td>Displays IPv4 Unicast as the address family.</td>
</tr>
<tr>
<td>BGP neighbor</td>
<td>Displays the name of the BGP neighbor.</td>
</tr>
</tbody>
</table>
show ip bgp regexp

Display the subset of BGP routing table matching the regular expressions specified.

**Syntax**

```
show ip bgp regexp regular-expression [character]
```

**Parameters**

- `regular-expression [character]` Enter a regular expression then use one or a combination of the following characters to match:
  - `.` = (period) any single character (including a white space)
  - `*` = (asterisk) the sequences in a pattern (0 or more sequences)
  - `+` = (plus) the sequences in a pattern (1 or more sequences)
  - `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
  - `[ ]` = (brackets) a range of single-character patterns.
  - `( )` = (parenthesis) groups a series of pattern elements to a single element
  - `{ }` = (braces) minimum and the maximum match count
  - `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - `$` = (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege
Example Figure 8-26. Command Example: show ip bgp regexp (Partial)

```
FTOS#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric  LocPrf Weight Path
+> I 3.0.0.0/8 1.1.1.2 0 100 0 2914 1299 80 i
+> I 4.0.0.0/8 1.1.1.2 0 100 0 2914 3356 1
+> I 4.17.225.0/24 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 11853 6496
+> I 4.17.226.0/23 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 11853 6496
+> I 4.17.251.0/24 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 11853 6496
+> I 4.17.252.0/23 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 11853 6496
+> I 4.19.2.0/23 1.1.1.2 0 100 0 2914 701 6167 6167 6167 i
+> I 4.19.16.0/23 1.1.1.2 0 100 0 2914 701 6167 6167 6167 i
+> I 4.21.80.0/22 1.1.1.2 0 100 0 2914 174 4200 16559 1
+> I 4.21.82.0/24 1.1.1.2 0 100 0 2914 174 4200 16559 1
+> I 4.21.252.0/23 1.1.1.2 0 100 0 2914 701 6389 8063 19198 1
+> I 4.23.180.0/24 1.1.1.2 0 100 0 2914 3561 6128 30576 1
+> I 4.36.200.0/21 1.1.1.2 0 100 0 2914 14742 11854 14135 1
+> I 4.67.64.0/22 1.1.1.2 0 100 0 2914 11608 19281 1
+> I 4.78.32.0/21 1.1.1.2 0 100 0 2914 3491 29748 1
+> I 6.1.0.0/16 1.1.1.2 0 100 0 2914 701 668 i
+> I 6.2.0.0/22 1.1.1.2 0 100 0 2914 701 668 i
+> I 6.3.0.0/18 1.1.1.2 0 100 0 2914 701 668 i
```

Table 8-15. Command Example fields: show ip bgp regexp

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP router’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the AS paths the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show ip bgp summary

Enables you to view the status of all BGP connections.

Syntax show ip bgp [ipv4 unicast] summary

Command Modes EXEC
EXEC Privilege
Figure 8-27. Command Example: show ip bgp summary

```
FTOS#show ip bgp summary
BGP router identifier 120.10.10.1, local AS number 100
BGP table version is 34, main routing table version 34
9 network entry(s) using 1372 bytes of memory
4 denied paths using 164 bytes of memory
BGP-RIB over all using 385 bytes of memory
2 BGP path attribute entry(s) using 168 bytes of memory
1 BGP AS-PATH entry(s) using 59 bytes of memory
1 BGP community entry(s) using 43 bytes of memory
2 neighbor(s) using 7322 bytes of memory
```

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/Pfx</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.10.10.2</td>
<td>200</td>
<td>46</td>
<td>41</td>
<td>34</td>
<td>0</td>
<td>0</td>
<td>00:14:33</td>
<td>5</td>
</tr>
<tr>
<td>120.10.10.2</td>
<td>300</td>
<td>40</td>
<td>47</td>
<td>34</td>
<td>0</td>
<td>0</td>
<td>00:37:10</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 8-16. Command Example fields: show ip bgp summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP router identifier</td>
<td>Displays the local router ID and the AS number.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the BGP table version and the main routing table version.</td>
</tr>
<tr>
<td>network entries</td>
<td>Displays the number of network entries and route paths and the amount of memory used to process those entries.</td>
</tr>
<tr>
<td>paths</td>
<td>Displays the number of paths and the amount of memory used.</td>
</tr>
<tr>
<td>denied paths</td>
<td>Displays the number of denied paths and the amount of memory used.</td>
</tr>
<tr>
<td>BGP path attribute entries</td>
<td>Displays the number of BGP path attributes and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP AS-PATH entries</td>
<td>Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP community entries</td>
<td>Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The <code>show ip bgp community</code> command provides more details on the COMMUNITY attributes.</td>
</tr>
<tr>
<td>Dampening enabled</td>
<td>Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Displays the BGP neighbor address.</td>
</tr>
<tr>
<td>AS</td>
<td>Displays the AS number of the neighbor.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Displays the number of BGP messages that neighbor received.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Displays the number of BGP messages that neighbor sent.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Displays the version of the BGP table that was sent to that neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Displays the number of messages from that neighbor waiting to be processed.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Displays the number of messages waiting to be sent to that neighbor.</td>
</tr>
<tr>
<td></td>
<td>If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.</td>
</tr>
</tbody>
</table>
Command Example fields: show ip bgp summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up/Down</td>
<td>Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed. The output format is:</td>
</tr>
<tr>
<td></td>
<td><strong>Time Established</strong>----------<strong>Display Example</strong></td>
</tr>
<tr>
<td></td>
<td>&lt; 1 day ------------------------ 00:12:23 (hours:minutes:seconds)</td>
</tr>
<tr>
<td></td>
<td>&lt; 1 week ---------------------- 1d21h (Days:Hours)</td>
</tr>
<tr>
<td></td>
<td>&gt; 1 week ---------------------- 11w2d (Weeks:Days)</td>
</tr>
<tr>
<td>State/Pfxrd</td>
<td>If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the neighbor maximum-prefix command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm) When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.</td>
</tr>
</tbody>
</table>

Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

**show running-config bgp**

Use this feature to display the current BGP configuration.

**Syntax**

```
show running-config bgp
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

**timers bgp**

Adjust BGP Keep Alive and Hold Time timers.

**Syntax**

```
timers bgp keepalive holdtime
```

To return to the default, enter **no timers bgp**.
Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). FTOS MBGP is implemented as per IETF RFC 1858.

The MBGP commands are:

- `debug ip bgp dampening`
- `distance bgp`
- `show ip bgp dampened-paths`

### debug ip bgp dampening

View information on routes being dampened.

**Syntax**

```
debug ip bgp ipv4 multicast dampening
```

To disable debugging, enter no `debug ip bgp ipv4 multicast dampening`

**Parameters**

- `dampening`
  - Enter the keyword `dampening` to clear route flap dampening information.

**Command Modes**

EXEC Privilege

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**distance bgp**

Define an administrative distance for routes.

**Syntax**

```
distance bgp external-distance internal-distance local-distance
```

To return to default values, enter `no distance bgp`.

**Parameters**

- **external-distance**: Enter a number to assign to routes learned from a neighbor external to the AS.
  - Range: 1 to 255
  - Default: 20

- **internal-distance**: Enter a number to assign to routes learned from a router within the AS.
  - Range: 1 to 255
  - Default: 200

- **local-distance**: Enter a number to assign to routes learned from networks listed in the `network` command.
  - Range: 1 to 255
  - Default: 200

**Defaults**

- `external-distance = 20`
- `internal-distance = 200`
- `local-distance = 200`

**Command Modes**

ROUTER BGP (conf-router_bgp_af)

**Caution:** Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

**Usage Information**

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

**show ip bgp dampened-paths**

View BGP routes that are dampened (non-active).

**Syntax**

```
show ip bgp [ipv4 unicast] dampened-paths
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>
The following describes the show ip bgp dampened-paths command in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the network ID to which the route is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>Displays the IP address of the neighbor advertising the dampened route.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Displays the hour:minutes:seconds until the dampened route is available.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS>show ip bgp dampened-paths
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
Network From Reuse Path
```

**BGP Extended Communities (RFC 4360)**

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute. It provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new “Type” field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

The BGP Extended Community commands are:

- `set extcommunity rt`
- `set extcommunity soo`
- `show ip bgp paths extcommunity`
- `show ip extcommunity-list`

**set extcommunity rt**

Use this feature to set Route Origin community attributes in Route Map.

**Syntax**

```plaintext
set extcommunity rt {as4 ASN4:NN [non-trans] | ASN:NNNN [non-trans] | IPADDR:NN [non-trans]} [additive]
```

To delete the Route Origin community, use the `no set extcommunity` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as4 ASN4:NN</td>
<td>Enter the keyword as4 followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).</td>
</tr>
<tr>
<td>ASN:NNNN</td>
<td>Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).</td>
</tr>
<tr>
<td>IPADDR:NN</td>
<td>Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).</td>
</tr>
</tbody>
</table>
set extcommunity soo

Use this feature to set extended community site-of-origin in Route Map.

Syntax

```plaintext
set extcommunity soo \{as4 ASN4:NN | ASN:NNNN | IPADDR:NN [non-trans]\}
```

To delete the site-of-origin community, use the no set extcommunity command.

Parameters

- **as4 ASN4:NN**
  - Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format "ASN4:NN (4-byte AS number:2-byte community value)".

- **ASN:NNNN**
  - Enter the 2-octet AS specific extended community number in the format "ASN:NNNN (2-byte AS number:4-byte community value)".

- **IPADDR:NN**
  - Enter the IP address specific extended community in the format "IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value)".

- **non-trans**
  - (OPTIONAL) Enter the keyword `non-trans` to indicate a non-transitive BGP extended community.

Defaults

No default behavior or values

Command Modes

ROUTE MAP (config-route-map)

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, we can define the behavior as:

- If `rt` option comes before `soo`, with or without `additive` option, then `soo` overrides the communities set by `rt`
- If `rt` options comes after `soo`, without the `additive` option, then `rt` overrides the communities set by `soo`
- If `rt` with `additive` option comes after `soo`, then `rt` adds the communities set by `soo`
show ip bgp paths extcommunity

Use this feature to display all BGP paths having extended community attributes.

**Syntax**  
show ip bgp paths extcommunity

**Command Modes**  
EXEC  
EXEC Privilege

**Example**  

```
FTOS#show ip bgp paths extcommunity
Total 1 Extended Communities
Address          Hash    Refcount    Extended Community
0x41d57024       12272    1           RT:7:200 SoO:5:300 SoO:0.0.0.3:1285
FTOS#
```

**Table 8-17. Command Example fields: show ip bgp paths community**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using these extended communities.</td>
</tr>
<tr>
<td>Community</td>
<td>Displays the extended community attributes in this BGP path.</td>
</tr>
</tbody>
</table>

**Command History**  
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show ip extcommunity-list

Display the IP extended community list.

**Syntax**  
show ip extcommunity-list [word]

**Parameters**  

<table>
<thead>
<tr>
<th>word</th>
<th>Enter the name of the extended community list you want to view.</th>
</tr>
</thead>
</table>

**Defaults**  
None.

**Command Modes**  
EXEC  
EXEC Privilege
IPv6 BGP Commands

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on the MXL 10/40GbE Switch IO Module.

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

- `bgp soft-reconfig-backup`
- `clear ip bgp ipv6 unicast soft`
- `debug ip bgp ipv6 unicast soft-reconfiguration`
- `ipv6 prefix-list`
- `show ipv6 prefix-list`

`bgp soft-reconfig-backup`
To avoid the peer from resending messages, use this command only when route-refresh is not negotiated.

**Syntax**
```
bgp soft-reconfig-backup
```

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

**Defaults**
Disabled.

**Command Modes**
ROUTER BGP

**Usage Information**
When you enable soft-reconfiguration for a neighbor and you execute the clear ip bgp soft in command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the clear ip bgp soft in command), BGP sends a route-refresh request to the neighbor and receives all of the peer’s updates.

**Related Commands**
- `clear ip bgp` Activates inbound policies without resetting the BGP TCP session.
clear ip bgp ipv6 unicast soft
Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

Syntax
```
clear ip bgp {* | as-number | ipv4-neighbor-addr | ipv6-neighbor-addr | peer-group name} ipv6 unicast soft [in | out]
```

Parameters
- `*` Clear and reapply policies for all BGP sessions.
- `as-number` Clear and reapply policies for all neighbors belonging to the AS. The range is from 0 to 65535 (2 Byte), from 1 to 4294967295 (4 Byte), or from 0.1 to 0.65535.65535 (Dotted format).
- `ipv4-neighbor-addr | ipv6-neighbor-addr` Clear and reapply policies for a neighbor.
- `peer-group name` Clear and reapply policies for all BGP routers in the specified peer group.
- `ipv6 unicast soft` Clear and reapply policies for all IPv6 unicast routes.
- `in` Reapply only inbound policies.
  - Note: If you enter soft, without an in or out option, both inbound and outbound policies are reset.
- `out` Reapply only outbound policies.
  - Note: If you enter soft, without an in or out option, both inbound and outbound policies are reset.

Command Modes
- EXEC Privilege

debug ip bgp ipv6 unicast soft-reconfiguration
Enable soft-reconfiguration debugging for IPv6 unicast routes.

Syntax
```
debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration
```

To disable debugging, use the no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration command.

Parameters
- `ipv4-address` Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
- `ipv6-address` Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
- `peer-group-name` Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
- `ipv6 unicast` Debug soft reconfiguration for IPv6 unicast routes.

Defaults
- Disabled.
**ipv6 prefix-list**

Configure an IPv6 prefix list.

**Syntax**

`ipv6 prefix-list prefix-list name`

**Parameters**

- `prefix-list name`: Enter the name of the prefix list.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `show ipv6 prefix-list`: View the selected IPv6 prefix list.

**show ipv6 prefix-list**

Displays the specified IPv6 prefix list.

**Syntax**

`show ipv6 prefix-list detail {prefix-list name} | summary`

**Parameters**

- `detail`: Display a detailed description of the selected IPv6 prefix list.
- `prefix-list name`: Enter the name of the prefix list. Maximum 140 characters.
- `summary`: Display a summary of RPF routes.

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `ipv6 prefix-list`: Configure an IPv6 prefix-list.
# IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). FTOS MBGP is implemented as per IETF RFC 1858. The MBGP commands are:

- `show ipv6 mbgproutes`

## show ipv6 mbgproutes

Display the selected IPv6 MBGP route or a summary of all MBGP routes in the table.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>show ipv6 mbgproutes ipv6-address prefix-length</th>
<th>summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td><code>ipv6-address prefix-length</code> (OPTIONAL) Enter the IPv6 address in the <code>x:x:x:x::x</code> format followed by the prefix length in the <code>/x</code> format. Range: /0 to /128. The <code>::</code> notation specifies successive hexadecimal fields of zeros.</td>
<td>Display a summary of RPF routes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>EXEC</th>
</tr>
</thead>
</table>

**Command History**

- **Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.
Content Addressable Memory (CAM)

Overview

⚠️ Warning: If you are using these features for the first time, contact Dell Networking Technical Assistance Center (TAC) for guidance. For information on contacting Dell Networking TAC, visit the Dell Networking website at www.force10networks.com/support.

CAM Profile Commands

The content addressable memory (CAM) profiling feature allows you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 forwarding information base (FIB) entries when the system is deployed as a switch.
- Configure more Layer 3 FIB entries when the system is deployed as a router.
- Configure more access control list (ACLs).
- Optimize the virtual local area network (VLAN) ACL group feature, which permits group VLANs for IP egress ACLs.

Important Points to Remember

- The Dell Networking operating software (FTOS) versions 7.8.1.0 and later support CAM allocations on the MXL 10/40GbE Switch IO Module.
- The CAM configuration is applied to entire system when you use CONFIGURATION mode commands. You must save the running-configuration to affect the change.
- When budgeting your CAM allocations for ACLs and quality of service (QoS) configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, transmission control protocol (TCP) and user datagram protocol (UDP) rules with port range options might require more than one CAM entry.
- You MUST save your changes and reboot the system for CAM profiling or allocations to take effect.

The CAM Profiling commands are:

- `cam-acl (Configuration)`
- `cam-optimization`
- `show cam-acl`
Content Addressable Memory (CAM)

- show cam-acl-egress

# cam-acl (Configuration)

Select the default CAM allocation settings or reconfigure new CAM allocation for Layer 2, IPv4 and IPv6 ACLs, Layer 2 and Layer 3 (IPv4) QoS, Layer 2 Protocol Tunneling (L2PT), IP and MAC source address validation for DHCP, Ethernet Connectivity Fault Management (CFM) ACLs, and Policy-based Routing (PBR).

**Syntax**

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number ipv4qos number l2qos number l2pt number ipmacacl number [vman-qos | vman-qos-dual- number | vman-qos-dual-fp number] ipv4pbr number} ecfmacl number fcoeacl number iscsioptacl number
```

**Parameters**

- `default` Use the default CAM profile settings, and set the CAM as follows.
  - L3 ACL (ipv4acl): 2
  - L2 ACL(l2acl): 2
  - IPv6 L3 ACL(ipv6Acl): 0
  - L3 QoS (ipv4qos): 2
  - L2 QoS(L2Qos): 1
  - L2PT (L2PT): 0
  - MAC ACL (IpMacAcl): 0
  - VmanDualQos: 0
  - EcfmAcl: 0
  - FcoeAcl: 4
  - iscsioptAcl: 2

- `l2acl number ipv4acl number ipv6acl number l2qos number, l2pt number ipmacacl number ecfmacl number [vman-qos | vman-qos-dual- number | vman-qos-dual-fp number] ipv4pbr number` Allocate space to each CAM region.
  - Enter the CAM profile name followed by the amount of CAM space to be allotted.
  - The total space allocated must equal 13.
  - The range for `ipv4acl` is 1 to 4.
  - The ipv4acl range must be a factor of 2.
  - The vman-qos-dual-fp number must be entered as a multiple of 4.

**Command Modes**

- **CONFIGURATION**

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must save the new CAM settings to the startup-config (write-mem or copy run start) then reload the system for the new settings to take effect.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these cannot be reallocated. The `ipv4acl` profile range is 1-4.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

On the MXL 10/40GbE Switch IO Module, there can be only one odd number of Blocks in the CLI configuration; the other Blocks must be in factors of two. For example, a CLI configuration of 5+4+2+1+1 Blocks is not supported; a configuration of 6+4+2+1 Blocks is supported.
Ranges for the CAM profiles are 1-10, except for the ipv6acl profile which is 0-10. The ipv6acl allocation must be a factor of two (2, 4, 6, 8, 10).

**cam-optimization**

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

- **Syntax**
  ```
  cam-optimization [qos]
  ```

- **Parameters**
  - `qos` Optimize CAM usage for Quality of Service (QoS)

- **Command Modes**
  - CONFIGURATION

- **Defaults**
  - Disabled

- **Command History**
  - Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

- **Usage Information**
  - When this command is enabled, if a Policy Map containing classification rules (ACL and/or dscp/ip-precedence rules) is applied to more than one physical interface on the same port pipe, only a single copy of the policy will be written (only one FP entry is used).

  **Note:** An ACL may still require more that a single FP entry, regardless of the number of interfaces. Refer to the *IP Access Control Lists, Prefix Lists, and Route-map in the FTOS Configuration Guide* for complete description.

**show cam-acl**

Display the details of the CAM profiles on the chassis and all stack units.

- **Syntax**
  ```
  show cam-acl
  ```

- **Defaults**
  - none

- **Command Modes**
  - EXEC Privilege

- **Command History**
  - Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

- **Usage Information**
  - The display reflects the settings implemented with the cam-acl command.
Example

**Figure 9-1. show cam-acl (default) Command Example**

```
FTOS#show cam-acl
-- Chassis Cam ACL --
   Current Settings (in block sizes)
  L2Acl :  6
  Ipv4Acl :  2
  Ipv6Acl :  0
  Ipv4Qos :  2
  L2Qos :  1
  L2PT :  0
  IpMacAcl :  0
  VmanQos :  0
  VmanDualQos :  0
  EcfmAcl :  0
  FcoeAcl :  0
  iscsiOptAcl :  2
-- Stack unit 5 --
   Current Settings (in block sizes)
  L2Acl :  6
  Ipv4Acl :  2
  Ipv6Acl :  0
  Ipv4Qos :  2
  L2Qos :  1
  L2PT :  0
  IpMacAcl :  0
  VmanQos :  0
  VmanDualQos :  0
  EcfmAcl :  0
  FcoeAcl :  0
  iscsiOptAcl :  2
FTOS#
```

**Figure 9-2. show cam-acl (non-default) Command Example**

```
FTOS#show cam-acl
-- Chassis Cam ACL --
   Current Settings (in block sizes)
  L2Acl :  2
  Ipv4Acl :  2
  Ipv6Acl :  2
  Ipv4Qos :  2
  L2Qos :  2
  L2PT :  1
  IpMacAcl :  2
  VmanQos :  0
  VmanDualQos :  0
  Ipv4pbr :  0
-- Line card 4 --
   Current Settings (in block sizes)
  L2Acl :  5
  Ipv4Acl :  5
  Ipv6Acl :  1
  Ipv4Qos :  1
  L2Qos :  1
  L2PT :  0
  IpMacAcl :  0
  VmanQos :  0
  VmanDualQos :  0
  Ipv4pbr :  0
FTOS#
```
**show cam-acl-egress**

Display the details of the FP groups allocated for the egress ACL.

**Syntax**

```
show cam-acl-egress
```

**Defaults**

none

**Command Modes**

EXEC

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The display reflects the settings implemented with the `cam-acl-egress` command.

**Example**

```
Figure 9-3. show cam-acl-egress (default) Command Example

FTOS#show cam-acl-egress

-- Chassis Egress Cam ACL --
Current Settings (in block sizes)
L2Acl : 1
Ipv4Acl : 1
Ipv6Acl : 2

-- Stack unit 5 --
Current Settings (in block sizes)
L2Acl : 1
Ipv4Acl : 1
Ipv6Acl : 2

FTOS#
```
Control Plane Policing (CoPP)

Overview

The CoPP commands are supported on the Dell Networking MXL 10/40GbE Switch IO Module.

Commands

- control-plane-cpuqos
- service-policy rate-limit-cpu-queues
- service-policy rate-limit-protocols
- show cpu-queue rate cp
- show ip protocol-queue-mapping
- show ipv6 protocol-queue-mapping
- show mac protocol-queue-mapping

control-plane-cpuqos

Enter control-plane mode and configure the switch to manage control-plane traffic.

Syntax

control-plane-cpuqos

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

service-policy rate-limit-cpu-queues

Apply a policy map for the system to rate limit control traffic on a per-queue basis.

Syntax

service-policy rate-limit-cpu-queues policy-name

Parameters

- **policy-name**
  
  Enter the service-policy name in a string up to 32 characters.

Defaults

Not configured.
### Command Modes

| Command Modes | CONTROL-PLANE-CPUQOS |

### Command History

| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |

### Usage Information

Create a policy-map by associating a queue number with the qos-policy.

Create QoS policies prior to enabling this command.

For CoPP, do not use the keywords cpu-qos when creating qos-policy-input.

### Related Commands

<table>
<thead>
<tr>
<th>qos-policy-input</th>
<th>Create a QoS input policy map.</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map</td>
<td>Create a QoS class map.</td>
</tr>
<tr>
<td>policy-map-input</td>
<td>Create an input policy map.</td>
</tr>
</tbody>
</table>

---

### service-policy rate-limit-protocols

Apply a policy for the system to rate limit control protocols on a per-protocol basis.

#### Syntax

```
service-policy rate-limit-protocols policy-name
```

#### Parameters

- **policy-name**: Enter the service-policy name, in a string up to 32 characters.

#### Defaults

Not configured.

#### Command Modes

| Command Modes | CONTROL-PLANE-CPUQOS |

#### Command History

| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |

#### Usage Information

This command applies the service-policy based on the type of protocol defined in the ACL rules.

Create ACL and QoS policies prior to enabling this command.

For CoPP, do not use the keywords cpu-qos when creating qos-policy-input.

#### Related Commands

<table>
<thead>
<tr>
<th>ip access-list extended</th>
<th>Create an extended IP ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 access-list</td>
<td>Create an IPv6 ACL</td>
</tr>
<tr>
<td>mac access-list extended</td>
<td>Create an extended MAC ACL.</td>
</tr>
<tr>
<td>qos-policy-input</td>
<td>Create a QoS input policy map.</td>
</tr>
<tr>
<td>class-map</td>
<td>Create a QoS class map.</td>
</tr>
<tr>
<td>policy-map-input</td>
<td>Create an input policy map.</td>
</tr>
</tbody>
</table>

---

### show cpu-queue rate cp

Display the rates for each queue.

#### Syntax

```
show cpu-queue rate cp
```

---

250 | Control Plane Policing (CoPP)
Defaults: Not configured.

Command Modes: EXEC Privilege

Command History:

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information:

This command applies the service-policy based on the type of protocol defined in the ACL rules.

Create ACL and QoS policies prior to enabling this command.

Example:

```
FTOS# show cpu-queue rate cp
Service-Queue Rate (PPS)
-------------  -----------
Q0            1300
Q1            300
Q2            300
Q3            300
Q4            2000
Q5            400
Q6            400
Q7            1100
FTOS#
```

```
show ip protocol-queue-mapping
Display the queue mapping for each configured protocol.

Syntax:
show ip protocol-queue-mapping

Defaults: Not configured.

Command Modes: EXEC Privilege

Command History:

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example:

```
FTOS# show ip protocol-queue-mapping
Protocol   Src-Port   Dst-Port   TcpFlag  Queue   EgPort     Rate (kbps)
--------   --------   --------   -------  -----   ------     -----------
TCP (BGP)     any/179    179/any    _        Q6      CP          100
UDP (DHCP)    67/68      68/67      _        Q6/Q5   CP          _
UDP (DHCP-R)  67         67         _        Q6      CP          _
TCP (FTP)     any        21         _        Q6      CP          _
ICMP         any        any        _        Q6      CP          _
IGMP          any        any        _        Q7      CP          _
TCP (MSDP)    any/639    639/any    _        Q6      CP          _
UDP (NTP)     any        123        _        Q6      CP          _
OSPF          any        any        _        Q7      CP          _
PIM           any        any        _        Q7      CP          _
UDP (RIP)     any        520        _        Q7      CP          _
TCP (SSH)     any        22         _        Q6      CP          _
TCP (TELNET)  any        23         _        Q6      CP          _
VRRP          any        any        _        Q7      CP          _
FTOS#
```
### show ipv6 protocol-queue-mapping

Display the queue mapping for each configured IPv6 protocol.

**Syntax**

```
show ipv6 protocol-queue-mapping
```

**Defaults**

Not configured.

**Command Modes**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
FTOS# show ipv6 protocol-queue-mapping

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Src-Port</th>
<th>Dst-Port</th>
<th>TcpFlag</th>
<th>Queue</th>
<th>EgPort</th>
<th>Rate (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP (BGP)</td>
<td>any/179</td>
<td>179/any</td>
<td>_</td>
<td>Q6</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>ICMP</td>
<td>any</td>
<td>any</td>
<td>_</td>
<td>Q6</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>VRRP</td>
<td>any</td>
<td>any</td>
<td>_</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
</tbody>
</table>

FTOS#
```

### show mac protocol-queue-mapping

Display the queue mapping for the MAC protocols.

**Syntax**

```
show mac protocol-queue-mapping
```

**Defaults**

Not configured.

**Command Modes**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
FTOS# show mac protocol-queue-mapping

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Destination Mac</th>
<th>EtherType</th>
<th>Queue</th>
<th>EgPort</th>
<th>Rate (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>any</td>
<td>0x0806</td>
<td>Q5/Q6</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>FRRP</td>
<td>01:01:e8:00:00:10/11</td>
<td>any</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>LACP</td>
<td>01:80:c2:00:00:02</td>
<td>0x8809</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>LLDP</td>
<td>any</td>
<td>0x88cc</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>GVRP</td>
<td>01:80:c2:00:00:21</td>
<td>any</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>STP</td>
<td>01:80:c2:00:00:00</td>
<td>any</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td>ISIS</td>
<td>01:80:c2:00:00:14/15</td>
<td>any</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
<tr>
<td></td>
<td>09:00:2b:00:00:04/05</td>
<td>any</td>
<td>Q7</td>
<td>CP</td>
<td>_</td>
</tr>
</tbody>
</table>

FTOS#
```
Data Center Bridging

Overview

Data center bridging (DCB) refers to a set of IEEE Ethernet enhancements that provide data centers with a single, robust, converged network to support multiple traffic types, including LAN, server, and storage traffic.

The Dell Networking operating software (FTOS) commands for data center bridging features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the Data Center Bridging Exchange (DCBX) protocol. CLI commands for individual DCB features are as follows:

DCB Command

- dcb-enable

PFC Commands

- dcb-input
- dcb-policy input
- dcb-policy input stack-unit stack-ports all
- dcb stack-unit all pfc-buffering pfc-port-count pfc-queues
- dcb stack-unit pfc-buffering pfc-port pfc-queues
- description
- pfc link-delay
- pfc mode on
- pfc priority
- pfc no-drop queues
- show dcb
- show interface pfc
- show interface pfc statistics
- show qos priority-groups
- show stack-unit stack-ports pfc detail
ETS Commands

- bandwidth-percentage
- dcb-output
- dcb-policy output
- dcb-policy output stack-unit stack-ports all
- description
- ets mode on
- priority-list
- priority-group
- priority-group qos-policy
- qos-policy-output ets
- scheduler
- set-pgid
- show interface ets
- show qos dcb-output
- show stack-unit stack-ports ets detail

DCBX Commands

- advertise dcbx-appln-tlv
- advertise dcbx-tlv
- dcbx version
- dcbx port-role
- fcoe priority-bits
- iscsi priority-bits
- debug dcbx
- show interface dcbx detail

advertise dcbx-appln-tlv

On a DCBX port with a manual role, configure the application priority TLVs advertised on the interface to DCBX peers.

Syntax

advertise dcbx-appln-tlv {fcoe | iscsi}

To remove the application priority TLVs, use the no advertise dcbx-appln-tlv {fcoe | iscsi} command.

Parameters

| {fcoe | iscsi} | Enter the application priority TLVs, where: |
|---------------|------------------------------------------|
|               | • fcoe: enables the advertisement of FCoE in application priority TLVs. |
|               | • iscsi: enables the advertisement of iSCSI in application priority TLVs. |

Defaults

Application priority TLVS are enabled to advertise FCoE and iSCSI.

Command Modes

PROTOCOL LLDP
advertise dcbx-tlv

On a DCBX port with a manual role, configure the PFC and ETS TLVs advertised to DCBX peers.

Syntax
advertise dcbx-tlv {ets-conf | ets-reco | pfc} [ets-conf | ets-reco | pfc] [ets-conf | ets-reco | pfc]

To remove the advertised ETS TLVs, use the no advertise dcbx-tlv command.

Parameters
(ets-conf | ets-reco | pfc) Enter the PFC and ETS TLVs to be advertised, where:
• ets-conf: enables the advertisement of ETS configuration TLVs.
• ets-reco: enables the advertisement of ETS recommend TLVs.
• pfc: enables the advertisement of PFC TLVs.

Defaults
All PFC and ETS TLVs are advertised.

Command Modes
PROTOCOL LLDP

Usage Information
You can configure the transmission of more than one TLV type at a time; for example: advertise dcbx-tlv ets-conf ets-reco.

You can enable ETS recommend TLVs (ets-reco) only if ETS configuration TLVs (ets-conf) are enabled. To disable TLV transmission, use the no form of the command; for example, no advertise dcbx-tlv pfc ets-reco.

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the show interface dcbx detail command.

bandwidth-percentage

Configure the bandwidth percentage allocated to priority traffic in port queues.

Syntax
bandwidth-percentage percentage

To remove the configured bandwidth percentage, use the no bandwidth-percentage command.

Parameters
percentage (Optional) Enter the bandwidth percentage.
The percentage range is 1 to 100% in units of 1%.
By default, equal bandwidth is assigned to each port queue and each dot1p priority in a priority group. Use the `bandwidth-percentage` command to configure bandwidth amounts in associated dot1p queues. When specified bandwidth is assigned to some port queues and not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to unassigned non-strict priority queues in the priority group. The sum of the allocated bandwidth to all queues in a priority group should be 100% of the bandwidth on the link.

ETS-assigned bandwidth allocation applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If both are configured, the configured bandwidth allocation will be ignored for priority-group traffic when you apply the output policy on an interface.

By default, equal bandwidth is assigned to each priority group in the ETS output policy applied to an egress port if no bandwidth allocation is configured. The sum of configured bandwidth allocation to dot1p priority traffic in all ETS priority groups must be 100%. You must allocate at least 1% of the total bandwidth to each priority group and queue. If bandwidth is assigned to some priority groups but not to others, the remaining bandwidth (100% minus assigned bandwidth amount) is equally distributed to non-strict-priority groups which have no configured scheduler.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos-policy-output ets</td>
<td>Create a QoS output policy.</td>
</tr>
<tr>
<td>scheduler</td>
<td>Schedule priority traffic in port queues.</td>
</tr>
</tbody>
</table>

**dcb-enable**

Enable DCB.

**Syntax**

```plaintext
dcb enable
```

To disable DCB, use the no `dcb enable` command.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

DCB is not supported if link-level flow control is enabled on one or more interfaces.
**dcb-input**

Create a DCB input policy to apply pause or flow control for specified priorities using a configure delay time.

**Syntax**

```plaintext
dcb-input policy-name
```

To delete the DCB input policy, use the `no dcb-input` command.

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-name</code></td>
<td>Maximum: 32 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

As soon as you apply a DCB policy with PFC enabled on an interface, DCBX starts exchanging information with PFC-enabled peers. The IEEE802.1Qbb, CEE, and CIN versions of PFC TLV are supported. DCBX also validates PFC configurations received in TLVs from peer devices.

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, you must also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (see `pfc no-drop queues`).

To remove a DCB input policy, including the PFC configuration it contains, enter the `no dcb-input policy-name` command in interface configuration mode.

**Related Commands**

- `dcb-policy input` — Apply the input policy with the PFC configuration.

**dcb-output**

Create a DCB output policy to associate an ETS configuration with priority traffic.

**Syntax**

```plaintext
dcb-output policy-name
```

To remove the ETS output policy from an interface, use the `no dcb-policy output` command.

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
</table>
| `policy-name` | Enter the DCB output policy name.  
               | Maximum: 32 alphanumeric characters.        |

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Usage Information
Create a DCB output policy to associate a priority group with an ETS output policy with scheduling and bandwidth configuration. You can apply a DCB output policy on multiple egress ports. When you apply an ETS output policy on an interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies.

The ETS configuration associated with 802.1 priority traffic in a DCB output policy is used in DCBX negotiation with ETS peers.

Related Commands

- **dcb-policy output** Apply the output policy.

---

**dcb-policy input**

Apply the input policy with the PFC configuration to an ingress interface.

**Syntax**

dcb-policy input *policy-name*

To delete the input policy, use the `no dcb-policy input` command.

**Parameters**

- **policy name** Enter the input policy name with the PFC configuration to an ingress interface.

**Defaults**

none

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

If you apply an input policy with PFC disabled (no pfc mode on):

- Link-level flow control can be enabled on the interface. To delete the input policy, you must first disable link-level flow control. PFC is then automatically enabled on the interface because an interface is by default PFC-enabled.
- PFC still allows you to configure lossless queues on a port to ensure no-drop handling of lossless traffic.

When you apply an input policy to an interface, an error message is displayed if:

- The PFC dot1p priorities result in more than two lossless port queues globally on the switch.
- Link-level flow control is already enabled. PFC and link-level flow control cannot be enabled at the same time on an interface.

In a switch stack, you must configure all stacked ports with the same PFC configuration.

A DCB input policy for PFC applied to an interface may become invalid if the dot1p-queue mapping is reconfigured. This situation occurs when the new dot1p-queue assignment exceeds the maximum number (2) of lossless queues supported globally on the switch. In this case, all PFC configurations received from PFC-enabled peers are removed and re-synchronized with the peer devices.

Traffic may be interrupted when you reconfigure PFC no-drop priorities in an input policy or re-apply the policy to an interface.

**Related Commands**

- **dcb-input** Create a DCB input policy.
**dcb-policy input stack-unit stack-ports all**

Apply the specified DCB input policy on all ports of the switch stack or a single stacked switch.

**Syntax**

dcb-policy input stack-unit \{all | stack-unit-id\} stack-ports all \textit{dcb-input-policy-name}

To remove all DCB input policies applied to the stacked ports and rest the PFC to its default settings, use the no dcb-policy input stack-unit all command.

To remove only the DCB input policies applied to the specified switch, use the no dcb-policy input stack-unit command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{stack-unit-id}</td>
<td>Enter the stack unit identification.</td>
</tr>
<tr>
<td>\textit{dcb-input-policy-name}</td>
<td>Enter the policy name for the DCB input policy.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

The dcb-policy input stack-unit all command overwrites any previous dcb-policy input stack-unit \textit{stack-unit-id} configurations. Similarly, a dcb-policy input stack-unit \textit{stack-unit-id} command overwrites any previous dcb-policy input stack-unit all configuration.

**Related Commands**

dcb-policy output stack-unit stack-ports all  
Apply the specified DCB output policy.

---

**dcb-policy output**

Apply the output policy with the ETS configuration to an egress interface.

**Syntax**

dcb-policy output \textit{policy-name}

To delete the output policy, use the no dcb-policy output command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\textit{policy name}</td>
<td>Enter the output policy name.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

When you apply an ETS output policy to on interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies.
To remove an ETS output policy from an interface, enter the `no dcb-policy output policy-name` command. ETS is enabled by default with the default ETS configuration applied (all dot1p priorities in the same group with equal bandwidth allocation).

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcb-output</td>
<td>Create a DCB output policy.</td>
</tr>
</tbody>
</table>

### `dcb-policy output stack-unit stack-ports all` Command

Apply the specified DCB output policy on all ports of the switch stack or a single stacked switch.

**Syntax**

```plaintext
dcb-policy output stack-unit {all | stack-unit-id} stack-ports all dcb-output-policy-name
```

To remove all DCB input policies applied to the stacked ports, use the `no dcb-policy output stack-unit all` command.

To remove only the DCB input policies applied to the specified switch, use the `no dcb-policy output stack-unit` command.

**Parameters**

- `stack-unit-id`: Enter the stack unit identification.
- `dcb-output-policy-name`: Enter the policy name for the DCB output policy.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The `dcb-policy output stack-unit all` command overwrites any previous `dcb-policy output stack-unit stack-unit-id` configurations. Similarly, a `dcb-policy output stack-unit stack-unit-id` command overwrites any previous `dcb-policy output stack-unit all` configuration.

You can apply a DCB output policy with ETS configuration to all stacked ports in a switch stack or an individual stacked switch. You can apply different DCB output policies to different stack units.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcb-policy input stack-unit</td>
<td>Apply the specified DCB input policy.</td>
</tr>
<tr>
<td>stack-ports all</td>
<td></td>
</tr>
</tbody>
</table>

### `dcb stack-unit all pfc-buffering pfc-port-count pfc-queues` Command

Configure the PFC buffer for all switches in the stack.

**Syntax**

```plaintext
dcb stack-unit all pfc-buffering pfc-port-count {1-56} pfc-queues {1-2}
```

To remove the configuration for the PFC buffer on all switches in the stack, use the `no dcb stack-unit all pfc-buffering pfc-port-count pfc-queues` command.
### Parameters

- **pfc-port-count {1-56}**
  - Enter the pfc-port count.
  - The valid range is 1 to 56.

- **pfc-queues {1-2}**
  - Enter the pfc-queue number.
  - The valid range is 1 to 2.

### Defaults

The PFC buffer is enabled on all ports on the stack unit.

### Command Modes

**CONFIGURATION**

### Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### Usage Information

If you configure PFC on a 40GbE port, count the 40GbE port as four PFC-enabled ports in the pfc-port number you enter in the command syntax.

To achieve lossless PFC operation, the PFC port count and queue number used for the reserved buffer size that is created must be greater than or equal to the buffer size required for PFC-enabled ports and lossless queues on the switch.

You must reload the stack or a specified stack unit (use the `reload` command in EXEC Privilege mode) for the PFC buffer configuration to take effect.

### Related Commands

**dcb stack-unit pfc-buffering pfc-port pfc-queues**

Configure the PFC buffer for all port pipes in a specified stack unit.

### Syntax

```
dcb stack-unit stack-unit-id [port-set port-set-id] pfc-buffering pfc-ports {1-56} pfc-queues {1-2}
```

To remove the configuration for the PFC buffer on all port pipes in a specified stack unit, use the `no dcb stack-unit stack-unit-id [port-set port-set-id] pfc-buffering pfc-ports pfc-queues` command.

### Parameters

- **stack-unit-id**
  - Enter the stack-unit identification.
  - The valid stack-unit IDs are 0 to 5.

- **port-set**
  - Enter the port-set identification.
  - The only valid port-set ID (port-pipe number) on an MXL Switch is 0.

- **pfc-ports {1-56}**
  - Enter the pfc-ports.
  - The valid range is 1 to 56.

- **pfc-queues {1-2}**
  - Enter the pfc-queue number.
  - The valid range is 1 to 2.

### Command Modes

**CONFIGURATION**

### Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
If you configure PFC on a 40GbE port, count the 40GbE port as four PFC-enabled ports in the pfc-port number you enter in the command syntax.

To achieve lossless PFC operation, the PFC port count and queue number used for the reserved buffer size that is created must be greater than or equal to the buffer size required for PFC-enabled ports and lossless queues on the switch.

You must reload the stack or a specified stack unit (use the reload command in EXEC Privilege mode) for the PFC buffer configuration to take effect.

**Usage Information**

**Related Commands**

- `dcb stack-unit all pfc-buffering`
- `pfc-port-count pfc-queues`

Configure the PFC buffer for all switches in the stack.

### dbcbx port-role

Configure the DCBX port role used by the interface to exchange DCB information.

**Syntax**

```
dcbx port-role {config-source | auto-downstream | auto-upstream | manual}
```

To remove DCBX port role, use the `no dcbx port-role {config-source | auto-downstream | auto-upstream | manual}` command.

**Parameters**

- `config-source | auto-downstream | auto-upstream | manual`

  Enter the DCBX port role, where:

  - `config-source`: configures the port to serve as the configuration source on the switch.
  - `auto-upstream`: configures the port to receive a peer configuration. The configuration source is elected from auto-upstream ports.
  - `auto-downstream`: configures the port to accept the internally propagated DCB configuration from a configuration source.
  - `manual`: configures the port to operate only on administer-configured DCB parameters. The port does not accept a DCB configuration received from a peer or a local configuration source.

**Defaults**

Manual.

**Command Modes**

PROTOCOL LLDP

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.
**dcbx version**

Configure the DCBX version used on the interface.

**Syntax**

dcbx version {auto | cee | cin | ieee-v2.5}

To remove the DCBX version, use the `no dcbx version {auto | cee | cin | ieee-v2.5}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| auto | Enter the DCBX version type used on the interface, where:
| cee | configurations the port to use CDD (Intel 1.01).
| cin | configurations the port to use Cisco-Intel-Nuova (DCBX 1.0).
| ieee-v2 | configurations the port to use IEEE 802.1az (Draft 2.5).

**Defaults**

Auto

**Command Modes**

PROTOCOL LLDP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

---

**debug dcbx**

Enable DCBX debugging.

**Syntax**

debuge dcbx {all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}

To disable DCBX debugging, use the `no debug dcbx` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| all | Enter the type of debugging, where:
| auto-detect-timer | enables traces for DCBX auto-detect timers.
| config-exchng | enables traces for DCBX configuration exchanges.
| fail | enables traces for DCBX failures.
| mgmt | enables traces for DCBX management frames.
| resource | enables traces for DCBX system resource frames.
| sem | enables traces for the DCBX state machine.
| tlv | enables traces for DCBX TLVs.

**Defaults**

none

**Command Modes**

EXEC PRIVILEGE
**description**

Enter a text description of the DCB policy (PFC input or ETS output).

**Syntax**

description text

To remove the text description, use the **no description** command.

**Parameters**

- **text**
  - Enter the description of the output policy.
  - Maximum: 32 characters.

**Defaults**

- none

**Command Modes**

- DCB INPUT POLICY
- DCB OUTPUT POLICY

**Related Commands**

- dcb-input
  - Create a DCB PFC input policy.
- dcb-policy input
  - Apply the output policy.
- dcb-output
  - Create a DCBETS output policy.
- dcb-policy output
  - Apply the output policy.

**ets mode on**

Enable the ETS configuration so that scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.

**Syntax**

ets mode on

To remove the ETS configuration, use the **ets mode on** command.

**Defaults**

- ETS mode is on.

**Command Modes**

- DCB OUTPUT POLICY

**Usage Information**

If you disable ETS in an output policy applied to an interface using the **no ets mode on** command, any previously configured QoS settings at the interface or global level take effect. If QoS settings are configured at the interface or global level and in an output policy map (service-policy output command), the QoS configuration in the output policy takes precedence.
fcoe priority-bits

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

Syntax

fcoe priority-bits priority-bitmap

Parameters

priority-bitmap

Enter the priority-bitmap range.
The valid range is 1 to FF.

Defaults

0x8

Usage Information

This command is available at the global level only.

Command Modes

PROTOCOL LLDP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

iscsi priority-bits

Configure the iSCSI priority advertised for the iSCSI protocol in application priority TLVs.

Syntax

iscsi priority-bits priority-bitmap

Parameters

priority-bitmap

Enter the priority bitmap.
The valid range is 1 to FF.

Defaults

0x10

Usage Information

This command is available at the global level only.

Command Modes

PROTOCOL LLDP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
**pfc link-delay**

Configure the link delay used to pause specified priority traffic.

**Syntax**

```
pfc link-delay value
```

To remove the link delay, use the `no pfc link-delay` command.

**Parameters**

- `value`  
  Valid values (in quanta) are 712-65535. One quantum is equal to a 512-bit transmission.

**Defaults**

45556 quantum

**Command Modes**

DCB INPUT POLICY

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The minimum link delay should be greater than the round-trip transmission time required by a peer to honor a PFC pause frame multiplied by the number of PFC-enabled ingress ports.

**Related Commands**

- `dcb-input` Create a DCB input policy.

---

**pfc mode on**

Enable the PFC configuration on the port so that the priorities are included in DCBX negotiation with peer PFC devices.

**Syntax**

```
pfc mode on
```

To disable the PFC configuration, use the `no pfc mode on` command.

**Defaults**

PFC mode is on.

**Command Modes**

DCB INPUT POLICY

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, you must also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (see `pfc no-drop queues`).

To disable PFC operation on an interface, enter the `no pfc mode on` command in DCB input policy configuration mode. PFC is enabled and disabled as global DCB operation is enabled (`dcb-enable`) or disabled (`no dcb-enable`).

PFC and link-level flow control cannot be enabled at the same time on an interface.

**Related Commands**

- `dcb-input` Create a DCB input policy.
pfc no-drop queues

Configure the port queues that will still function as no-drop queues for lossless traffic.

Syntax

```
pfc no-drop queues queue-range
```

To remove the no-drop port queues, use the `no pfc no-drop queues` command.

Parameters

| queue-range | Enter the queue range. Separate the queue values with a comma; specify a priority range with a dash; for example, `pfc no-drop queues 1,3` or `pfc no-drop queues 2-3`. Valid values: 0 to 3. |

Defaults
No lossless queues are configured.

Command Modes INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
The maximum number of lossless queues globally supported on the switch is two.

Table 11-1 lists the dot1p priority-queue assignments.

<table>
<thead>
<tr>
<th>dot1p Value in the Incoming Frame</th>
<th>Egress Queue Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

pfc priority

Configure the CoS traffic to be stopped for the specified delay.

Syntax

```
pfc priority priority-range
```

To delete the pfc priority configuration, use the `no pfc priority` command.

Parameters

| priority-range | Enter the 802.1p values of the frames to be paused. Separate the priority values with a comma; specify a priority range with a dash; for example, `pfc priority 1,3,5-7`. Valued values: 0 to 7. |

you can enable any number of 802.1p priorties for PFC. Queues to which PFC priority traffic is mapped are lossless by default. Traffic may be interrupted due to an interface flap (going down and coming up) when you reconfigure the lossless queues for no-drop priorities in a PFC input policy and re-apply the policy to an interface.

The maximum number of lossless queues supported on the switch is two.

The configured priority traffic must be supported by a PFC peer (as detected by DCBX) for PFC to be applied.

Related Commands

priority-group

Create an ETS priority group to use with an ETS output policy.

Syntax

priority-group group-name

To remove the priority group, use the no priority-group command.

Parameters

<table>
<thead>
<tr>
<th>group-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the name of the ETS priority group. Maximum: 32 characters.</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share the same latency and loss requirements. All 802.1p priorities mapped to the same queue should be in the same priority group.

All 802.1p priorities should be configured in priority groups associated with an ETS output policy. You can assign each dot1p priority to only one priority group.

The maximum number of priority groups supported in ETS output policies on an interface is equal to the number of data queues (4) on the port. The 802.1p priorities in a priority group can map to multiple queues.

If you configure more than one priority queue as strict priority or more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-list</td>
<td>Configure the 802.1p priorities for an ETS output policy.</td>
</tr>
<tr>
<td>set-pgid</td>
<td>Configure the priority-group.</td>
</tr>
</tbody>
</table>

**priority-group qos-policy**

Associate the 802.1p priority traffic in a priority group with the ETS configuration in a QoS output policy.

**Syntax**

```
priority-group group-name qos-policy ets-policy-name
```

To remove the 802.1p priority group, use the no priority-group qos-policy command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-name</td>
<td>Enter the group name of the 802.1p priority group. Maximum: 32 characters.</td>
</tr>
<tr>
<td>ets-policy-name</td>
<td>Enter the ETS policy name.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

DCB OUTPUT POLICY

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The ETS configuration associated with 802.1p priority traffic in a DCB output policy is used in DCBX negotiation with ETS peers.

If you disable ETS in an output policy applied to an interface using the no ets mode on command, any previously configured QoS settings at the interface or global level take effect. If QoS settings are configured at the interface or global level and in an output policy map (service-policy output command), the QoS configuration in the output policy takes precedence.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcb-output</td>
<td>Create a DCB output policy.</td>
</tr>
<tr>
<td>dcb-policy output</td>
<td>Apply the output policy.</td>
</tr>
</tbody>
</table>

**priority-list**

Configure the 802.1p priorities for the traffic on which you want to apply an ETS output policy.

**Syntax**

```
priority-list value
```

To remove the priority list, use the no priority-list command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Enter the priority list value. Separate priority values with a comma; specify a priority range with a dash; for example, priority-list 3,5-7. The value range is 0 to 7.</td>
</tr>
</tbody>
</table>

**Defaults**

none
Command Modes

<table>
<thead>
<tr>
<th>Command</th>
<th>PRIORITY-GROUP</th>
</tr>
</thead>
</table>

Command History

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

Usage Information

By default:

- All 802.1p priorities are grouped in priority group 0.
- 100% of the port bandwidth is assigned to priority group 0. The complete bandwidth is equally assigned to each priority class so that each class has 12-13%.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-group</td>
<td>Create an ETS priority group.</td>
</tr>
<tr>
<td>qos-policy</td>
<td></td>
</tr>
<tr>
<td>set-pgid</td>
<td>Configure the priority-group.</td>
</tr>
</tbody>
</table>

qos-policy-output ets

Create a QoS output policy to configure the ETS bandwidth allocation and scheduling for priority traffic.

Syntax

```
qos-policy-output policy-name ets
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-name</td>
<td>Enter the policy name.</td>
</tr>
<tr>
<td>Maximum: 32 characters.</td>
<td></td>
</tr>
</tbody>
</table>

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

If an error occurs in an ETS output-policy configuration, the configuration is ignored and the scheduler and bandwidth allocation settings are reset to the ETS default values (all priorities are in the same ETS priority group and bandwidth is allocated equally to each priority).

If an error occurs when a port receives a peer’s ETS configuration, the port’s configuration is reset to the previously configured ETS output policy. If no ETS output policy was previously applied, the port is reset to the default ETS parameters.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler</td>
<td>Schedule priority traffic in port queues.</td>
</tr>
<tr>
<td>bandwidth-percentange</td>
<td>Bandwidth percentage allocated to priority traffic in port queues.</td>
</tr>
</tbody>
</table>

scheduler

Configure the method used to schedule priority traffic in port queues.

Syntax

```
scheduler value
```
To remove the configured priority schedule, use the `no scheduler` command.

| Parameters | value | Enter schedule priority value.  
The valid values are:  
  - `strict`: strict priority traffic is serviced before any other queued traffic.  
  - `werr`: weighted elastic round robin (werr) provides low-latency scheduling for priority traffic on port queues. |

| Defaults | WERR scheduling is used to queue priority traffic. |

| Command Modes | POLICY-MAP-OUT-ETS |

| Command History | Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module |

| Usage Information | dot1p priority traffic on the switch is scheduled to the current queue mapping. dot1p priorities within the same queue should have the same traffic properties and scheduling method.  
ETS-assigned scheduling applies only to data queues, not to control queues.  
The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If both are configured, the configured bandwidth allocation will be ignored for priority-group traffic when you apply the output policy on an interface. |

| Related Commands | qos-policy-output ets Configure the ETS bandwidth allocation.  
`bandwidth-percentage` Bandwidth percentage allocated to priority traffic in port queues. |

```
set-pgid
```

Configure the priority-group identifier.

| Syntax | set-pgid value |

To remove the priority group, use the `no set-pgid` command.

| Parameters | value | Enter the priority group identification.  
The valid values are 0 to 7. |

| Defaults | none |

| Command Modes | PRIORITY-GROUP |

| Command History | Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module |

| Related Commands | priority-group qos-policy Create an ETS priority group.  
priority-list Configure the 802.1p priorities. |
**show dcb**

Displays the data center bridging status, the number of PFC-enabled ports, and the number of PFC-enabled queues.

**Syntax**

```
show dcb [stack-unit unit-number]
```

**Parameters**

- `unit-number` Enter the DCB unit number.
  The valid values are 0 to 5.

**Command Mode**

EXEC PRIVILEGE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
Figure 11-1. show dcb Command Example

FTOS# show dcb
stack-unit 0 port-set 0
  DCB Status : Enabled
  PFC Port Count : 56 (current), 56 (configured)
PFC Queue Count : 2 (current), 2 (configured)
```

**Usage Information**

Specify a stack-unit number on the Master switch in a stack.

**show interface dcbx detail**

Displays the DCBX configuration on an interface.

**Syntax**

```
show interface port-type slot/port dcbx detail
```

**Parameters**

- `port-type` Enter the port type.
- `slot/port` Enter the slot/port number.

**Command Mode**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Table 11-2 lists the show interface dcbx detail field descriptions.

### Table 11-2.  show interface dcbx detail Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface type with chassis slot and port number.</td>
</tr>
<tr>
<td>Port-Role</td>
<td>Configured the DCBX port role: auto-upstream, auto-downstream, config-source, or manual.</td>
</tr>
<tr>
<td>DCBX Operational Status</td>
<td>Operational status (enabled or disabled) used to elect a configuration source and internally propagate a DCB configuration. The DCBX operational status is the combination of PFC and ETS operational status.</td>
</tr>
<tr>
<td>Configuration Source</td>
<td>Specifies whether the port serves as the DCBX configuration source on the switch: true (yes) or false (no).</td>
</tr>
<tr>
<td>Local DCBX Compatibility mode</td>
<td>DCBX version accepted in a DCB configuration as compatible. In auto-upstream mode, a port can only received a DCBX version supported on the remote peer.</td>
</tr>
</tbody>
</table>
### Table 11-2. show interface dcbx detail Command Example Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local DCBX Configured mode</td>
<td>DCBX version configured on the port: CEE, CIN, IEEE v2.5, or Auto (port auto-configures to use the DCBX version received from a peer).</td>
</tr>
<tr>
<td>Peer Operating version</td>
<td>DCBX version that the peer uses to exchange DCB parameters.</td>
</tr>
<tr>
<td>Local DCBX TLVs Transmitted</td>
<td>Transmission status (enabled or disabled) of advertised DCB TLVs (see TLV code at the top of the show command output).</td>
</tr>
<tr>
<td>Local DCBX Status: DCBX Version</td>
<td>DCBX version advertised in Control TLVs.</td>
</tr>
<tr>
<td>Local DCBX Status: DCBX Max Version Supported</td>
<td>Highest DCBX version supported in Control TLVs.</td>
</tr>
<tr>
<td>Local DCBX Status: Sequence Number</td>
<td>Sequence number transmitted in Control TLVs.</td>
</tr>
<tr>
<td>Local DCBX Status: Acknowledgment Number</td>
<td>Acknowledgement number transmitted in Control TLVs.</td>
</tr>
<tr>
<td>Local DCBX Status: Protocol State</td>
<td>Current operational state of the DCBX protocol: ACK or IN-SYNC.</td>
</tr>
<tr>
<td>Peer DCBX Status: DCBX Version</td>
<td>DCBX version advertised in Control TLVs received from the peer device.</td>
</tr>
<tr>
<td>Peer DCBX Status: DCBX Max Version Supported</td>
<td>Highest DCBX version supported in Control TLVs received from the peer device.</td>
</tr>
<tr>
<td>Peer DCBX Status: Sequence Number</td>
<td>Sequence number transmitted in Control TLVs received from the peer device.</td>
</tr>
<tr>
<td>Peer DCBX Status: Acknowledgment Number</td>
<td>Acknowledgement number transmitted in Control TLVs received from the peer device.</td>
</tr>
<tr>
<td>Total DCBX Frames transmitted</td>
<td>Number of DCBX frames sent from the local port.</td>
</tr>
<tr>
<td>Total DCBX Frames received</td>
<td>Number of DCBX frames received from the remote peer port.</td>
</tr>
<tr>
<td>Total DCBX Frame errors</td>
<td>Number of DCBX frames with errors received.</td>
</tr>
<tr>
<td>Total DCBX Frames unrecognized</td>
<td>Number of unrecognizable DCBX frames received.</td>
</tr>
</tbody>
</table>

**Usage Information**

To clear DCBX frame counters, use the `clear dcbx counters interface stack-unit/port` command.
show interface ets

Displays the ETS configuration applied to egress traffic on an interface, including priority groups with priorities and bandwidth allocation.

**Syntax**

```
show interface port-type slot/port ets {summary | detail}
```

**Parameters**

- `port-type slot/port ets` Enter the port-type slot and port ETS information.
- `{summary | detail}` Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

**Command Mode**

CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### Example

**Figure 11-3. show interfaces ets summary Command Example**

```
FTOS(conf)# show interfaces te 0/0 ets summary
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters:
--------------------
Admin is enabled
TC-grp   Priority#          Bandwidth  TSA
0        0,1,2,3,4,5,6,7   100%       ETS
1        0%                ETS
2        0%                ETS
3        0%                ETS
4        0%                ETS
5        0%                ETS
6        0%                ETS
7        0%                ETS
Priority#    Bandwidth  TSA
0            13%        ETS
1            13%        ETS
2            13%        ETS
3            13%        ETS
4            12%        ETS
5            12%        ETS
6            12%        ETS
7            12%        ETS
Remote Parameters:
-------------------
Remote is disabled
Local Parameters:
--------------------
Local is enabled
TC-grp   Priority#          Bandwidth  TSA
0        0,1,2,3,4,5,6,7   100%       ETS
1        0%                ETS
2        0%                ETS
3        0%                ETS
4        0%                ETS
5        0%                ETS
6        0%                ETS
7        0%                ETS
Priority#    Bandwidth  TSA
0            13%        ETS
1            13%        ETS
2            13%        ETS
3            13%        ETS
4            12%        ETS
5            12%        ETS
6            12%        ETS
7            12%        ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
```
show interfaces ets detail Command Example

FTOS(conf)# show interfaces tengigabitethernet 0/0 ets detail
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters:
------------------
Admin is enabled
TC-grp   Priority#         Bandwidth       TSA
0        0,1,2,3,4,5,6,7   100%            ETS
1                            0%            ETS
2                            0%            ETS
3                            0%            ETS
4                            0%            ETS
5                            0%            ETS
6                            0%            ETS
7                            0%            ETS

Priority#                  Bandwidth       TSA
0                              13%         ETS
1                              13%         ETS
2                              13%         ETS
3                              13%         ETS
4                              12%         ETS
5                              12%         ETS
6                              12%         ETS
7                              12%         ETS

Remote Parameters:
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled
TC-grp   Priority#         Bandwidth       TSA
0        0,1,2,3,4,5,6,7   100%            ETS
1                            0%            ETS
2                            0%            ETS
3                            0%            ETS
4                            0%            ETS
5                            0%            ETS
6                            0%            ETS
7                            0%            ETS

Priority#                  Bandwidth       TSA
0                              13%         ETS
1                              13%         ETS
2                              13%         ETS
3                              13%         ETS
4                              12%         ETS
5                              12%         ETS
6                              12%         ETS
7                              12%         ETS

Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
0 Input Conf TLV Pkts, 0 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
0 Input Traffic Class TLV Pkts, 0 Output Traffic Class TLV Pkts, 0 Error Traffic Class TLV Pkts
Table 11-3 lists the show interface ets detail field descriptions.

### Table 11-3. show interfaces ets detail Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface type with stack-unit and port number.</td>
</tr>
<tr>
<td>Max Supported TC Group</td>
<td>Maximum number of priority groups supported.</td>
</tr>
<tr>
<td>Number of Traffic Classes</td>
<td>Number of 802.1p priorities currently configured.</td>
</tr>
<tr>
<td>Admin mode</td>
<td>ETS mode: on or off. When on, the scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.</td>
</tr>
<tr>
<td>Admin Parameters</td>
<td>ETS configuration on local port, including priority groups, assigned dot1p priorities, and bandwidth allocation.</td>
</tr>
<tr>
<td>Remote Parameters</td>
<td>ETS configuration on remote peer port, including admin mode (enabled if a valid TLV was received or disabled), priority groups, assigned dot1p priorities, and bandwidth allocation. If ETS admin mode is enabled on the remote port for DCBX exchange, the Willing bit received in ETS TLVs from the remote peer is included.</td>
</tr>
<tr>
<td>Local Parameters</td>
<td>ETS configuration on local port, including admin mode (enabled when a valid TLV is received from a peer), priority groups, assigned dot1p priorities, and bandwidth allocation.</td>
</tr>
</tbody>
</table>
| Operational status (local port) | Port state for current operational ETS configuration:  
  • **Init**: Local ETS configuration parameters were exchanged with the peer.  
  • **Recommend**: Remote ETS configuration parameters were received from the peer.  
  • **Internally propagated**: ETS configuration parameters were received from the configuration source. |
| ETS DCBX Oper status         | Operational status of the ETS configuration on the local port: match or mismatch.               |
| State Machine Type           | Type of state machine used for DCBX exchanges of ETS parameters:  
  Feature - for legacy DCBX versions; Asymmetric - for an IEEE version. |
| Conf TLV Tx Status           | Status of ETS Configuration TLV advertisements: enabled or disabled.                           |
| ETS TLV Statistic: Input Conf TLV pkts | Number of ETS Configuration TLVs received.                                                      |
| ETS TLV Statistic: Output Conf TLV pkts | Number of ETS Configuration TLVs transmitted.                                                   |
| ETS TLV Statistic: Error Conf TLV pkts | Number of ETS Error Configuration TLVs received.                                               |

### Usage Information

To clear ETS TLV counters, use the `clear ets counters interface port-type slot/port` command.
show interface pfc

Displays the PFC configuration applied to ingress traffic on an interface, including priorities and link delay.

**Syntax**

```
show interface port-type slot/port pfc {summary | detail}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-type slot/port pfc</td>
<td>Enter the port-type slot and port PFC information.</td>
</tr>
<tr>
<td>{summary</td>
<td>detail}</td>
</tr>
</tbody>
</table>

**Command Mode**

INTERFACE

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
To clear the PFC TLV counters, use the clear pfc counters interface port-type slot/port command.

Table 11-4 lists the show interface pfc summary field descriptions.

Table 11-4. show interfaces pfc summary Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface type with stack-unit and port number.</td>
</tr>
<tr>
<td>Admin mode is on</td>
<td>PFC admin mode is on or off with a list of the configured PFC priorities. When the PFC admin mode is on, PFC advertisements are enabled to be sent from peers; received PFC configuration will take effect. The admin operational status for a DCBX exchange of PFC configuration is enabled or disabled.</td>
</tr>
</tbody>
</table>
Remote is enabled, Priority list Remote Willing Status is enabled

- Operational status (enabled or disabled) of peer device for DCBX exchange of PFC configuration with a list of the configured PFC priorities. Willing status of peer device for DCBX exchange (Willing bit received in PFC TLV): enabled or disabled.

Local is enabled

- DCBX operational status (enabled or disabled) with a list of the configured PFC priorities.

Operational status (local port)

- Port state for current operational PFC configuration:
  - Init: Local PFC configuration parameters were exchanged with the peer.
  - Recommend: Remote PFC configuration parameters were received from the peer.
  - Internally propagated: PFC configuration parameters were received from the configuration source.

PFC DCBX Oper status

- Operational status for the exchange of the PFC configuration on the local port: match (up) or mismatch (down).

State Machine Type

- Type of state machine used for DCBX exchanges of the PFC parameters:
  - Feature - for legacy DCBX versions; Symmetric - for an IEEE version.

TLV Tx Status

- Status of the PFC TLV advertisements: enabled or disabled.

PFC Link Delay

- Link delay (in quanta) used to pause specified priority traffic.

Application Priority TLV: FCOE TLV Tx Status

- Status of FCoE advertisements in application priority TLVs from the local DCBX port: enabled or disabled.

Application Priority TLV: SCSI TLV Tx Status

- Status of iSCSI advertisements in application priority TLVs from the local DCBX port: enabled or disabled.

Application Priority TLV: Local FCOE Priority Map

- Priority bitmap used by the local DCBX port in FCoE advertisements in application priority TLVs.

Application Priority TLV: Local ISCSI Priority Map

- Priority bitmap used by the local DCBX port in iSCSI advertisements in application priority TLVs.

Application Priority TLV: Remote FCOE Priority Map

- Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.

Application Priority TLV: Remote ISCSI Priority Map

- Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.

PFC TLV Statistics: Input TLV pkts

- Number of PFC TLVs received.

PFC TLV Statistics: Output TLV pkts

- Number of PFC TLVs transmitted.

PFC TLV Statistics: Error pkts

- Number of PFC error packets received.

PFC TLV Statistics: Pause Tx pkts

- Number of PFC pause frames transmitted.

PFC TLV Statistics: Pause Rx pkts

- Number of PFC pause frames received.
show interface pfc statistics

Displays counters for the PFC frames received and transmitted (by dot1p priority class) on an interface.

**Syntax**

show interface *port-type* *slot/port* pfc statistics

**Parameters**

*port-type*  
Enter the port type.

*slot/port*  
Enter the slot/port number.

**Command Mode**

INTERFACE

**Command History**

Version 8.3.16.1  
Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 11-5. show interfaces pfc statistics Command Example**

```
FTOS#show interface tengigabitethernet 0/3 pfc statistics
Interface TenGigabitEthernet 0/3

Priority       Rx XOFF Frames          Rx Total Frames         Tx Total Frames
-------------------------------------------------------------------------------
0               0                       0                       0
1               0                       0                       0
2               0                       0                       0
3               0                       0                       0
4               0                       0                       0
5               0                       0                       0
6               0                       0                       0
7               0                       0                       0
```

show qos dcb-input

Displays the PFC configuration in a DCB input policy.

**Syntax**

show qos dcb-input [pfc-profile]

**Parameters**

[pfc-profile]  
Enter the PFC profile.

**Command Mode**

CONFIGURATION

**Command History**

Version 8.3.16.1  
Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 11-6. show qos dcb-input Command Example**

```
FTOS(conf)# show qos dcb-input
dcb-input pfc-profile
  pfc link-delay 32
  pfc priority 0-1
dcb-input pfc-profile1
  no pfc mode on
  pfc priority 6-7
```
show qos dcb-output

Displays the ETS configuration in a DCB output policy.

Syntax

show qos dcb-output [ets-profile]

Parameters

[ets-profile] Enter the ETS profile.

Command Mode

EXEC PRIVILEGE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 11-7. show qos dcb-output Command Example

FTOS# show qos dcb-output
dcb-output ets
  priority-group san qos-policy san
  priority-group ipc qos-policy ipc
  priority-group lan qos-policy lan

show qos priority-groups

Displays the ETS priority groups configured on the switch, including the 802.1p priority classes and ID of each group.

Syntax

show qos priority-groups

Command Mode

EXEC PRIVILEGE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 11-8. show qos priority-groups Command Example

FTOS#show qos priority-groups
priority-group ipc
  priority-list 4
  set-pgid 2

show stack-unit stack-ports ets detail

Displays the ETS configuration applied to egress traffic on stacked ports, including ETS operational mode on each unit and the configured priority groups with dot1p priorities, bandwidth allocation, and scheduler type.

Syntax

show stack-unit {all | stack-unit} stack-ports {all | port-number} ets detail
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit</td>
<td>Enter the stack unit identification.</td>
</tr>
<tr>
<td>port-number</td>
<td>Enter the port number.</td>
</tr>
</tbody>
</table>

### Command Mode

CONFIGURATION

### Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### Example

**Figure 11-9. show stack-unit stack-ports ets detail Command Example**

```plaintext
FTOS(conf)# show stack-unit all stack-ports all ets details

Stack unit 0 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on

Admin Parameters:
-------------------
Admin is enabled

<table>
<thead>
<tr>
<th>TC-grp</th>
<th>Priority#</th>
<th>Bandwidth</th>
<th>TSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0,1,2,3,4,5,6,7</td>
<td>100%</td>
<td>ETS</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Stack unit 1 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
Admin mode is on

Admin Parameters:
-------------------
Admin is enabled

<table>
<thead>
<tr>
<th>TC-grp</th>
<th>Priority#</th>
<th>Bandwidth</th>
<th>TSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0,1,2,3,4,5,6,7</td>
<td>100%</td>
<td>ETS</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
```
show stack-unit stack-ports pfc detail

Displays the PFC configuration applied to ingress traffic on stacked ports, including PFC operational mode on each unit with the configured priorities, link delay, and number of pause packets sent and received.

Syntax
show stack-unit {all | stack-unit} stack-ports {all | port-number} pfc detail

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit</td>
<td>Enter the stack unit.</td>
</tr>
<tr>
<td>port-number</td>
<td>Enter the port number.</td>
</tr>
</tbody>
</table>

Command Mode
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 11-10. show stack-unit all stack-ports all pfc details Command Example

```
FTOS(conf)# show stack-unit all stack-ports all pfc details

stack unit 0 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts

stack unit 1 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts
```
Debugging and Diagnostics

This chapter contains three sections:

- Offline Diagnostic Commands
- Buffer Tuning Commands
- Hardware Commands

Offline Diagnostic Commands

The offline diagnostics test suite is useful for isolating faults and debugging hardware. While tests are running, the Dell Networking operating software (FTOS) results are saved as a text file (TestReport-SU-X.txt) in the flash directory. The `show file` command is available only on Master and Standby.

Important Points to Remember

- Offline diagnostics can only be run when the unit is offline.
- You can only run offline diagnostics on a unit to which you are connected via the console. In other words, you cannot run diagnostics on a unit to which you are connected via a stacking link.
- Diagnostic results are stored in a file (TestReport-SU-X.txt) in the flash directory. To review the results, use the `show file` command, which prints the results to the screen.
- Diagnostics only test connectivity, not the entire data path.

The offline diagnostics commands are:

- `diag stack-unit`
- `offline stack-unit`
- `online stack-unit`

### diag stack-unit

Run offline diagnostics on a stack unit.

**Syntax**

```
diag stack-unit number [alllevels | level0 | level1 | level2] verbose no-reboot
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the stack-unit number.</td>
</tr>
<tr>
<td>alllevels</td>
<td>Enter the keyword <code>alllevels</code> to run the complete set of offline diagnostic tests.</td>
</tr>
</tbody>
</table>
### offline stack-unit

Place a stack unit in the offline state.

**Syntax**

```markdown
offline stack-unit number
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter the stack unit number. Range: 0 to 5</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The system reboots when the off-line diagnostics complete. This is an automatic process. A warning message appears when the `offline stack-unit` command is implemented.

```
Warning: Diagnostic execution will cause stack-unit to reboot after completion of diags.
Proceed with Offline-Diags [confirm yes/no]:y
```
online stack-unit

Place a stack unit in the online state.

Syntax

```plaintext
online stack-unit number
```

Parameters

- `number` Enter the stack unit number.

  range: 0 to 5

Defaults

none

Command Mode

EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Buffer Tuning Commands

The buffer tuning commands are:

- `buffer (Buffer Profile)`
- `buffer (Configuration)`
- `buffer-profile (Configuration)`
- `buffer-profile (Interface)`
- `show buffer-profile`
- `show buffer-profile interface`

⚠️ **Warning:** Altering the buffer allocations is a sensitive operation. Do not use any buffer tuning commands without first contacting the Dell Networking Technical Assistance Center (TAC).

buffer (Buffer Profile)

Allocate an amount of dedicated buffer space, dynamic buffer space, or packet pointers to queues 0 to 3.

Syntax

```plaintext
buffer [dedicated | dynamic | packets-pointers] queue0 number queue1 number queue2 number queue3 number
```

Parameters

- `dedicated` Enter this keyword to configure the amount of dedicated buffer space per queue.

- `dynamic` Enter this keyword to configure the amount of dynamic buffer space per Field Processor.

- `packets-pointers` Enter this keyword to configure the number of packet pointers per queue.
| queue0 number | Enter this keyword to allocate an amount of buffer space or packet pointers to Queue 0.  
Dedicated Buffer Range: 0-2013  
Dynamic Buffer Range:  
  FP: 0-2013  
  CSF: 0-131200 (in multiples of 80)  
Packet Pointer Range: 0-2047 |
|---|---|
| queue1 number | Enter this keyword to allocate an amount of buffer space or packet pointers to Queue 1.  
Dedicated Buffer Range: 0-2013  
Dynamic Buffer Range:  
  FP: 0-2013  
  CSF: 0-131200 (in multiples of 80)  
Packet Pointer Range: 0-2047 |
| queue2 number | Enter this keyword to allocate an amount of buffer space or packet pointers to Queue 2.  
Dedicated Buffer Range: 0-2013  
Dynamic Buffer Range:  
  FP: 0-2013  
  CSF: 0-131200 (in multiples of 80)  
Packet Pointer Range: 0-2047 |
| queue3 number | Enter this keyword to allocate an amount of buffer space or packet pointers to Queue 3.  
Dedicated Buffer Range: 0-2013  
Dynamic Buffer Range:  
  FP: 0-2013  
  CSF: 0-131200 (in multiples of 80)  
Packet Pointer Range: 0-2047 |

**Defaults**

| none |

**Command Mode**

| BUFFER PROFILE |

**Command History**

| Version 8.3.16.1 | Introduced on the MXL 10/40GbE Switch IO Module. |

**Related Commands**

| buffer-profile (Configuration) | Creates a buffer profile that can be applied to an interface. |

**buffer (Configuration)**

Apply a buffer profile to all Field or Switch Fabric processors in a port-pipe.

```
buffer [csf | fp-uplink] port-set port-pipe buffer-policy buffer-profile
```

**Parameters**

| csf | Enter this keyword to apply a buffer profile to all Switch Fabric processors in a port-pipe. |
| fp-uplink | Enter this keyword to apply a buffer profile to all Field Processors in a port-pipe. |
buffer-profile (Configuration)

Create a buffer profile that can be applied to an interface.

Syntax

```
buffer-profile {fp | csf} profile-name | global {1Q/4Q}
```

Parameters

- **fp**
  - Enter this keyword to create a buffer profile for the Field Processor.

- **csf**
  - Enter this keyword to create a buffer profile for the Switch Fabric Processor.

- **profile-name**
  - Create a name for the buffer profile.

- **global**
  - Apply one of two pre-defined buffer profiles to all of the port-pipes in the system.

- **1Q**
  - Enter this keyword to choose a pre-defined buffer profile for single queue (i.e non-QoS) applications.

- **4Q**
  - Enter this keyword to choose a pre-defined buffer profile for four queue (i.e QoS) applications.

Defaults

Dynamic

Command Mode

CONFIGURATION

Command History

- **Version 8.3.16.1**
  - Introduced on the MXL 10/40GbE Switch IO Module.

- **Version 9.2(0.0)**
  - Changed the Default value from global 4Q to Dynamic.
Usage Information

The **buffer-profile global** command fails if you have already applied a custom buffer-profile on an interface. Similarly, when you configure **buffer-profile global**, you cannot apply buffer-profile on any interface.

If the default buffer-profile (4Q) is active, FTOS displays an error message instructing you to remove the default configuration using the **no buffer-profile global** command.

You must reload the system for the global buffer-profile to take effect.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffer (Buffer Profile)</td>
<td>Allocates an amount of dedicated buffer space, dynamic buffer space, or packet pointers to queues 0 to 3.</td>
</tr>
</tbody>
</table>

**buffer-profile (Interface)**

Apply a buffer profile to an interface.

Syntax

```
buffer-profile profile-name
```

Parameters

- **profile-name**: Enter the name of the buffer profile you want to apply to the interface.

Defaults

none

Command Mode

INTERFACE

Command History

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffer-profile (Configuration)</td>
<td>Creates a buffer profile that can be applied to an interface.</td>
</tr>
</tbody>
</table>

**show buffer-profile**

Display the buffer profile that is applied to an interface.

Syntax

```
show buffer-profile {detail | summary} {csf | fp-uplink}
```

Parameters

- **detail**: Display the buffer allocations of the applied buffer profiles.
- **summary**: Display the buffer-profiles that are applied to line card port-pipes in the system.
- **csf**: Display the Switch Fabric Processor buffer profiles that you have applied to line card port-pipes in the system.
- **fp-uplink**: Display the Field Processor buffer profiles that you have applied to line card port-pipes in the system.

Defaults

none

Command Mode

INTERFACE

Command History

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.
Example Figure 12-1. show buffer-profile Command Example

```
FTOS#show buffer-profile summary fp-uplink
Stack Unit Port-set Buffer-profile
 0    0     test1
 4    0     test2
FTOS#
```

Related Commands

**buffer-profile (Configuration)** Creates a buffer profile that can be applied to an interface.

### show buffer-profile interface

Display the buffer profile that is applied to an interface.

**Syntax**

```
show buffer-profile {detail | summary} interface interface slot/port
```

**Parameters**

- `detail` Display the buffer allocations of a buffer profile.
- `summary` Display the Field Processors and Switch Fabric Processors that are applied in the system.
- `interface interface` Enter the keyword interface followed by the interface type, either `tengigabitethernet` or `fortygigabitethernet`.
- `slot/port` Enter the slot and port number of the interface.

**Defaults**

none

**Command Mode**

INTERFACE

**Command History**

| Version 8.3.16.1 | Introduced on the MXL 10/40GbE Switch IO Module. |

Example Figure 12-2. show buffer-profile interface Command Example

```
FTOS#show buffer-profile detail csf linecard 4 port-set 0
Linecard 4 Port-set 0
Buffer-profile test
Queue# Dedicated Buffer Buffer Packets
(Bytes)
0   36960    718
1   18560    358
2   18560    358
3   18560    358
4   9600     64
5   9600     64
6   9600     64
7   9600     63
FTOS#
```

Related Commands

**buffer-profile (Configuration)** Creates a buffer profile that can be applied to an interface.
Hardware Commands

These commands display information from a hardware sub-component or ASIC.

The hardware commands are:

- `clear hardware stack-unit`
- `clear hardware system-flow`
- `show hardware layer2 acl`
- `show hardware layer3`
- `show hardware stack-unit`
- `show hardware system-flow`

### clear hardware stack-unit
Clear statistics from selected hardware components.

**Syntax**
```
clear hardware stack-unit 0–5 {counters | unit 0–1 counters | cpu data-plane statistics | cpu party-bus statistics | stack-port 0–52}
```

**Parameters**
- **stack-unit 0–5**
  - Enter the keyword `stack-unit` followed by 0 to 5 to select a particular stack member and then enter one of the following command options to clear a specific collection of data.
- **counters**
  - Enter the keyword `counters` to clear the counters on the selected stack member.
- **unit 0–0 counters**
  - Enter the keyword `unit` along with a port-pipe number, from 0 to 1, followed by the keyword `counters` to clear the counters on the selected port-pipe.
- **cpu data-plane statistics**
  - Enter the keywords `cpu data-plane statistics` to clear the data plane statistics.
- **cpu party-bus statistics**
  - Enter the keywords `cpu party-bus statistics` to clear the management statistics.
- **stack-port 33–56**
  - Enter the keyword `stack-port` followed by the port number of the stacking port to clear the statistics of the particular stacking port.

  **Range:** 33 to 56

  **Note:** You can identify stack port numbers by physical inspection of the rear modules. The numbering is the same as for the 10G ports. You can also inspect the output of the `show system stack-ports` command.

**Defaults**
```
none
```

**Command Modes**
```
EXEC Privilege
```

**Command History**
```
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
```

**Related Commands**
- `show hardware stack-unit`
  - Displays the data plane or management plane input and output statistics of the designated component of the designated stack member.
clear hardware system-flow

Clear system-flow statistics from selected hardware components.

**Syntax**

```plaintext
clear hardware system-flow layer2 stack-unit 0-5 port-set 0-0 counters
```

**Parameters**

- `stack-unit 0-5`
  - Enter the keyword `stack-unit` followed by 0 to 5 to select a particular stack member and then enter one of the following command options to clear a specific collection of data.

- `port-set 0-0 counters`
  - Enter the keyword `port-set` along with a port-pipe number, followed by the keyword `counters` to clear the system-flow counters on the selected port-pipe.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `show hardware stack-unit` — Displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

**show hardware layer2 acl**

Display Layer 2 ACL data for the selected stack member and stack member port-pipe.

**Syntax**

```plaintext
show hardware layer2 acl stack-unit 0-5 port-set 0-0
```

**Parameters**

- `stack-unit 0-5`
  - Enter the keyword `stack-unit` followed by 0 to 5 to select a stack ID.

- `port-set 0-0`
  - Enter the keyword `port-set` with a port-pipe number — 0.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**show hardware layer3**

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

**Syntax**

```plaintext
show hardware layer3 {acl | qos} stack-unit 0-5 port-set 0-0
```

**Parameters**

- `acl | qos`
  - Enter either the keyword `acl` or the keyword `qos` to select between ACL or QoS data.
show hardware stack-unit

Display the data plane or management plane input and output statistics of the designated component of the designated stack member.

Syntax


Parameters

stack-unit 0-5 {command-option} Enter the keyword stack-unit followed by a numeral from 0 to 5 to select a stack ID.

port-set 0-0 Enter the keyword port-set with a port-pipe number — 0.

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
**show hardware stack-unit phy-firmware-version**

Enter the `drops` keyword to display internal drops on the selected stack member. Optionally, use the `unit` keyword with 0 to select port-pipe 0, and then use `port 1-56` to select a port on that port-pipe.

Enter this keyword and a stacking port number to select a stacking port for which to display statistics. Identify the stack port number as you would to identify a 10G port that was in the same place in one of the rear modules.

**Note:** You can identify stack port numbers by physical inspection of the rear modules. The numbering is the same as for the 10G ports. You can also inspect the output of the `show system stack-ports` command.

Enter the `unit` keyword followed by 0 for port-pipe 0, and then enter one of the following keywords to troubleshoot errors on the selected port-pipe and to give status on why a port is not coming up to register level: `counters`, `details`, `port-stats [detail]`, or `register`.

**Defaults**

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

**Example 1**

```
FTOS#show hardware stack-unit 0 phy-firmware-version

<table>
<thead>
<tr>
<th>PortNumber</th>
<th>Status</th>
<th>Programmed Version</th>
<th>SW Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>41</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Present</td>
<td>01.06</td>
<td></td>
</tr>
<tr>
<td>01.06</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Not Present</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

FTOS#
Example 2  Figure 12-4.  show hardware stack-unit cpu data-plane statistics Command Example

```
FTOS#show hardware stack-unit 0 cpu data-plane statistics
bc pci driver statistics for device:
rxHandle        :0
noMhdr          :0
noMbuf          :0
recvvd          :0
dropped         :0
recvToNet       :0
rxError         :0
rxDatapathErr   :0
rxPkt(COS0)     :0
rxPkt(COS1)     :0
rxPkt(COS2)     :0
rxPkt(COS3)     :0
rxPkt(COS4)     :0
rxPkt(COS5)     :0
rxPkt(COS6)     :0
rxPkt(COS7)     :0
rxPkt(UNIT0)    :0
transmitted     :1696
txRequested     :1696
noTxDesc        :0
txError         :0
txReqTooLarge   :0
txInternalError :0
txDatapathErr   :0
txPkt(COS0)     :0
txPkt(COS1)     :0
txPkt(COS2)     :0
txPkt(COS3)     :0
txPkt(COS4)     :0
txPkt(COS5)     :0
txPkt(COS6)     :0
txPkt(COS7)     :0
txPkt(UNIT0)    :0
FTOS#
```
Example 5  
**Figure 12-7.** show hardware stack-unit drops unit (drop summary per port) Command Example

```
FTOS#show hardware stack-unit 0 drops unit 0
      PortNumber  Ingress Drops IngMac Drops Total Mmu Drops EgMac Drops Egress Drops
 1      0           0             0           0           0           0           0
 2      0           0             0           0           0           0           0
 3      0           0             0           0           0           0           0
 4      0           0             0           0           0           0           0
FTOS#
```

Example 6  
**Figure 12-8.** show hardware stack-unit drops (drop counters per port) Command Example

```
FTOS#show hardware stack-unit 0 drops unit 0 port 27
--- Ingress Drops ---
  Ingress Drops : 0
  IBP CBP Full Drops : 0
  PortSTPnotFwd Drops : 0
  IPv4 L3 Discards : 0
  Policy Discards : 0
  Packets dropped by FP : 0
  (L2+L3) Drops : 0
  Port bitmap zero Drops : 0
  Rx VLAN Drops : 0
--- Ingress MAC counters---
  Ingress FCSDrops : 0
  Ingress MTUExceeds : 0
--- MMU Drops ---
  HOL DROPS : 0
  TxPurge CellErr : 0
  Aged Drops : 0
--- Egress MAC counters---
  Egress FCS Drops : 0
--- Egress FORWARD PROCESSOR Drops ---
  IPv4 L3UC Aged & Drops : 0
  TTL Threshold Drops : 0
  INVALID VLAN CNTR Drops : 0
  L2MC Drops : 0
  PKT Drops of ANY Conditions : 0
  Hg MacUnderflow : 0
  TX Err PKT Counter : 0 25
FTOS#
```
Figure 12-9. show hardware stack-unit port-statistics Command Example

```
FTOS#show hardware stack-unit 0 unit 0 port-stats
ena/ speed/ link auto STP
port link duplex scan neg? state pause discard ops face frame back
xe0  !ena  1G FD SW Yes Forward    Tag  F  GMII 1554
xe2  up   1G FD SW Yes Forward    None  FA GMII 11996
xe3  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe4  down 10G FD SW Yes Block     None  FA KR  8996
xe5  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe6  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe7  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe8  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe9  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe10 down 10G FD SW Yes Forward   Tag  F   KR 1550
xe11  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe12  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe13  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe14  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe15  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe16  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe17  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe18 down 1G FD SW Yes Forward Tag  F  GMII 1550
xe19  !ena  1G FD SW Yes Forward    Tag  F  GMII 1550
xe20 down 1G FD SW Yes Forward    Tag  F  GMII 1550

FTOS#
```

Figure 12-10. show hardware stack-unit unit 0 register Command Example

```
FTOS#show hardware stack-unit 0 unit 0 register

0x0f180d34 ALTERNATE_EMIRROR_BITMAP_PARITY_CONTROL.ipipe0 = 0x00000001
0x0f180d35 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_INTR.ipipe0 = 0x00000000
0x0f180d36 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_NACK.ipipe0 = 0x00000000
0x0018070c ARB_EOP_DEBUG.ipipe0 = 0x00000000
0x00180312 ARB_RAM_DBGCTRL.ipipe0 = 0x00000000
0x03300000 ASF_PORT_SPEED.cpu0 = 0x00000000
0x03322000 ASF_PORT_SPEED.xe0 = 0x00000000
0x03326000 ASF_PORT_SPEED.xe1 = 0x00000000
0x0332a000 ASF_PORT_SPEED.xe2 = 0x00000007
0x0332e000 ASF_PORT_SPEED.xe3 = 0x00000000
0x03332000 ASF_PORT_SPEED.xe4 = 0x00000000
0x03336000 ASF_PORT_SPEED.xe5 = 0x00000000
0x0333a000 ASF_PORT_SPEED.xe6 = 0x00000000
0x0333e000 ASF_PORT_SPEED.xe7 = 0x00000000
0x03342000 ASF_PORT_SPEED.xe8 = 0x00000000
0x03346000 ASF_PORT_SPEED.xe9 = 0x00000000
0x0334a000 ASF_PORT_SPEED.xe10 = 0x00000000
0x03350000 ASF_PORT_SPEED.xe11 = 0x00000000
0x03354000 ASF_PORT_SPEED.xe12 = 0x00000000
0x03358000 ASF_PORT_SPEED.xe13 = 0x00000000
0x0335c000 ASF_PORT_SPEED.xe14 = 0x00000000
0x03360000 ASF_PORT_SPEED.xe15 = 0x00000000
0x03364000 ASF_PORT_SPEED.xe16 = 0x00000000
0x03368000 ASF_PORT_SPEED.xe17 = 0x00000000
0x0336c000 ASF_PORT_SPEED.xe18 = 0x00000000
0x03370000 ASF_PORT_SPEED.xe19 = 0x00000000
0x03374000 ASF_PORT_SPEED.xe20 = 0x00000000
0x03378000 ASF_PORT_SPEED.xe21 = 0x00000000
0x0337c000 ASF_PORT_SPEED.xe22 = 0x00000000
0x03380000 ASF_PORT_SPEED.xe23 = 0x00000000
0x03384000 ASF_PORT_SPEED.xe24 = 0x00000000
0x03388000 ASF_PORT_SPEED.xe25 = 0x00000000
0x0338c000 ASF_PORT_SPEED.xe26 = 0x00000000
0x03390000 ASF_PORT_SPEED.xe27 = 0x00000000
0x03394000 ASF_PORT_SPEED.xe28 = 0x00000000
0x03398000 ASF_PORT_SPEED.xe29 = 0x00000000
 !------------------ output truncated ------------------!
```
Example 9  Figure 12-11.  show hardware stack-unit unit details Command Example

```plaintext
FTOS#show hardware stack-unit 0 unit 0 details
******************************************************
The total no of FP & CSF Devices in the Card is 1
The total no of FP Devices in the Card is 1
The total no of CSF Devices in the Card is 0
The number of ports in device 0 is - 49
The number of Hg ports in devices 0 is - 1
The CPU Port of the device is 0
The staring unit no the SWF in the device is 0
******************************************************

bcmLinkMonStatusShow: The Current Link Status Is
Front End Link Status  0x200000000000000000000000
Front End Port Present Status 0x000000000000000000000000
Back Plane Link Status  0x00000000

******************************************************
Link Status of all the ports in the Device - 0
The linkStatus of Front End Port 1 is FALSE
The linkStatus of Front End Port 2 is FALSE
The linkStatus of Front End Port 3 is TRUE
The linkStatus of Front End Port 4 is FALSE
The linkStatus of Front End Port 5 is FALSE
The linkStatus of Front End Port 6 is FALSE
The linkStatus of Front End Port 7 is FALSE
The linkStatus of Front End Port 8 is FALSE
The linkStatus of Front End Port 9 is FALSE
The linkStatus of Front End Port 10 is FALSE
The linkStatus of Front End Port 11 is FALSE
The linkStatus of Front End Port 12 is FALSE
The linkStatus of Front End Port 13 is FALSE
The linkStatus of Front End Port 14 is FALSE
The linkStatus of Front End Port 15 is FALSE
The linkStatus of Front End Port 16 is FALSE
The linkStatus of Front End Port 17 is FALSE
The linkStatus of Front End Port 18 is FALSE
The linkStatus of Front End Port 19 is FALSE
The linkStatus of Front End Port 20 is FALSE
The linkStatus of Front End Port 21 is FALSE
The linkStatus of Front End Port 22 is FALSE
The linkStatus of Front End Port 23 is FALSE
The linkStatus of Front End Port 24 is FALSE
The linkStatus of Front End Port 25 is FALSE
The linkStatus of Front End Port 26 is FALSE
The linkStatus of Front End Port 27 is FALSE
The linkStatus of Front End Port 28 is FALSE
The linkStatus of Front End Port 29 is FALSE
The linkStatus of Front End Port 30 is FALSE
The linkStatus of Front End Port 31 is FALSE
The linkStatus of Front End Port 32 is FALSE
The linkStatus of Front End Port 37 is FALSE
!------------------ output truncated ---------------!
```

Example 10  Figure 12-12.  show hardware stack-unit per stack unit buffer Command Example

```plaintext
FTOS(conf)#sh hardware stack-unit 0 buffer total-buffer

FTOS#sh hardware stack-unit 0 buffer total-buffer
Total Buffers allocated per Stack-Unit 46080
```
Example 11  Figure 12-13.  show hardware stack-unit per port buffer (a Specific Port) Command Example

```
FTOS(conf)#show hardware stack-unit 0 buffer unit 0 port 1 buffer-info
----- Buffer Stats for Unit 0 Port 1 -----
Maximum Shared Limit for the Port: 30720
Default Packet Buffer allocate for the Port: 120
Used Packet Buffer for the Port: 0
```

Example 12  Figure 12-14.  show hardware stack-unit queue buffer Command Example

```
FTOS(conf)#show hardware stack-unit 0 buffer unit 0 port 1 queue 2 buffer-info
----- Buffer Stats for Unit 0 Port 1 Queue 2 -----
Maximum Shared Limit: 30720
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear hardware system-flow</td>
<td>Clears statistics from selected hardware components.</td>
</tr>
<tr>
<td>show interfaces stack-unit</td>
<td>Displays information on all interfaces on a specific stack member.</td>
</tr>
<tr>
<td>show processes cpu</td>
<td>Displays CPU usage information based on running processes.</td>
</tr>
<tr>
<td>show system stack-ports</td>
<td>Displays information about the stacking ports on all switches in the stack.</td>
</tr>
<tr>
<td>show system</td>
<td>Displays the current status of all stack members or a specific member.</td>
</tr>
</tbody>
</table>

show hardware system-flow

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax

```
show hardware system-flow layer2 stack-unit 0-5 port-set 0-0 [counters]
```

Parameters

- `acl | qos` For the selected stack member and stack member port-pipe, display which system flow entry the packet hits and what queue the packet takes as it dumps the raw system flow tables.
- `stack-unit 0-5` Enter the keyword `stack-unit` followed by 0 to 5 to select a stack member ID.
- `port-set 0-0 [counters]` Enter the keyword `port-set` with a port-pipe number — 0. (OPTIONAL) Enter the keyword `counters` to display hit counters for the selected ACL or QoS option.

Defaults

none

Command Modes

EXEC Privilege

Command History

- Version 8.3.16.1  Introduced on the MXL 10/40GbE Switch IO Module.
### Example 1

**Figure 12-15. show hardware system-flow layer2 counters Command Example**

<table>
<thead>
<tr>
<th>EntryId</th>
<th>Description</th>
<th>#HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2048</td>
<td>STP BPDU Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2047</td>
<td>LLDP BPDU Redirects</td>
<td>164904</td>
</tr>
<tr>
<td>2045</td>
<td>LACP traffic Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2044</td>
<td>GVRP traffic Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2043</td>
<td>ARP Reply Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2042</td>
<td>802.1x frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2041</td>
<td>VRRP frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2040</td>
<td>IPv6VRRP frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2039</td>
<td>GRAT ARP</td>
<td>0</td>
</tr>
<tr>
<td>2036</td>
<td>IPV6 Mcast Control Traffic</td>
<td>128840</td>
</tr>
<tr>
<td>2000</td>
<td>VLT ARP SYNC Frames</td>
<td>0</td>
</tr>
<tr>
<td>1999</td>
<td>ICL Hellos</td>
<td>0</td>
</tr>
<tr>
<td>1998</td>
<td>ICL MAC SYNC Frames</td>
<td>0</td>
</tr>
<tr>
<td>1997</td>
<td>VLT Tunnelled STP Frames</td>
<td>0</td>
</tr>
<tr>
<td>1995</td>
<td>DROP Cases</td>
<td>43207</td>
</tr>
<tr>
<td>1917</td>
<td>L3 Term Traffic ClassID 1 to Q6</td>
<td>0</td>
</tr>
<tr>
<td>1916</td>
<td>L3 CPU Bound Traffic ClassId 2 to Q5</td>
<td>0</td>
</tr>
<tr>
<td>1915</td>
<td>Unknown MCAST Packets</td>
<td>0</td>
</tr>
<tr>
<td>1792</td>
<td>BGP with TTL1, L4 SRC port Redirects</td>
<td>0</td>
</tr>
<tr>
<td>1791</td>
<td>BGP with TTL1, L4 DST Port Redirects</td>
<td>0</td>
</tr>
</tbody>
</table>

```bash
FTOS#show hardware system-flow layer2 stack-unit 0 port-set 0 counters
---------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>EntryId</th>
<th>Description</th>
<th>#HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2048</td>
<td>STP BPDU Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2047</td>
<td>LLDP BPDU Redirects</td>
<td>164904</td>
</tr>
<tr>
<td>2045</td>
<td>LACP traffic Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2044</td>
<td>GVRP traffic Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2043</td>
<td>ARP Reply Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2042</td>
<td>802.1x frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2041</td>
<td>VRRP frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2040</td>
<td>IPv6VRRP frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2039</td>
<td>GRAT ARP</td>
<td>0</td>
</tr>
<tr>
<td>2036</td>
<td>IPV6 Mcast Control Traffic</td>
<td>128840</td>
</tr>
<tr>
<td>2000</td>
<td>VLT ARP SYNC Frames</td>
<td>0</td>
</tr>
<tr>
<td>1999</td>
<td>ICL Hellos</td>
<td>0</td>
</tr>
<tr>
<td>1998</td>
<td>ICL MAC SYNC Frames</td>
<td>0</td>
</tr>
<tr>
<td>1997</td>
<td>VLT Tunnelled STP Frames</td>
<td>0</td>
</tr>
<tr>
<td>1995</td>
<td>DROP Cases</td>
<td>43207</td>
</tr>
<tr>
<td>1917</td>
<td>L3 Term Traffic ClassID 1 to Q6</td>
<td>0</td>
</tr>
<tr>
<td>1916</td>
<td>L3 CPU Bound Traffic ClassId 2 to Q5</td>
<td>0</td>
</tr>
<tr>
<td>1915</td>
<td>Unknown MCAST Packets</td>
<td>0</td>
</tr>
<tr>
<td>1792</td>
<td>BGP with TTL1, L4 SRC port Redirects</td>
<td>0</td>
</tr>
<tr>
<td>1791</td>
<td>BGP with TTL1, L4 DST Port Redirects</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Example 2  Figure 12-16. show hardware system-flow layer2 (non-counters) Command Example

```
FTOS#show hardware system-flow layer2 stack-unit 0 port-set 0

############## FP Entry for redirecting STP BPDU to CPU Port ##############
EID 2048: gid=1,
  slice=15, slice_idx=0x00, prio=0x800, flags=0x82, Installed
  tcam: color_indep=0,
  higig=0, higig_mask=0,
  FPF4=0x00
  MASK=0x00000000 00000000 00000000 0180c200 00000000 00000000 00000000
  action={act=Drop, param0=0(0x00), param1=0(0x00)},
  action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
  action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
  action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
  meter=NULL,
  counter={idx=0, mode=0x01, entries=1}

############## FP Entry for redirecting LLDP BPDU to RSM ##############
EID 2047: gid=1,
  slice=15, slice_idx=0x01, prio=0x7ff, flags=0x82, Installed
  tcam: color_indep=0,
  higig=0, higig_mask=0,
  FPF4=0x00
  MASK=0x00000000 00000000 00000000 0180c200 00000000 00000000 00000000
  action={act=Drop, param0=0(0x00), param1=0(0x00)},
  action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
  action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
  action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
  meter=NULL,
  counter={idx=1, mode=0x01, entries=1}

############## FP Entry for redirecting LACP traffic to CPU Port ##############
EID 2045: gid=1,
  slice=15, slice_idx=0x02, prio=0x7fd, flags=0x82, Installed
  tcam: color_indep=0,
  higig=0, higig_mask=0,
  FPF4=0x00
  MASK=0x00000000 00000000 00000000 0180c200 00000000 00000000 00000000
  action={act=Drop, param0=0(0x00), param1=0(0x00)},
  action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
  action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
  action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
  meter=NULL,
  counter={idx=2, mode=0x01, entries=1}

############## FP Entry for redirecting GVRP traffic to RSM ##############
EID 2044: gid=1,
  slice=15, slice_idx=0x03, prio=0x7fc, flags=0x82, Installed
  tcam: color_indep=0,
  higig=0, higig_mask=0,
  FPF4=0x00
  MASK=0x00000000 00000000 00000000 00000000 00000000 00000000 0000806 0001600
  action={act=Drop, param0=0(0x00), param1=0(0x00)},
  action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
  action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
  action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
  meter=NULL,
  counter={idx=3, mode=0x01, entries=1}

############## FP Entry for redirecting ARP Replies to RSM ##############
EID 2043: gid=1,
  slice=15, slice_idx=0x04, prio=0x7fb, flags=0x82, Installed
  tcam: color_indep=0,
  higig=0, higig_mask=0,
  FPF4=0x00
  MASK=0x00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
  action={act=Drop, param0=0(0x00), param1=0(0x00)},
  action={act=CosQCpuNew, param0=6(0x06), param1=0(0x00)},
  action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
  action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},

!--------- output truncated -----------------!
```
Dynamic Host Configuration Protocol (DHCP)

Overview

Dynamic host configuration protocol (DHCP) is an application layer protocol that dynamically assigns IP addresses and other configuration parameters to network end-stations (hosts) based on configuration policies determined by network administrators.

An MXL Switch can operate as a DHCP server or DHCP client. As a DHCP client, the switch requests an IP address from a DHCP server.

The following types of DHCP commands are described in this chapter:

- Commands to Configure the System to be a DHCP Server
- Commands to Configure the System to be a DHCP Client
- Other Commands supported by DHCP Client
- Commands to Configure Secure DHCP

Commands to Configure the System to be a DHCP Server

- clear ip dhcp
- debug ip dhcp server
- default-router
- disable
- dns-server
- domain-name
- excluded-address
- hardware-address
- host
- disable
- lease
- netbios-name-server
- netbios-node-type
- network
- show ip dhcp binding
- show ip dhcp configuration
- show ip dhcp conflict
- show ip dhcp server
clear ip dhcp
Reset DHCP counters.

Syntax
clear ip dhcp [binding {address} | conflict | server statistics]

Parameters
- binding: Enter this keyword to delete all entries in the binding table.
- address: Enter the IP address to clear the binding entry for a single IP address.
- conflict: Enter this keyword to delete all of the log entries created for IP address conflicts.
- server statistics: Enter this keyword to clear all the server counter information.

Command Mode
EXEC Privilege

Default
none

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
Entering <CR> after clear ip dhcp binding, clears all the IPs from the binding table.

default-router
Assign a default gateway to clients based on address pool.

Syntax
default-router address [address2...address8]

Parameters
- address: Enter the a list of routers that may be the default gateway for clients on the subnet. You may specify up to 8. List them in order of preference.

Command Mode
DHCP <POOL>
**disable**

Disable the DHCP server.

DHCP Server is disabled by default. Enable the system to be a DHCP server using the **no** form of the **disable** command.

**Syntax**

disable

**Command Mode**

DHCP

**Default**

Disabled

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**dns-server**

Assign a DNS server to clients based on address pool.

**Syntax**

dns-server address [address2...address8]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Enter the a list of DNS servers that may service clients on the subnet. You may list up to 8 servers, in order of preference.</td>
</tr>
</tbody>
</table>

**Command Mode**

DHCP <POOL>

**Default**

none

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**domain-name**

Assign a domain to clients based on address pool.

**Syntax**

domain-name name

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Give a name to the group of addresses in a pool.</td>
</tr>
</tbody>
</table>

**Command Mode**

DHCP <POOL>

**Default**

none
excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

**Syntax**

```
excluded-address [address | low-address high-address]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Enter a single address to be excluded from the pool.</td>
</tr>
<tr>
<td>low-address</td>
<td>Enter the lowest address in a range of addresses to be excluded from the pool.</td>
</tr>
<tr>
<td>high-address</td>
<td>Enter the highest address in a range of addresses to be excluded from the pool.</td>
</tr>
</tbody>
</table>

**Command Mode**

DHCP

**Default**

none

**Command History**

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```

hardware-address

For manual configurations, specify the client hardware address.

**Syntax**

```
hardware-address address
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Enter the hardware address of the client.</td>
</tr>
</tbody>
</table>

**Command Mode**

DHCP <POOL>

**Default**

none

**Command History**

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```

host

For manual (rather than automatic) configurations, assign a host to a single-address pool.

**Syntax**

```
host address
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address/mask</td>
<td>Enter the host IP address and subnet mask.</td>
</tr>
</tbody>
</table>

**Command Mode**

DHCP <POOL>

**Default**

none

**Command History**

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```
### lease

Specify a lease time for the addresses in a pool.

**Syntax**

```
lease \{days [hours] [minutes] | infinite\}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>days</code></td>
<td>Enter the number of days of the lease. Range: 0-31</td>
</tr>
<tr>
<td><code>hours</code></td>
<td>Enter the number of hours of the lease. Range: 0-23</td>
</tr>
<tr>
<td><code>minutes</code></td>
<td>Enter the number of minutes of the lease. Range: 0-59</td>
</tr>
<tr>
<td><code>infinite</code></td>
<td>Specify that the lease never expires.</td>
</tr>
</tbody>
</table>

**Command Mode**

DHCP <POOL>

**Default**

24 hours

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### netbios-name-server

Specify the NetBIOS windows internet naming service (WINS) name servers, in order of preference, that are available to Microsoft dynamic host configuration protocol (DHCP) clients.

**Syntax**

```
netbios-name-server address [address2...address8]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address</code></td>
<td>Enter the address of the NETBIOS name server. You may enter up to 8, in order of preference.</td>
</tr>
</tbody>
</table>

**Command Mode**

DHCP <POOL>

**Default**

none

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking recommends specifying clients as hybrid.

**Syntax**

```
netbios-node-type type
```
network

Specify the range of addresses in an address pool.

**Syntax**

```
network network /prefix-length
```

**Parameters**

- `network` Specify a range of addresses.
- `prefix-length` Prefix-length Range: 17-31

**Command Mode**

DHCP <POOL>

**Default**

None

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**show ip dhcp binding**

Display the DHCP binding table.

**Syntax**

```
show ip dhcp binding
```

**Command Mode**

EXEC Privilege

**Default**

None

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**show ip dhcp configuration**

Display the DHCP configuration.

**Syntax**

```
show ip dhcp configuration [global | pool name]
```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command Mode</th>
<th>Default</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool name</td>
<td>EXEC Privilege</td>
<td>none</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
<tr>
<td>global</td>
<td>EXEC Privilege</td>
<td>none</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**show ip dhcp conflict**

Display the address conflict log.

**Syntax**

```
show ip dhcp conflict address
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Command Mode</th>
<th>Default</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>EXEC Privilege</td>
<td>none</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**show ip dhcp server**

Display the DHCP server statistics.

**Syntax**

```
show ip dhcp server statistics
```

**Command Mode**

EXEC Privilege

**Default**

none

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### Commands to Configure the System to be a DHCP Client

- clear ip dhcp

### ip address dhcp

Configure an Ethernet interface to acquire its IP address from a DHCP network server.

#### Syntax

```
ip address dhcp
```

#### Command Mode

**INTERFACE**

#### Default

The Ethernet is not configured to operate as a DHCP client and receive a dynamic IP address.

#### Command History

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

#### Usage Information

The **ip address dhcp** command enables an Ethernet interface to acquire a DHCP server-assigned dynamic IP address. This setting persists after a switch reboot. If you enter the **shutdown** command on the interface, DHCP transactions are stopped and the dynamically-acquired IP address is saved. Use the **show interface type slot/port** command to display the dynamic IP address and DHCP as the mode of IP address assignment. If you later enter the **no shutdown** command and the lease timer for the dynamic IP address has expired, the IP address is unconfigured and the interface tries to acquire a new dynamic address from DHCP server.

You cannot configure a secondary (backup) IP address on an interface using the **ip address dhcp** command; you must use the **ip address** command at the interface configuration level.

To release a DHCP-assigned IP address and remove the interface from being a DHCP client, enter the **no ip address dhcp** command. When you enter the no ip address dhcp command:

- The IP address dynamically acquired from a DHCP server is released from the interface.
- The DHCP client is disabled on the interface; it can no longer acquire a dynamic IP address from a DHCP server.
- DHCP packet transactions on the interface are stopped.

To display the currently configure dynamic IP address and lease time, enter the **show ip dhcp lease** command.
Other Commands supported by DHCP Client

- clear ip dhcp client statistics
- debug ip dhcp clients events
- debug ip dhcp clients packets
- release dhcp interface
- renew dhcp interface
- show ip dhcp client statistics
- show ip dhcp lease

**clear ip dhcp client statistics**

Display DHCP client statistics, including the number of DHCP messages sent and received on an interface.

**Syntax**

```
clear ip dhcp client statistics {all | interface type slot/port}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clear DHCP client statistics on all DHCP client-enabled interfaces on the switch.</td>
</tr>
</tbody>
</table>
| interface type slot/port | Clear DHCP client statistics on the specified interface.  
For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` followed by the `slot/port` numbers; for example, `tengigabitethernet 1/3`.  
For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` followed by the `slot/port` numbers; for example, `fortygigabitethernet 0/2`. |

**Command Mode**

EXEC Privilege

**Default**

None.

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40Gbe Switch IO Module

**debug ip dhcp clients events**

Enable the display of log messages for the following events on DHCP client interfaces:

- IP address acquisition
- IP address release
- Renewal of IP address and lease time
- Release of an IP address

**Syntax**

```
depbug ip dhcp client events [interface type slot/port]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| interface type slot/port | Display log messages for DHCP events on the specified interface.  
For a 10-GigabitEthernet Ethernet interface, enter `TenGigabitEthernet` followed by the `slot/port` numbers; for example, `tengigabitethernet 1/3`.  
For a 40-GigabitEthernet Ethernet interface, enter `FortyGigabitEthernet` followed by the `slot/port` numbers; for example, `fortygigabitethernet 0/2`. |

Dynamic Host Configuration Protocol (DHCP) | 315
**debug ip dhcp clients packets**

Enable the display of log messages for all DHCP packets sent and received on DHCP client interfaces.

**Syntax**

d debug ip dhcp client packets [interface type slot/port]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface type</td>
<td>Display log messages for DHCP packets sent and received on the specified interface. For a 10-GigabitEthernet Ethernet interface, enter TenGigabitEthernet followed by the slot/port numbers; for example, TenGigabitEthernet 1/3. For a 40-GigabitEthernet Ethernet interface, enter FortyGigabitEthernet followed by the slot/port numbers; for example, FortyGigabitEthernet 0/2.</td>
</tr>
<tr>
<td>slot/port</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

EXEC Privilege

**Default**

None

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**release dhcp interface**

Release the dynamically-acquired IP address on an Ethernet interface while retaining the DHCP client configuration on the interface.

**Syntax**

release dhcp interface type slot/port

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface type</td>
<td>For a 10-GigabitEthernet Ethernet interface, enter TenGigabitEthernet followed by the slot/port numbers; for example, TenGigabitEthernet 1/3. For a 40-GigabitEthernet Ethernet interface, enter FortyGigabitEthernet followed by the slot/port numbers; for example, FortyGigabitEthernet 0/2.</td>
</tr>
<tr>
<td>slot/port</td>
<td></td>
</tr>
</tbody>
</table>

**Command Mode**

EXEC Privilege

**Default**

None

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When you enter the release dhcp command, although the IP address that was dynamically-acquired from a DHCP server is released from an interface, the ability to acquire a new DHCP server-assigned address remains in the running configuration for the interface. To acquire a new IP address, enter either the renew dhcp command at the EXEC privilege level or the ip address dhcp command at the interface configuration level.
renew dhcp interface

Re-acquire a dynamic IP address on an Ethernet interface enabled as a DHCP client.

Syntax

renew dhcp interface type slot/port

Parameters

interface type slot/port  For a 10-GigabitEthernet Ethernet interface, enter TenGigabitEthernet followed by the slot/port numbers; for example, tengigabitethernet 1/3.
For a 40-GigabitEthernet Ethernet interface, enter FortyGigabitEthernet followed by the slot/port numbers; for example, fortygigabitethernet 0/2.

Command Mode

EXEC Privilege

Default

None.

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

When you enter the renew dhcp command, a new dynamic IP address is acquired on the specified Ethernet interface for the renewed lease time.

To display the currently configure dynamic IP address and lease time, enter the show ip dhcp lease command.

show ip dhcp client statistics

Display DHCP client statistics, including the number of DHCP messages sent and received on an interface.

Syntax

show ip dhcp client statistics {all | interface type slot/port}

Parameters

all  Display DHCP client statistics on all DHCP client-enabled interfaces on the switch.
interface type slot/port  Display DHCP client statistics on the specified interface.
For a 10-GigabitEthernet Ethernet interface, enter TenGigabitEthernet followed by the slot/port numbers; for example, tengigabitethernet 1/3.
For a 40-GigabitEthernet Ethernet interface, enter FortyGigabitEthernet followed by the slot/port numbers; for example, fortygigabitethernet 0/2.

Command Mode

EXEC Privilege

Default

None.

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

show ip dhcp lease

Display lease information about the dynamic IP address currently assigned to a DHCP client-enabled interface.

Syntax

show ip dhcp lease [interface type slot/port]
DHCP as defined by RFC 2131 provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

- arp inspection
- arp inspection-trust
- clear ip dhcp snooping
- ip dhcp snooping
- ip dhcp snooping database
- ip dhcp snooping binding
- ip dhcp snooping database renew
- ip dhcp snooping trust
- ip dhcp source-address-validation
- ip dhcp snooping vlan
- ip dhcp relay
- ip dhcp snooping verify mac-address
- show ip dhcp snooping

### Commands to Configure Secure DHCP

**arp inspection**

Enable dynamic ARP inspection (DAI) on a VLAN.

**Syntax**

```
arp inspection
```

**Command Modes**

INTERFACE VLAN

**Default**

Disabled

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- **arp inspection-trust**
  Specifies a port as trusted so that ARP frames are not validated against the binding table.
arp inspection-trust

Specify a port as trusted so that ARP frames are not validated against the binding table.

**Syntax**

```
arp inspection-trust
```

**Command Modes**

`INTERFACE`

`INTERFACE PORT-CHANNEL`

**Default**

Disabled

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `arp inspection` Enables Dynamic ARP Inspection on a VLAN.

---

clear ip dhcp snooping

Clear the DHCP binding table.

**Syntax**

```
clear ip dhcp snooping binding
```

**Command Modes**

`EXEC Privilege`

**Default**

none

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `show ip dhcp snooping` Displays the contents of the DHCP binding table.

---

ip dhcp snooping

Enable DHCP snooping globally.

**Syntax**

```
[no] ip dhcp snooping
```

**Command Modes**

`CONFIGURATION`

**Default**

Disabled

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP snooping, the binding table is deleted, and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.
Introduced in FTOS version 7.8.1.0, DHCP snooping was available for Layer 3 only and dependent on DHCP Relay Agent (ip helper-address). FTOS version 8.2.1.0 extends DHCP Snooping to Layer 2, and you do not have to enable relay agent to snoop on Layer 2 interfaces.

Related Commands

### ip dhcp snooping database

Delay writing the binding table for a specified time.

**Syntax**

```
ip dhcp snooping database write-delay minutes
```

**Parameters**

- `minutes`
  - Range: 5-21600

**Command Modes**

- CONFIGURATION

**Default**

- none

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### ip dhcp snooping binding

Create a static entry in the DHCP binding table.

**Syntax**

```
[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number
```

**Parameters**

- `mac address`
  - Enter the keyword `mac` followed by the MAC address of the host to which the server is leasing the IP address.

- `vlan-id vlan-id`
  - Enter the keyword `vlan-id` followed by the VLAN to which the host belongs.
  - Range: 2-4094

- `ip ip-address`
  - Enter the keyword `ip` followed by the IP address that the server is leasing.

- `interface type`
  - Enter the keyword `interface` followed by the type of interface to which the host is connected.
  - For a Ten Gigabit Ethernet interface, enter the keyword `tengigabitethernet`.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.

- `slot/port`
  - Enter the slot and port number of the interface.

- `lease time`
  - Enter the keyword `lease` followed by the amount of time the IP address will be leased.
  - Range: 1-4294967295

**Command Modes**

- EXEC

- EXEC Privilege

**Default**

- none
ip dhcp snooping database renew
Renew the binding table.

Syntax
ip dhcp snooping database renew

Command Modes
EXEC
EXEC Privilege

Default
none

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ip dhcp snooping trust
Configure an interface as trusted.

Syntax
[no] ip dhcp snooping trust

Command Modes
INTERFACE

Default
Untrusted

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ip dhcp source-address-validation
Enable IP source guard.

Syntax
[no] ip dhcp source-address-validation [ipmac]

Parameters
ipmac Enable IP+MAC Source Address Validation

Command Modes
INTERFACE

Default
Disabled

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
You must allocate at least one FP block to ipmacacl before you can enable IP+MAC Source Address Validation.
1. Use the command `cam-acl l2acl` from `CONFIGURATION` mode
2. Save the running-config to the startup-config
3. Reload the system.

### ip dhcp snooping vlan

Enable DHCP snooping on one or more VLANs.

**Syntax**

```
[ip dhcp snooping vlan name]
```

**Parameters**

- `name` Enter the name of a VLAN on which to enable DHCP Snooping.

**Command Modes**

`CONFIGURATION`

**Default**

Disabled

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When enabled the system begins creating entries in the binding table for the specified VLAN(s). Note that learning only happens if there is a trusted port in the VLAN.

**Related Commands**

- `ip dhcp snooping trust` Configures an interface as trusted.

### ip dhcp relay

Enable Option 82.

**Syntax**

```
ip dhcp relay information-option [remote-id | trust-downstream]
```

**Parameters**

- `remote-id` Configure the system to enable remote-id string in Option 82.
- `trust-downstream` Configure the system to trust Option 82 when it is received from the previous-hop router.

**Command Modes**

`CONFIGURATION`

**Default**

Disabled

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP source guard.

**Syntax**

```
show ip dhcp snooping [binding | source-address-validation]
```
### ip dhcp snooping verify mac-address

Validate a DHCP packet’s source hardware address against the client hardware address field (CHADDR) in the payload.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] ip dhcp snooping verify mac-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>CONFIGURATION</td>
</tr>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
<tr>
<td>Command History</td>
<td>Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

### Related Commands
- clear ip dhcp snooping
  Clears the contents of the DHCP binding table.
**Equal Cost Multi-Path**

**Overview**

Equal cost multi-path (ECMP) is supported on the MXL 10/40GbE Switch IO Module.

**Commands**

The ECMP commands are:

- `ecmp-group`
- `hash-algorithm /
- `hash-algorithm ecmp`
- `hash-algorithm seed`
- `ip ecmp-group`
- `link-bundle-monitor enable`

**ecmp-group**

Provides a mechanism to monitor traffic distribution on an ECMP link bundle. A system log is generated when the standard deviation of traffic distribution on a member link exceeds a defined threshold.

**Syntax**

```plaintext
ecmp-group {ecmp-group ID interface interface | link-bundle-monitor}
```

To remove the selected interface, use the `ecmp-group no interface` command.

To disable link bundle monitoring, use the `ecmp-group no link-bundle-monitor` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecmp-group ID</td>
<td>Enter the identifier number for the ECMP group.</td>
</tr>
<tr>
<td>Range: 2 to 64</td>
<td></td>
</tr>
</tbody>
</table>

...
hash-algorithm /

Change the hash algorithm used to distribute traffic flows across a Port Channel.

Syntax

hash-algorithm \{algorithm-number | \{ecmp | crc16 | crc16cc | crc32MSB | crc32LSB | crc-upper | dest-ip | lsb | xor1 | xor2 | xor4 | xor8 | xor16 \} [number] lag \{checksum | crc | xor\} \[number\] nh-ecmp \{checksum | crc | xor\}[number] linecard number ip-sa-mask value ip-da-mask value | seed seed-value \}

To return to the default hash algorithm, use the no hash-algorithm command.

To return to the default Equal-cost Multipath Routing (ECMP) hash algorithm, use the no hash-algorithm ecmp algorithm-value command.

To remove the hash algorithm on a particular line card, use the no hash-algorithm linecard number command.
Parameters

```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>algorithm-number</td>
<td>Enter the algorithm number. Range: 0 to 47</td>
</tr>
<tr>
<td>ecmp {crc16</td>
<td>crc16cc</td>
</tr>
<tr>
<td>nh-ecmp hash algorithm value</td>
<td>(OPTIONAL) Enter the keyword nh-ecmp followed by the ECMP hash algorithm value.</td>
</tr>
<tr>
<td>linecard number</td>
<td>(OPTIONAL) Enter the keyword linecard followed by the linecard slot number.</td>
</tr>
<tr>
<td>ip-sa-mask value</td>
<td>(OPTIONAL) Enter the keyword ip-sa-mask followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF</td>
</tr>
<tr>
<td>ip-da-mask value</td>
<td>(OPTIONAL) Enter the keyword ip-da-mask followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF</td>
</tr>
</tbody>
</table>
```

Defaults

0 for hash-algorithm value on TeraScale and ExaScale IPSA and IPDA mask value is FF for line card

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

Usage Information

To ensure that CRC is not used for LAG, set the default hash-algorithm method on ExaScale systems. For example, hash-algorithm ecmp xor lag checksum nh-ecmp checksum.

To achieve the functionality of hash-align on the ExaScale platform, do not use CRC as a hash-algorithm method.

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The hash algorithm command with the line card option changes the hash for a particular line card by applying the mask specified in the IPSA and IPDA fields.
The line card option is applicable with the lag-hash-align microcode only. Any other microcode returns an error message as follows:

```
FTOS(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff
% Error: This command is not supported in the current microcode configuration.
```

In addition, the `linecard number ip-sa-mask value ip-da-mask value` option has the following behavior to maintain bi-directionality:

- When hashing is done on both IPSA and IPDA, the `ip-sa-mask` and `ip-da-mask` values must be equal. (Single Linecard)
- When hashing is done only on IPSA or IPDA, FTOS maintains bi-directionality with masks set to XX 00 for line card 1 and 00 XX for line card 2 (`ip-sa-mask` and `ip-da-mask`). The mask value must be the same for both line cards when using multiple line cards as ingress (where XX is any value from 00 to FF for both line cards). For example, assume traffic is flowing between linecard 1 and linecard 2:

```
hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00
hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa
```

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, then use the `hash-algorithm` command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

On TeraScale if the keyword `ECMP` or `LAG` is not entered, FTOS assumes it to be common for both. If the keyword `ECMP` or `LAG` is entered separately, both should fall in the range of 0 to 23 or 24 to 47 since compression enable/disable is common for both TeraScale and ExaScale support the range 0-47. The default for ExaScale is 24.

### hash-algorithm ecmp

Change the hash algorithm used to distribute traffic flows across an ECMP (equal-cost multipath routing) group.

**Syntax**
```
hash-algorithm ecmp {crc-upper} | {dest-ip} | {lsb} /
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crc-upper</td>
<td>Uses the upper 32 bits of the key for the hash computation. Default: crc-lower</td>
</tr>
<tr>
<td>dest-ip</td>
<td>Uses the destination IP for ECMP hashing. Default: enabled</td>
</tr>
<tr>
<td>lsb</td>
<td>Returns the LSB of the key as the hash. Default: crc-lower</td>
</tr>
</tbody>
</table>
The hash value calculated with the `hash-algorithm` command is unique to the entire chassis. The default ECMP hash configuration is `crc-lower`. This takes the lower 32 bits of the hash key to compute the egress port and is the “fall-back” configuration if the user hasn’t configured anything else.

The different hash algorithms are based on the number of ECMP group members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide satisfactory distribution of traffic, then use this command to designate another algorithm.

When a member leaves or is added to the ECMP group, the hash algorithm is recalculated to balance traffic across the members.

### hash-algorithm seed

Select the seed value for the ECMP, LAG, and NH hashing algorithm.

<table>
<thead>
<tr>
<th>Syntax</th>
<th><code>hash-algorithm seed value [linecard slot] [port-set number]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td><code>seed value</code></td>
<td>Enter the keyword followed by the seed value. Range: 0 - 4095</td>
</tr>
<tr>
<td><code>linecard slot</code></td>
<td>Enter the keyword <code>linecard</code> then the linecard slot number.</td>
</tr>
<tr>
<td><code>port-set number</code></td>
<td>Enter the keyword <code>port-set</code> then the port-pipe number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>CONFIGURATION</th>
</tr>
</thead>
</table>

| Command History | Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module. |

Deterministic ECMP sorts ECMPs in order even though RTM provides them in a random order. However, the hash algorithm uses as a seed the lower 12 bits of the chassis MAC, which yields a different hash result for every chassis. This means that for a given flow, even though the prefixes are sorted, two unrelated chassis will select different hops.
FTOS provides a CLI-based solution for modifying the hash seed to ensure that on each configured system, the ECMP selection is same. When configured, the same seed is set for ECMP, LAG, and NH, and is used for incoming traffic only.

**Note:** While the seed is stored separately on each port-pipe, the same seed is used across all CAMs.

**Note:** You cannot separate LAG and ECMP, but you can use different algorithms across chassis with the same seed. If LAG member ports span multiple port-pipes and line cards, set the seed to the same value on each port-pipe to achieve deterministic behavior.

**Note:** If the hash algorithm configuration is removed, the hash seed does not go to the original factory default setting.

### ip ecmp-group

Enable and specify the maximum number of ecmp that the L3 CAM can hold for a route. By default, when maximum paths are not configured, the CAM can hold a maximum of 16 ecmp per route.

**Syntax**

```plaintext
ip ecmp-group {maximum-paths | {number} path-fallback}
```

To negate a command, use the `no ip ecmp-group maximum-paths` command.

**Parameters**

- `maximum-paths`: Specify the maximum number of ecmp for a route.
  - Range: 2 to 64
- `path-fallback`: Use the keyword `path-fallback` to enable this feature. If the feature is enabled, re-enter this keyword to disable the feature.

**Defaults**

- 16

**Command Modes**

- **CONFIGURATION**

**Command History**

| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |

**Usage Information**

You must save the new ECMP settings to the startup-config (`write-mem`) then reload the system for the new settings to take effect.

**Related Commands**

- `show ip cam stack-unit` to display content-addressable memory (CAM) entries.

### link-bundle-distribution trigger-threshold

Provides a mechanism to set the threshold to trigger when traffic distribution begins being monitored on an ECMP link bundle.

**Syntax**

```plaintext
link-bundle-distribution trigger-threshold [percent]
```

**Parameters**

- `percent`: Indicate the threshold value when traffic distribution starts being monitored on the ECMP link bundle. The range is from 1 to 90%. The default is 60%.

**Command Modes**

- **EXEC Privilege**
link-bundle-monitor enable
Provides a mechanism to enable monitoring of traffic distribution on an ECMP link bundle.

**Syntax**
link-bundle-monitor enable

To exit from ecmp group mode, use the `exit` command.

**Command Modes**
- ECMP-GROUP
- PORT-CHANNEL INTERFACE

**Command History**
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show config
Display the ECMP configuration.

**Syntax**
show config

**Command Modes**
- CONFIGURATION-ECMP-GROUP

**Command History**
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show link-bundle distribution
Display the link-bundle distribution for the interfaces in the bundle, type of bundle (LAG or ECMP), and the most recently calculated interface utilization (either bytes per second rate or maximum rate) for each interface.

**Syntax**
show link-bundle-distribution

**Command Modes**
- EXEC Privilege

**Command History**
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**
```
FTOS#show link-bundle-distribution
Link-bundle trigger threshold - 60
ECMP bundle - 5 Utilization[In Percent] - 0 Alarm State - Inactive
Interface Line Protocol Utilization[In Percent]
Te 0/4 Up 5
Te 0/3 Up 30
```
FIPS Cryptography

Overview

The following commands are used to configure the FIPS Cryptography feature on the MXL 10/40GbE Switch IO Module.

FIPS

- fips mode enable
- show fips status
- show ip ssh
- ssh

fips mode enable

Enable the FIPS cryptography mode on the platform.

**Syntax**

```
[no] fips mode enable
```

Use the `no fips mode enable` command to disable the FIPS cryptography mode.

**Default**

Disabled

**Command Mode**

CONFIGURATION

**Example**

```
FTOS(conf)#fips mode enable
WARNING: Enabling FIPS mode will close all SSH/Telnet connections, restart those servers, and destroy all configured host keys.
proceed (y/n) ? y
FTOS(conf)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh</td>
<td>Open an SSH connection specifying the hostname, username, port number and version of the SSH client.</td>
</tr>
</tbody>
</table>

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
show fips status
Displays the status of the FIPs mode.

**Syntax**
show fips status

**Default**
None

**Command Mode**
EXEC

**Example**
FTOS#show fips status
FIPS Mode       : Enabled
FTOS#

**Command History**
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

show ip ssh
Display information about established SSH sessions.

**Syntax**
show ip ssh

**Command Modes**
EXEC

EXEC Privilege

**Example**
Without FIPS Mode enabled:

```
FTOS#sh ip ssh
SSH server                : enabled.
SSH server version        :
  v1 and v2.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA       Authentication  : disabled.
                   Vty     Encryption  HMAC        Remote IP
                   1        3des-cbc   hmac-md5  10.1.20.48
                   2        3des-cbc   hmac-md5  10.1.20.48
```

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
With FIPS Mode enabled:

FTOS#sh ip ssh
SSH server : enabled.
SSH server version : v2.
Password Authentication : enabled.
Hostbased Authentication : disabled.

<table>
<thead>
<tr>
<th>Vty</th>
<th>Encryption</th>
<th>HMAC</th>
<th>Remote IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>aes128-cbc</td>
<td>hmac-sha1</td>
<td>10.11.8.13</td>
</tr>
<tr>
<td>1</td>
<td>aes128-cbc</td>
<td>hmac-sha1</td>
<td>10.1.20.48</td>
</tr>
</tbody>
</table>

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**ssh**

Open an SSH connection specifying the hostname, username, port number and version of the SSH client.

**Syntax**

```
ssh {hostname | ipv4 address | ipv6 address} [-c encryption cipher | -l username | -m HMAC algorithm | -p port-number | -v {1 | 2}]
```

**Parameters**

- `hostname` (OPTIONAL) Enter the IP address or the hostname of the remote device.
- `ipv4 address` (OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
- `ipv6-address prefix-length` (OPTIONAL) Enter the IPv6 address in the x:x:x:x format followed by the prefix length in the /x format.
  
  **Note:** The :: notation specifies successive hexadecimal fields of zeros
- `-c encryption cipher` Enter the following encryption cipher to use. (For v2 clients only.):
  - Without the FIPS mode enabled:
    - 3des-cbc: Force ssh to use 3des-cbc encryption cipher.
  - With the FIPS mode enabled:
    - aes128-cbc: Force ssh to use the aes128-cbc encryption cipher.
    - aes256-cbc: Force ssh to use the aes256-cbc encryption cipher.
- `-l username` (OPTIONAL) Enter the keyword -l followed by the user name used in this SSH session.
  
  Default: The user name of the user associated with the terminal.
- `-m HMAC algorithm` Enter one of the following HMAC algorithms to use. (For v2 clients only.):
  - Without the FIPS mode enabled:
    - hmac-sha1: Force ssh to use the hmac-sha1 HMAC algorithm.
    - hmac-sha1-96: Force ssh to use the hmac-sha1-96 HMAC algorithm.
    - hmac-md5: Force ssh to use the hmac-md5 HMAC algorithm.
    - hmac-md5-96: Force ssh to use the hmac-md5-96 HMAC algorithm.
  - With the FIPS mode enabled:
    - hmac-sha1: Force ssh to use the hmac-sha1 HMAC algorithm.
    - hmac-sha1-96: Force ssh to use the hmac-sha1-96 HMAC algorithm.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>As indicated above.</td>
<td></td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
<tr>
<td>Version 9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

### Example

If FIPS mode is not enabled:

```plaintext
FTOS#ssh 10.11.8.12 ?
-c Encryption cipher to use (for v2 clients only)
-l User name option
-m HMAC algorithm to use (for v2 clients only)
-p SSH server port option (default 22)
-v SSH protocol version
<cr>
FTOS#ssh 10.11.8.12 -c ?
3des-cbc Force ssh to use 3des-cbc encryption cipher
FTOS#ssh 10.11.8.12 -m ?
hmac-sha1 Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-md5 Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96 Force ssh to use hmac-md5-96 HMAC algorithm
```

If FIPS mode is enabled:

```plaintext
FTOS#ssh 10.11.8.12 ?
-c Encryption cipher to use (for v2 clients only)
-l User name option
-m HMAC algorithm to use (for v2 clients only)
-p SSH server port option (default 22)
<cr>
FTOS#ssh 10.11.8.12 -c ?
aes128-cbc Force ssh to use aes128-cbc encryption cipher
aes256-cbc Force ssh to use aes256-cbc encryption cipher
FTOS#ssh 10.11.8.12 -m ?
hmac-sha1 Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
```
FIP Snooping

Overview

In a converged Ethernet network, an MXL Switch can operate as an intermediate Ethernet bridge to snoop on Fibre Channel over Ethernet Initialization Protocol (FIP) packets during the login process on Fibre Channel over Ethernet (FCoE) forwarders (FCFs). Acting as a transit FIP snooping bridge, the switch uses dynamically-created ACLs to permit only authorized FCoE traffic to be transmitted between an FCoE end-device and an FCF.

The following FTOS commands are used to configure and verify the FIP snooping feature:

- clear fip-snooping database interface vlan
- clear fip-snooping statistics
- feature fip-snooping
- fip-snooping enable
- fip-snooping fc-map
- fip-snooping port-mode fcf
- show fip-snooping config
- show fip-snooping enode
- show fip-snooping fcf
- show fip-snooping sessions
- show fip-snooping statistics
- show fip-snooping system
- show fip-snooping vlan

clear fip-snooping database interface vlan

Clear FIP snooping information on a VLAN for a specified FCoE MAC address, ENode MAC address, or FCF MAC address, and remove the corresponding ACLs generated by FIP snooping.

**Syntax**

clear fip-snooping database interface vlan vlan-id {fcoe-mac-address | enode-mac-address | fcf-mac-address}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcoe-mac-address</td>
<td>Enter the FCoE MAC address to be cleared of FIP snooping information.</td>
</tr>
<tr>
<td>enode-mac-address</td>
<td>Enter the ENode MAC address to be cleared of FIP snooping information.</td>
</tr>
<tr>
<td>fcf-mac-address</td>
<td>Enter the FCF MAC address to be cleared of FIP snooping information.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege
clear fip-snooping statistics

Clears the statistics on the FIP packets snooped on all VLANs, a specified VLAN, or a specified port interface.

**Syntax**

```
clear fip-snooping statistics [interface vlan vlan-id | interface port-type port/slot | interface port-channel port-channel-number]
```

**Parameters**

- `vlan-id`
  - Enter the VLAN ID of the FIP packet statistics to be cleared.
- `port-type port/slot`
  - Enter the port-type and slot number of the FIP packet statistics to be cleared.
- `port-channel-number`
  - Enter the port channel number of the FIP packet statistics to be cleared.

**Command Modes**

EXEC Privilege

---

feature fip-snooping

Enable the FIP snooping feature on a switch.

**Syntax**

```
feature fip-snooping
```

To disable the FIP snooping feature, use the `no feature fip-snooping` command.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

---

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

---

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>
fip-snooping enable

Enable FIP snooping on all VLANs or on a specified VLAN.

Syntax

fip-snooping enable

To disable the FIP snooping feature on all or a specified VLAN, use the no fip-snooping enable command.

Defaults

FIP snooping is disabled on all VLANs.

Command Modes

• CONFIGURATION
• VLAN INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The maximum number of FCFs supported per FIP snooping-enabled VLAN is four. The maximum number of FIP snooping sessions supported per ENode server is 16.

fip-snooping fc-map

Configure the FC-MAP value used by FIP snooping on all VLANs.

Syntax

fip-snooping fc-map fc-map-value

To remove the configured FM-MAP value, use the no fip-snooping fc-map command.

Parameters

fc-map-value

Enter the FC-MAP value used by FIP snooping.
The valid values are from 0EFC00 to 0EFCFF.

Defaults

0x0EFC00

Command Modes

• CONFIGURATION
• VLAN INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The maximum number of FCFs supported per FIP snooping-enabled VLAN is four.

fip-snooping port-mode fcf

Configure the port for bridge-to-FCF links.

Syntax

fip-snooping port-mode fcf

To disable the bridge-to-FCF link on a port, use the no fip-snooping port-mode fcf command.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The maximum number of FCFs supported per FIP snooping-enabled VLAN is four.
show fip-snooping config

Display the FIP snooping status and configured FC-MAP values.

Syntax

```
show fip-snooping config
```

Command Mode

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

**Figure 16-1. show fip-snooping config Command Example**

```
FTOS# show fip-snooping config
FIP Snooping Feature enabled Status: Enabled
FIP Snooping Global enabled Status: Enabled
Global FC-MAP Value: 0X0EFC00

FIP Snooping enabled VLANs
VLAN  Enabled        FC-MAP
-----  --------       --------
100    TRUE          0X0EFC00
```

show fip-snooping enode

Display information on the ENodes in FIP-snooped sessions, including the ENode interface and MAC address, FCF MAC address, VLAN ID and FC-ID.

Syntax

```
show fip-snooping enode [enode-mac-address]
```

Parameters

- `enode-mac-address`: Enter the MAC address of the ENodes to be displayed.

Command Mode

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

**Figure 16-2. show fip-snooping enode Command Example**

```
FTOS# show fip-snooping enode
Enode MAC        Enode Interface     FCF MAC       VLAN     FC-ID
---------------  ---------------     --------       ----      ----
d4:ae:52:1b:e3:cd Te 0/11         54:7f:ee:37:34:40 100       62:00:11
```
Table 16-1.  show fip-snooping enode Command Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENode MAC</td>
<td>MAC address of the ENode</td>
</tr>
<tr>
<td>ENode Interface</td>
<td>Slot/ port number of the interface connected to the ENode.</td>
</tr>
<tr>
<td>FCF MAC</td>
<td>MAC address of the FCF</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN ID number used by the session</td>
</tr>
<tr>
<td>FC-ID</td>
<td>Fibre Channel session ID assigned by the FCF.</td>
</tr>
</tbody>
</table>

show fip-snooping fcf

Display information on the FCFs in FIP-snooped sessions, including the FCF interface and MAC address, FCF interface, VLAN ID, FC-MAP value, FKA advertisement period, and number of ENodes connected.

Syntax

show fip-snooping fcf [fcf-mac-address]

Parameters

- `fcf-mac-address` Enter the MAC address of the FCF to be displayed.

Command Mode

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 16-3.  show fip-snooping fcf Command Example

```
FTOS# show fip-snooping fcf
FCF MAC           FCF Interface       VLAN      FC-MAP    FKA_ADV_PERIOD   No. of Enodes
----------------- -------------       ----      ------    --------------   -------------
54:7f:ee:37:34:40 Po 22               100       0e:fc:00  4000             2
```

Table 16-2 lists the show fip-snooping fcf command field descriptions.

Table 16-2.  show fip-snooping fcf Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCF MAC</td>
<td>MAC address of the FCF</td>
</tr>
<tr>
<td>FCF Interface</td>
<td>Slot/port number of the interface to which the FCF is connected.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN ID number used by the session</td>
</tr>
<tr>
<td>FC-MAP</td>
<td>FC-Map value advertised by the FCF.</td>
</tr>
<tr>
<td>ENode Interface</td>
<td>Slot/ number of the interface connected to the ENode.</td>
</tr>
<tr>
<td>FKA ADV_PERIOD</td>
<td>Period of time (in milliseconds) during which FIP keep-alive advertisements are transmitted.</td>
</tr>
</tbody>
</table>
show fip-snooping sessions

Display information on FIP-snooped sessions on all VLANs or a specified VLAN, including the ENode interface and MAC address, the FCF interface and MAC address, VLAN ID, FCoE MAC address and FCoE session ID number (FC-ID), worldwide node name (WWNN) and the worldwide port name (WWPN).

**Syntax**

```
show fip-snooping sessions [interface vlan vlan-id]
```

**Parameters**

- **vlan-id**
  Enter the vlan-id of the specified VLAN to be displayed.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

Figure 16-4. show fip-snooping sessions Command Example

```
FTOS#show fip-snooping sessions

<table>
<thead>
<tr>
<th>ENode MAC</th>
<th>ENode Intf</th>
<th>FCF MAC</th>
<th>FCF Intf</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa:bb:cc:00:00:00</td>
<td>Te 0/42</td>
<td>aa:bb:cd:00:00:00</td>
<td>Te 0/43</td>
<td>100</td>
</tr>
<tr>
<td>aa:bb:cc:00:00:00</td>
<td>Te 0/42</td>
<td>aa:bb:cd:00:00:00</td>
<td>Te 0/43</td>
<td>100</td>
</tr>
<tr>
<td>aa:bb:cc:00:00:00</td>
<td>Te 0/42</td>
<td>aa:bb:cd:00:00:00</td>
<td>Te 0/43</td>
<td>100</td>
</tr>
<tr>
<td>aa:bb:cc:00:00:00</td>
<td>Te 0/42</td>
<td>aa:bb:cd:00:00:00</td>
<td>Te 0/43</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FCoE MAC</th>
<th>FC-ID</th>
<th>Port WWPN</th>
<th>Port WWNN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0e:fc:00:01:00:01</td>
<td>01:00:01</td>
<td>31:00:0e:fc:00:00:00:00</td>
<td>21:00:0e:fc:00:00:00:00</td>
</tr>
<tr>
<td>0e:fc:00:01:00:02</td>
<td>01:00:02</td>
<td>41:00:0e:fc:00:00:00:00</td>
<td>21:00:0e:fc:00:00:00:00</td>
</tr>
<tr>
<td>0e:fc:00:01:00:03</td>
<td>01:00:03</td>
<td>41:00:0e:fc:00:00:00:00</td>
<td>21:00:0e:fc:00:00:00:00</td>
</tr>
<tr>
<td>0e:fc:00:01:00:04</td>
<td>01:00:04</td>
<td>41:00:0e:fc:00:00:00:00</td>
<td>21:00:0e:fc:00:00:00:00</td>
</tr>
<tr>
<td>0e:fc:00:01:00:05</td>
<td>01:00:05</td>
<td>41:00:0e:fc:00:00:00:00</td>
<td>21:00:0e:fc:00:00:00:00</td>
</tr>
</tbody>
</table>
```

Table 16-3 lists the show fip-snooping sessions command field descriptions.

**Table 16-3. show fip-snooping sessions Command Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENode MAC</td>
<td>MAC address of the ENode.</td>
</tr>
<tr>
<td>ENode Interface</td>
<td>Slot/ port number of the interface connected to the ENode.</td>
</tr>
</tbody>
</table>
show fip-snooping statistics

Display statistics on the FIP packets snooped on all interfaces, including VLANs, physical ports, and port channels.

**Syntax**
```
show fip-snooping statistics [interface vlan vlan-id | interface port-type port/slot | interface port-channel port-channel-number]
```

**Parameters**
- `vlan-id` Enter the VLAN ID of the FIP packet statistics to be displayed.
- `port-type port/slot` Enter the port-type and slot number of the FIP packet statistics to be displayed.
- `port-channel-number` Enter the port channel number of the FIP packet statistics to be displayed.

**Command Mode**
- EXEC
- EXEC Privilege

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### Example

**Figure 16-5. show fip-snooping statistics Command Example**

<table>
<thead>
<tr>
<th>Command</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS# show fip-snooping statistics interface vlan 100</td>
<td></td>
</tr>
<tr>
<td>Number of Vlan Requests</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Vlan Notifications</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Multicast Discovery Solicits</td>
<td>:2</td>
</tr>
<tr>
<td>Number of Unicast Discovery Solicits</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGI</td>
<td>:2</td>
</tr>
<tr>
<td>Number of FDISC</td>
<td>:16</td>
</tr>
<tr>
<td>Number of FLOGO</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Enode Keep Alive</td>
<td>:9021</td>
</tr>
<tr>
<td>Number of VN Port Keep Alive</td>
<td>:3349</td>
</tr>
<tr>
<td>Number of Multicast Discovery Advertisement</td>
<td>:4437</td>
</tr>
<tr>
<td>Number of Unicast Discovery Advertisement</td>
<td>:2</td>
</tr>
<tr>
<td>Number of FLOGI Accepts</td>
<td>:2</td>
</tr>
<tr>
<td>Number of FLOGI Rejects</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FDISC Accepts</td>
<td>:16</td>
</tr>
<tr>
<td>Number of FDISC Rejects</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGO Accepts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGO Rejects</td>
<td>:0</td>
</tr>
<tr>
<td>Number of CVL</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FCF Discovery Timeouts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of VN Port Session Timeouts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Session failures due to Hardware Config</td>
<td>:0</td>
</tr>
<tr>
<td>FTOS(conf)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS# show fip-snooping statistics int tengigabitethernet 0/11</td>
<td></td>
</tr>
<tr>
<td>Number of Vlan Requests</td>
<td>:1</td>
</tr>
<tr>
<td>Number of Vlan Notifications</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Multicast Discovery Solicits</td>
<td>:1</td>
</tr>
<tr>
<td>Number of Unicast Discovery Solicits</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGI</td>
<td>:1</td>
</tr>
<tr>
<td>Number of FDISC</td>
<td>:16</td>
</tr>
<tr>
<td>Number of FLOGO</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Enode Keep Alive</td>
<td>:4416</td>
</tr>
<tr>
<td>Number of VN Port Keep Alive</td>
<td>:3136</td>
</tr>
<tr>
<td>Number of Multicast Discovery Advertisement</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Unicast Discovery Advertisement</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGI Accepts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGI Rejects</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FDISC Accepts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FDISC Rejects</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGO Accepts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FLOGO Rejects</td>
<td>:0</td>
</tr>
<tr>
<td>Number of CVL</td>
<td>:0</td>
</tr>
<tr>
<td>Number of FCF Discovery Timeouts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of VN Port Session Timeouts</td>
<td>:0</td>
</tr>
<tr>
<td>Number of Session failures due to Hardware Config</td>
<td>:0</td>
</tr>
</tbody>
</table>
Table 16-4 lists the show fip-snooping statistics command field descriptions.

### Table 16-4. show fip-snooping statistics Command Fields Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Vlan Requests</td>
<td>Number of FIP-snooped VLAN request frames received on the interface</td>
</tr>
<tr>
<td>Number of VLAN Notifications</td>
<td>Number of FIP-snooped VLAN notification frames received on the interface.</td>
</tr>
<tr>
<td>Number of Multicast Discovery Solicits</td>
<td>Number of FIP-snooped multicast discovery solicit frames received on the interface.</td>
</tr>
<tr>
<td>Number of Unicast Discovery Solicits</td>
<td>Number of FIP-snooped unicast discovery solicit frames received on the interface.</td>
</tr>
<tr>
<td>Number of FLOGI</td>
<td>Number of FIP-snooped FLOGI request frames received on the interface</td>
</tr>
<tr>
<td>Number of FLOGI Accepts</td>
<td>Number of FIP-snooped FLOGI accept frames received on the interface</td>
</tr>
<tr>
<td>Number of FLOGI Rejects</td>
<td>Number of FIP-snooped FLOGI reject frames received on the interface</td>
</tr>
<tr>
<td>Number of FDISC</td>
<td>Number of FIP-snooped FDISC request frames received on the interface</td>
</tr>
<tr>
<td>Number of FDISC Accepts</td>
<td>Number of FIP-snooped FDISC accept frames received on the interface</td>
</tr>
<tr>
<td>Number of FDISC Rejects</td>
<td>Number of FIP-snooped FDISC reject frames received on the interface</td>
</tr>
<tr>
<td>Number of CVL</td>
<td>Number of FIP-snooped CVL frames received on the interface</td>
</tr>
<tr>
<td>Number of ENode Keep Alives</td>
<td>Number of FIP-snooped ENode keep-alive frames received on the interface</td>
</tr>
<tr>
<td>Number of VN Port Keep Alives</td>
<td>Number of FIP-snooped VN port keep-alive frames received on the interface</td>
</tr>
<tr>
<td>Number of Multicast Discovery Advertisements</td>
<td>Number of FIP-snooped multicast discovery advertisements received on the interface.</td>
</tr>
<tr>
<td>Number of Unicast Discovery Advertisements</td>
<td>Number of FIP-snooped unicast discovery advertisements received on the interface.</td>
</tr>
</tbody>
</table>
show fip-snooping system

Display information on the status of FIP snooping on the switch (enabled or disabled), including the number of FCoE VLANs, FCFs, ENodes, and currently active sessions.

Syntax
show fip-snooping system

Command Mode
- EXEC
- EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 16-7. show fip-snooping system Command Example

```
FTOS# show fip-snooping system
Global Mode : Enabled
FCOE VLAN List (Operational) : 1, 100
FCFs : 1
Enodes : 2
Sessions : 17
```
show fip-snooping vlan

Display information on the FCoE VLANs on which FIP snooping is enabled.

**Syntax**

```
show fip-snooping vlan
```

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 16-8.  show fip-snooping vlan Command Example**

```
FTOS# show fip-snooping vlan
* = Default VLAN

+-----+--------+-------+-------+--------+
<table>
<thead>
<tr>
<th>VLAN</th>
<th>FC-MAP</th>
<th>FCFs</th>
<th>Enodes</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>100</td>
<td>0X0EFC00</td>
<td>1</td>
<td>2</td>
<td>17</td>
</tr>
</tbody>
</table>
```
Force10 Resilient Ring Protocol (FRRP)

Overview

Force10 Resilient Ring Protocol (FRRP) is supported on the MXL 10/40GbE Switch IO Module.

FRRP is a proprietary protocol for that offers fast convergence in a Layer 2 network without having to run the spanning tree protocol (STP). The resilient ring protocol is an efficient protocol that transmits a high-speed token across a ring to verify the link status. All the intelligence is contained in the master node with practically no intelligence required of the transit mode.

Important Points to Remember

- FRRP is media- and speed-independent.
- FRRP is a Dell Networking proprietary protocol that does not interoperate with any other vendor.
- Spanning Tree must be disabled on both primary and secondary interfaces before Resilient Ring protocol is enabled.
- A VLAN configured as the control VLAN for a ring cannot be configured as a control or member VLAN for any other ring.
- Member VLANs across multiple rings are not supported in Master nodes.
- If multiple rings share one or more member VLANs, they cannot share any links between them.
- Each ring can have only one Master node; all others are Transit nodes.

Commands

The FRRP commands are:

- `clear frrp`
- `debug frrp`
- `description`
- `disable`
- `interface`
- `member-vlan`
- `mode`
- `protocol frrp`
- `show frrp`
- `timer`
clear frrp

Clear the FRRP statistics counters.

**Syntax**

```
clear frrp [ring-id]
```

**Parameters**

- `ring-id` (Optional) Enter the ring identification number.  
  Range: 1 to 255

**Defaults**

No default values or behavior

**Command Modes**

EXEC

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

**Figure 17-1. clear frrp Command Examples**

```
FTOS#clear frrp  
clears the frrp counters for all the available rings

Clear frrp statistics counter on all ring [confirm] yes  
confirmation required

FTOS#clear frrp 4  
clears the frrp counters on the specified ring

Clear frrp statistics counter for ring 4 [confirm] yes  
confirmation required

FTOS#
```

**Usage Information**

Executing this command without the optional `ring-id` clears the statistics counters on all the available rings. FTOS requires a command line confirmation before the command is executed. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

**Related Commands**

- `show frrp` Display the Resilient Ring Protocol configuration

---

debug frrp

Enable FRRP debugging.

**Syntax**

```
debug frrp {event | packet | detail} [ring-id] [count number]
```

To disable debugging, use the `no debug frrp {event | packet | detail} {ring-id} [count number]` command.
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event</td>
<td>Enter the keyword <code>event</code> to display debug information related to ring protocol transitions.</td>
</tr>
<tr>
<td>packet</td>
<td>Enter the keyword <code>packet</code> to display brief debug information related to control packets.</td>
</tr>
<tr>
<td>detail</td>
<td>Enter the keyword <code>detail</code> to display detailed debug information related to the entire ring protocol packets.</td>
</tr>
<tr>
<td>ring-id</td>
<td>(Optional) Enter the ring identification number. Range: 1 to 255</td>
</tr>
<tr>
<td>count number</td>
<td>Enter the keyword <code>count</code> followed by the number of debug outputs. Range: 1 to 65534</td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Since the Resilient Ring Protocol can potentially transmit 20 packets per interface, restrict debug information.

description

Enter an identifying description of the ring.

Syntax

description Word

Parameters

Word | Enter a description of the ring. Maximum: 255 characters

Defaults

No default values or behavior

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

disable

Disable the Resilient Ring Protocol.

Syntax

disable

Parameters

None

Defaults

Disabled

Command Modes

CONFIGURATION (conf-frrp)
interface

Configure the primary, secondary, and control-vlan interfaces.

**Syntax**

```plaintext
interface {primary interface secondary interface control-vlan vlan-id}
```

To return to the default, use the `no interface {primary interface secondary interface control-vlan vlan-id}` command.

**Parameters**

- **primary interface**: Enter the keyword `primary` to configure the primary interface then one of the following interfaces and slot/port information:
  - For a Fast Ethernet interface, enter the keyword `FastEthernet` then the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` then a number: Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

- **secondary interface**: Enter the keyword `secondary` to configure the secondary interface then one of the following interfaces and slot/port information:
  - For a Fast Ethernet interface, enter the keyword `FastEthernet` then the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` then a number: Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

- **control-vlan vlan-id**: Enter the keyword `control-vlan` then the VLAN ID. Range: 1 to 4094

**Defaults**

No default values or behavior

**Command Modes**

CONFIGURATION (conf-frrp)

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
- **Version 8.2.1.0** Introduced for the C-Series
- **Version 7.4.1.0** Introduced

**Usage Information**

This command causes the Ring Manager to take ownership of these two ports after the configuration is validated by the IFM. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is, the interface does not belong to any ring.

**Related Commands**

- `show frrp` Display the Resilient Ring Protocol configuration information
**member-vlan**

Specify the member VLAN identification numbers.

**Syntax**

```
member-vlan {vlan-range}
```

To return to the default, use the `no member-vlan [vlan-range]` command.

**Parameters**

- `vlan-range` Enter the member VLANs using comma separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example:
  - Comma separated: 3, 4, 6
  - Range: 5-10
  - Combination: 3, 4, 5-10, 8

**Defaults**

No default values or behavior

**Command Modes**

CONFIGURATION (conf-frrp)

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**mode**

Set the Master or Transit mode of the ring.

**Syntax**

```
mode {master | transit}
```

To reset the mode, use the `no mode {master | transit}` command.

**Parameters**

- `master` Enter the keyword `master` to set the Ring node to Master mode.
- `transit` Enter the keyword `transit` to set the Ring node to Transit mode.

**Defaults**

Mode None

**Command Modes**

CONFIGURATION (conf-frrp)

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**protocol frrp**

Enter the Resilient Ring Protocol and designate a ring identification.

**Syntax**

```
protocol frrp {ring-id}
```

To exit the ring protocol, use the `no protocol frrp {ring-id}` command.

**Parameters**

- `ring-id` Enter the ring identification number.
  - Range: 1 to 255

**Defaults**

No default values or behavior
show frrp

Display the Resilient Ring Protocol configuration.

Syntax

show frrp [ring-id [summary]] | [summary]

Parameters

- **ring-id**: Enter the ring identification number.
  - Range: 1 to 255

- **summary**: (OPTIONAL) Enter the keyword summary to view just a summarized version of the Ring configuration.

Defaults

No default values or behavior

Command Modes

EXECS

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example 1

**Figure 17-2. show frrp summary Command Example**

```
FTOS#show frrp summary

+---------------+---------------+----------+-----------+------------------+
| Ring-ID       | State        | Mode     | Ctrl_Vlan | Member_Vlans     |
|---------------+---------------+----------+-----------+------------------|
| 2             | UP            | Master   | 2         | 11-20, 25,27-30  |
| 31            | UP            | Transit  | 31        | 40-41             |
| 50            | Down          | Transit  | 50        | 32               |

FTOS#
```

Example 2

**Figure 17-3. show frrp ring-id Command Example**

```
FTOS#show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
  Primary : GigabitEthernet 0/16 State: Forwarding
  Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150 msec
Ring Master's MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009

FTOS#
```
Example 3

Figure 17-4.  show frrp ring-id summary Command Example

<table>
<thead>
<tr>
<th>Ring-ID</th>
<th>State</th>
<th>Mode</th>
<th>Ctrl_Vlan</th>
<th>Member_Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Up</td>
<td>Master</td>
<td>2</td>
<td>11-20, 25, 27-30</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol frrp</td>
<td>Enter the Resilient Ring Protocol and designate a ring identification</td>
</tr>
</tbody>
</table>

**timer**

Set the hello or dead interval for the Ring control packets.

**Syntax**

```
timer {hello-interval milliseconds} | {dead-interval milliseconds}
```

To remove the timer, use the no timer {hello-interval [milliseconds]} | {dead-interval milliseconds} command.

**Parameters**

- **hello-interval milliseconds**
  - Enter the keyword `hello-interval` followed by the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be entered in increments of 50 milliseconds, for example 50, 100, 150 and so on. If an invalid value is entered, an error message is generated.
  - Range: 50 to 2000ms
  - Default: 500ms

- **dead-interval milliseconds**
  - Enter the keyword `dead-interval` followed by the time, in milliseconds, to set the dead interval of the control packets.
  - Range: 50 to 6000ms
  - Default: 1500ms
  - **Note:** The configured dead interval should be at least three times the hello interval.

**Defaults**

Default as shown

**Command Modes**

CONFIGURATION (conf-frrp)

**Command History**

```
Version 9.2(0.0)  Introduced on the Mxl 10/40GbE Switch IO Module.
```

**Usage Information**

The hello interval is the interval at which ring frames are generated from the primary interface of the master node. The dead interval is the time that elapses before a timeout occurs.
GARP VLAN Registration (GVRP)

Commands

The generic attribute registration protocol (GVRP) commands are:

- clear gvrp statistics
- debug gvrp
- disable
- garp timers
- gvrp enable
- gvrp registration
- protocol gvrp
- show config
- show garp timers
- show gvrp
- show gvrp statistics
- show vlan

The GARP mechanism allows the configuration of a GARP participant to propagate through a network quickly. A GARP participant registers or de-registers its attributes with other participants by making or withdrawing declarations of attributes. At the same time, based on received declarations or withdrawals, GARP handles attributes of other participants.

GVRP enables a device to propagate virtual local area network (VLAN) registration information to other participant devices and dynamically update the VLAN registration information from other devices. The registration information updates local databases regarding active VLAN members and through which port the VLANs can be reached.

GVRP ensures that all participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP include both manually configured local static entries and dynamic entries from other devices.

GVRP participants have the following components:

- The GVRP application
- GARP information propagation (GIP)
- GARP information declaration (GID)
Important Points to Remember

- GVRP is supported on Layer 2 ports only.
- All VLAN ports added by GVRP are tagged.
- GVRP is supported on untagged ports belonging to a default VLAN, and tagged ports.
- GVRP cannot be enabled on untagged ports belonging to a non-default VLAN unless native VLAN is turned on.
- GVRP requires end stations with dynamic access network interface controller (NICs).
- Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecified) with a specific VLAN ID and a specific port.
- On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
- GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
- GVRP updates are not sent to any blocked spanning tree protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- GVRP operates only on ports that are in the STP forwarding state. If GVRP is enabled, a port that changes to the STP forwarding state automatically begins to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.
- VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
- GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge needs to classify and analyze packets by VLAN protocols, you must manually configure protocol-based VLANs, and simply rely on GVRP for VLAN updates. But if the local bridge needs to know only how to reach a given VLAN, then GVRP provides all necessary information.
- The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

clear gvrp statistics

Clear GVRP statistics on an interface.

Syntax

```plaintext
clear gvrp statistics interface interface
```

Parameters

- **interface interface**
  - Enter the following keywords and slot/port or number information:
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number: Range: 1 to 128
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
debug gvrp

Enable debugging on GVRP.

Syntax
debug gvrp \{config | events | pdu\}

To disable debugging, use the no debug gvrp \{config | events | pdu\} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>config</strong></td>
<td>Enter the keyword config to enable debugging on the GVRP configuration.</td>
</tr>
<tr>
<td><strong>event</strong></td>
<td>Enter the keyword event to enable debugging on the JOIN/LEAVE events.</td>
</tr>
</tbody>
</table>
| **pdu** | Enter the keyword pdu followed one of the following Interface keywords and slot/port or number information:  
- For a Port Channel interface, enter the keyword port-channel followed by a number: Range: 1-128  
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.  
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information. |

Defaults
Disabled

Command Modes
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

disable

Globally disable GVRP.

Syntax
disable

To re-enable GVRP, use the no disable command.

Defaults
Enabled

Command Modes
CONFIGURATION-GVRP

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands
gvrp enable Enables GVRP on physical interfaces and LAGs.
protocol gvrp Accesses the GVRP protocol.
garp timers

Set the intervals (in milliseconds) for sending GARP messages.

**Syntax**

```
garp timers {join | leave | leave-all}
```

To return to the previous setting, use the `no garp timers {join | leave | leave-all}` command.

**Parameters**

- **join**
  - Enter the keyword `join` followed by the number of milliseconds to configure the join time.
  - Range: 100 to 147483647 milliseconds
  - Default: 200 milliseconds
  - **Note:** Designate the milliseconds in multiples of 100

- **leave**
  - Enter the keyword `leave` followed by the number of milliseconds to configure the leave time.
  - Range: 100 to 2147483647 milliseconds
  - Default: 600 milliseconds
  - **Note:** Designate the milliseconds in multiples of 100

- **leave-all**
  - Enter the keyword `leave-all` followed by the number of milliseconds to configure the leave-all time.
  - Range: 100 to 2147483647 milliseconds
  - Default: 1000 milliseconds
  - **Note:** Designate the milliseconds in multiples of 100

**Defaults**

Default as above

**Command Modes**

CONFIGURATION-GVRP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

- **Join Timer**—Join messages announce the willingness to register some attributes with other participants. Each GARP application entity sends a Join message twice, for reliability, and uses a join timer to set the sending interval.

- **Leave Timer**—Leave announces the willingness to de-register with other participants. Together with the Join, Leave messages help GARP participants complete attribute re-registration and de-registration. Leave Timer starts upon receipt of a leave message sent for de-registering some attribute information. If a join message is not received before the leave time expires, the GARP application entity removes the attribute information as requested.

- **Leave All Timer**—The Leave All Timer starts when a GARP application entity starts. When this timer expires, the entity sends a leave-all message so that other entities can re-register their attribute information. Then, the leave-all time begins again.

**Related Commands**

- `show garp timers` Displays the current GARP times.
### gvrp enable

Enable GVRP on physical interfaces and LAGs.

**Syntax**
gvrp enable

To disable GVRP on the interface, use the no gvrp enable command.

**Defaults**
Disabled

**Command Modes**
CONFIGURATION-INTERFACE

**Command History**
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**
disable Globally disables the GVRP.

### gvrp registration

Configure the GVRP register type.

**Syntax**
gvrp registration {fixed | normal | forbidden}

To return to the default, use the gvrp register normal command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fixed</td>
<td>Enter the keyword fixed followed by the VLAN range in a comma separated VLAN ID set.</td>
</tr>
<tr>
<td>normal</td>
<td>Enter the keyword normal followed by the VLAN range in a comma separated VLAN ID set. This is the default</td>
</tr>
<tr>
<td>forbidden</td>
<td>Enter the keyword forbidden followed by the VLAN range in a comma separated VLAN ID set.</td>
</tr>
</tbody>
</table>

**Defaults**
Default registration is normal

**Command Modes**
CONFIGURATION-INTERFACE

**Command History**
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**
The fixed registration prevents an interface, configured via the command line to belong to a VLAN (static configuration), from being un-configured when it receives a Leave message. Therefore, the registration mode on that interface is fixed.

The normal registration is the default registration. The port’s membership in the VLANs depends on GVRP. The interface becomes a member of VLANs after learning about the VLAN through GVRP. If the VLAN is removed from the port that sends GVRP advertisements to this device, then the port will stop being a member of the VLAN.

Use forbidden when you do not want the interface to advertise or learn about VLANs through GVRP.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show gvrp</td>
<td>Displays the GVRP configuration including the registration</td>
</tr>
</tbody>
</table>

**protocol gvrp**

Access GVRP protocol — (config-gvrp)#.

**Syntax**

```
protocol gvrp
```

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Globally disables the GVRP.</td>
</tr>
</tbody>
</table>

**show config**

Display the global GVRP configuration.

**Syntax**

```
show config
```

**Command Modes**

CONFIGURATION-GVRP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gvrp enable</td>
<td>Enables GVRP on physical interfaces and LAGs.</td>
</tr>
<tr>
<td>protocol gvrp</td>
<td>Accesses the GVRP protocol.</td>
</tr>
</tbody>
</table>

**show garp timers**

Display the GARP timer settings for sending GARP messages.

**Syntax**

```
show garp timers
```

**Defaults**

none

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
GARP VLAN Registration (GVRP)

Example

**Figure 18-1. show garp timers Command Example**

```
FTOS#show garp timers
GARP Timers Value (milliseconds)
----------------------------------------
Join Timer 200
Leave Timer 600
LeaveAll Timer 10000
FTOS#
```

Related Commands

garp timers
Sets the intervals (in milliseconds) for sending GARP messages.

**show gvrp**

Display the GVRP configuration.

Syntax

```
show gvrp [brief | interface]
```

Parameters

brief
(Optional) Enter the keyword brief to display a brief summary of the GVRP configuration.

interface
(Optional) Enter the following keywords and slot/port or number information:
- For a Port Channel interface, enter the keyword port-channel followed by a number: Range: 1-128
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

Defaults

none

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

**Figure 18-2. show gvrp brief Command Example**

```
R3#show gvrp brief
GVRP Feature is currently enabled.

<table>
<thead>
<tr>
<th>Port</th>
<th>GVRP Status</th>
<th>Edge-Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te 3/0</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/1</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/2</td>
<td>Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/3</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/4</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/5</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/6</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/7</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Te 3/8</td>
<td>Disabled</td>
<td>No</td>
</tr>
</tbody>
</table>
R3#show gvrp brief
```

Usage Information

If no ports are GVRP participants, the message output changes from:

GVRP Participants running on <port_list>
show gvrp statistics

Display the GVRP configuration statistics.

Syntax

    show gvrp statistics {interface interface | summary}

Parameters

- `interface interface` Enter the keyword `interface` followed by one of the interface keywords and slot/port or number information:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number: Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

- `summary` Enter the keyword `summary` to display just a summary of the GVRP statistics.

Defaults

- none

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```
FTOS#show gvrp statistics int tengig 1/0
Join Empty Received: 0
Join In Received: 0
Empty Received: 0
Leave In Received: 0
Leave Empty Received: 0
Leave All Received: 40
Join Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
Failed Registrations: 0
FTOS#
```

Usage Information

Invalid messages/attributes skipped can occur in the following cases:

- The incoming GVRP PDU has an incorrect length.
- “End of PDU” was reached before the complete attribute could be parsed.
- The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01).
• The attribute that was being parsed had an invalid attribute length.
• The attribute that was being parsed had an invalid GARP event.
• The attribute that was being parsed had an invalid VLAN ID. The valid range is 1 - 4095.

A failed registration can occur for the following reasons:
• Join requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state).
• An entry for a new GVRP VLAN could not be created in the GVRP database.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show gvrp</td>
<td>Displays the GVRP configuration.</td>
</tr>
</tbody>
</table>

### show vlan

Display the global VLAN configuration.

**Syntax**

```plaintext
show vlan
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40Gbe Switch IO Module

**Example**

**Figure 18-4. show vlan Command Example**

```plaintext
FTOS# show vlan
Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
x - Dot1x untagged, X - Dot1x tagged
G - GVRP tagged, M - Vlan-stack, H - VSN tagged
i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT tagged
NUM Status Description Q Ports
* 1 Active               U Te 3/20
G 10 Active             U Te 5/20-21
learned vlan
FTOS#
```
Internet Group Management Protocol (IGMP)

IGMP Snooping Commands

The Dell Networking operating software (FTOS) supports internet group management protocol (IGMP) snooping version 2 and 3 on all Dell Networking systems:

- ip igmp access-group
- ip igmp group-join-limit
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-resp-time
- ip igmp version
- ip igmp snooping enable
- ip igmp snooping fast-leave
- ip igmp snooping flood
- ip igmp snooping last-member-query-interval
- ip igmp snooping mrouter
- ip igmp snooping querier
- show ip igmp snooping mrouter

Important Points to Remember for IGMP Snooping

- FTOS supports version 1, version 2, and version 3 hosts.
- FTOS IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac-address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 forwarding information base (FIB).
- FTOS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- IGMP snooping is supported on all MXL 10/40GbE stack members.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 virtual local area network (VLAN) are supported.
- IGMP snooping is not supported on default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).
- IGMP snooping does not react to Layer 2 topology changes triggered by spanning tree protocol (STP).
- IGMP snooping reacts to Layer 2 topology changes triggered by multiple spanning tree protocol (MSTP) by sending a general query on the interface that comes in FWD state.
Important Points to Remember for IGMP Querier

- The IGMP snooping Querier supports version 2.
- You must configure an IP address to the VLAN interface for IGMP snooping Querier to begin. The IGMP snooping Querier disables itself when a VLAN IP address is cleared, and then it restarts itself when an IP address is re-assigned to the VLAN interface.
- When enabled, IGMP snooping Querier will not start if there is a statically configured multicast router interface in the VLAN.
- When enabled, IGMP snooping Querier starts after one query interval in case no IGMP general query (with IP SA lower than its VLAN IP address) is received on any of its VLAN members.
- When enabled, IGMP snooping Querier periodically sends general queries with an IP source address of the VLAN interface. If it receives a general query on any of its VLAN member, it will check the IP source address of the incoming frame.
- If the IP SA in the incoming IGMP general query frame is lower than the IP address of the VLAN interface, then the switch disables its IGMP snooping Querier functionality.
- If the IP SA of the incoming IGMP general query is higher than the VLAN IP address, the switch will continue to work as an IGMP snooping Querier.

ip igmp access-group

Use this feature to specify access control for packets.

Syntax

ip igmp access-group access-list

Parameters

access-list Enter the name of the extended ACL (16 characters maximum).

Defaults

Not configured

Command Modes

INTERFACE (conf-if-interface-slot/port)

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The access list accepted is an extended ACL. This feature is used to block IGMP reports from hosts, on a per-interface basis; based on the group address and source address specified in the access list.

ip igmp group-join-limit

Use this feature to limit the number of IGMP groups that can be joined in a second.

Syntax

ip igmp group-join-limit number

Parameters

number Enter the number of IGMP groups permitted to join in a second. Range: 1 to 10000

Defaults

none

Command Modes

CONFIGURATION (conf-if-interface-slot/port)
ip igmp querier-timeout

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

Syntax

```plaintext
ip igmp querier-timeout seconds
```

To return to the default value, enter no ip igmp querier-timeout.

Parameters

- `seconds` Enter the number of seconds the router must wait to become the new querier.
- Default: 125 seconds
- Range: 60 to 300

Defaults

125 seconds

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ip igmp query-interval

Change the transmission frequency of IGMP general queries sent by the Querier.

Syntax

```plaintext
ip igmp query-interval seconds
```

To return to the default values, enter no ip igmp query-interval.

Parameters

- `seconds` Enter the number of seconds between queries sent out.
- Default: 60 seconds
- Range: 1 to 18000

Defaults

60 seconds

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ip igmp query-max-resp-time

Set the maximum query response time advertised in general queries.

Syntax

```plaintext
ip igmp query-max-resp-time seconds
```

To return to the default values, enter no ip igmp query-max-resp-time.
### ip igmp version

Manually set the version of the router to IGMPv2 or IGMPv3.

**Syntax**

```
ip igmp version {2 | 3}
```

**Parameters**

- **2**: Enter the number 2 to set the IGMP version number to IGMPv2.
- **3**: Enter the number 3 to set the IGMP version number to IGMPv3.

**Defaults**

- 2 (that is IGMPv2)

**Command Modes**

- INTERFACE

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### ip igmp snooping enable

Enable IGMP snooping on all or a single VLAN. This is the master on/off switch to enable IGMP snooping.

**Syntax**

```
ip igmp snooping enable
```

**Defaults**

- Disabled

**Command Modes**

- CONFIGURATION
- INTERFACE VLAN

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must enter this command to enable IGMP snooping. When enabled from CONFIGURATION mode, IGMP snooping is enabled on all VLAN interfaces (except default VLAN).

**Note:** You must execute the `no shutdown` command on the VLAN interface for IGMP Snooping to function.
ip igmp snooping fast-leave

Enable IGMP snooping fast leave for this VLAN.

**Syntax**

```
ip igmp snooping fast-leave
```

To disable IGMP snooping fast leave, use the `no igmp snooping fast-leave` command.

**Defaults**

Not configured

**Command Modes**

INTERFACE VLAN — (conf-if-vl-<n>)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Queriers normally send a certain number of queries when a leave message is received prior to deleting a group from the membership database. There may be situations in which *fast* deletion of a group is required. When you enable IGMP fast leave processing, the switch removes an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

ip igmp snooping flood

This command controls the flooding behavior of unregistered multicast data packets. When flooding is disabled, unregistered multicast data traffic is forwarded to *only* multicast router ports, both static and dynamic, in a VLAN. If there is no multicast router port in a VLAN, unregistered multicast data traffic is dropped.

On the MXL Switch, when you configure `no ip igmp snooping flood`, the system forwards the frames on mrouter ports for first 96 IGMP snooping enabled VLANs. For all other VLANs, unregistered multicast packets are dropped.

**Syntax**

```
ip igmp snooping flood
```

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
ip igmp snooping last-member-query-interval

The last member query interval is the maximum response time inserted into Group-Specific queries sent in response to Group-Leave messages. This interval is also the interval between successive Group-Specific Query messages. Use this command to change the last member query interval.

Syntax

```
ip igmp snooping last-member-query-interval milliseconds
```

To return to the default value, enter no igmp snooping last-member-query-interval.

Parameters

```
milliseconds  Enter the interval in milliseconds.
              Default: 1000 milliseconds
              Range: 100 to 65535
```

Defaults

1000 milliseconds

Command Modes

INTERFACE VLAN

Command History

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

Syntax

```
ip igmp snooping mrouter interface interface
```

To delete a specific multicast router interface, use the no igmp snooping mrouter interface interface command.

Parameters

```
interface interface  Enter the following keywords and slot/port or number information:

  • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  • For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.
  • For a Port Channel interface, enter the keyword port-channel followed by a number:
    Range: 1 to 128
```

Defaults

Not configured

Command Modes

INTERFACE VLAN — (conf-if-vl-)

Command History

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Usage Information

FTOS provides the capability of statically configuring interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the ip igmp snooping mrouter interface command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.
ip igmp snooping querier
Enable IGMP querier processing for the VLAN interface.

Syntax
ip igmp snooping querier

To disable IGMP querier processing for the VLAN interface, enter no ip igmp snooping querier command.

Defaults
Not configured

Command Modes
INTERFACE VLAN — (conf-if-vl-n)

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
This command enables the IGMP switch to send General Queries periodically. This is useful when there is no multicast router present in the VLAN because the multicast traffic does not need to be routed. An IP address must be assigned to the VLAN interface for the switch to act as a querier for this VLAN.

show ip igmp snooping mrouter
Display multicast router interfaces.

Syntax
show ip igmp snooping mrouter [vlan number]

Parameters
vlan number Enter the keyword vlan followed by the vlan number.
Range: 1 to 4094

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 19-1. show ip igmp snooping mrouter Command Example

FTOS#show ip igmp snooping mrouter
Interface Router Ports
Vlan 2 Te 13/3, Po 1
FTOS#

Related Commands
show ip igmp groups Use this IGMP command to view groups.
Interfaces

Overview

This chapter defines interface commands and is divided into the following sections:

- Basic Interface Commands
- Port Channel Commands
- Time Domain Reflectometer (TDR)
- UDP Broadcast

Basic Interface Commands

The following commands are for physical, loopback, and null interfaces:

- clear counters
- clear dampening
- cx4-cable-length
- dampening
- description
- duplex (1000/10000 Interfaces)
- flowcontrol
- interface
- interface loopback
- interface ManagementEthernet
- interface null
- interface range
- interface range macro (define)
- interface range macro name
- interface vlan
- intf-type cr4 autoneg
- keepalive
- monitor interface
- mtu
- negotiation auto
- portmode hybrid
- rate-interval
- show config
- show config (from INTERFACE RANGE mode)
- show interfaces
- show interfaces configured
- show interfaces dampening
- show interfaces description
- show interfaces stack-unit
- show interfaces status
- show interfaces switchport
- show interfaces transceiver
- show range
- shutdown
- speed (for 1000/10000/auto interfaces)
- stack-unit portmode

**clear counters**

Clear the counters used in the show interfaces commands for all VRRP groups, VLANs, and physical interfaces, or selected ones.

**Syntax**

```
clear counters [interface] [vrrp [vrid | vrf instance]] | learning-limit
```

**Parameters**

- **interface** (OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface:
  - For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number. Range: 1-128
  - For the management interface on the stack-unit, enter the keyword `managementethernet` followed by slot/port information. The slot range is 0-1, and the port range is 0.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

- **vrrp** (OPTIONAL) Enter the keyword `vrrp` to clear the counters of all VRRP groups. To clear the counters of a specified group, enter a `vrid` number from 1 to 255.

- **vrrp** (OPTIONAL): Enter the keyword `vrrp` to clear counters for all VRRP groups. To clear the counters of VRRP groups in a specified VRF instance, enter the name of the instance (32 characters maximum).

- **learning-limit** (OPTIONAL) Enter the keyword `learning-limit` to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.

**Defaults**

Without a specific interface specified, the command clears all interface counters.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
clear dampening

Clear the dampening counters on all the interfaces or just the specified interface.

Syntax

clear dampening [interface]

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keyword port-channel followed by a number. Range: 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

Defaults

Without a specific interface specified, the command clears all interface dampening counters

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

On the MXL Switch, after you enter the clear counters command and verify the results with the show interfaces command, the line rate is not reset to 0.00%.

Example

Figure 20-2. clear dampening Command Example

FTOS#clear dampening tengigabitethernet 1/2
Clear dampening counters on tengig 1/2 [confirm] y
FTOS#

Related Commands

show interfaces dampening Displays interface dampening information.
dampening Configures dampening on an interface.

cx4-cable-length

Configure the length of the cable to be connected to the selected CX4 port.

Syntax

[no] cx4-cable-length {long | medium | short}
Parameters

<table>
<thead>
<tr>
<th>long</th>
<th>medium</th>
<th>short</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the keyword that matches the cable length to be used at the selected port:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>short = For 1-meter and 3-meter cable lengths</td>
<td></td>
<td></td>
</tr>
<tr>
<td>medium = For 5-meter cable length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>long = For 10-meter and 15-meter cable lengths</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Defaults

medium

Command Mode

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command only works on ports that the system recognizes as CX4 ports. The figure below shows an attempt to configure an XFP port with the command after inserting a CX4 converter into the port:

Example

**Figure 20-3. Example of Unsuccessful CX4 Cable Length Configuration**

```
FTOS#show interfaces tengigabitethernet 0/26 | grep "XFP type"
Pluggable media present, XFP type is 10GBASE-CX4
FTOS(conf-if-te-0/26)#cx4-cable-length short
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length medium
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length long
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#
```

**Figure 20-4. Example of CX4 Cable Length Configuration**

```
FTOS(conf-if-te-0/26)#cx4-cable-length short
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length medium
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length long
% Error: Unsupported command.
```

For details on using XFP ports with CX4 cables, refer to your MXL Switch hardware guide.

Related Commands

| show config | Displays the configuration of the selected interface. |

**dampening**

Configures dampening on an interface.

**Syntax**

dampening [[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]

To disable dampening, use the no dampening [[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]] command syntax.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>half-life</strong></td>
<td>Enter the number of seconds after which the penalty is decreased. The penalty is decreased by half after the half-life period expires. Range: 1 to 30 seconds Default: 5 seconds</td>
</tr>
<tr>
<td><strong>reuse-threshold</strong></td>
<td>Enter a number as the reuse threshold, the penalty value below which the interface state is changed to “up”. Range: 1 to 20000 Default: 750</td>
</tr>
<tr>
<td><strong>suppress-threshold</strong></td>
<td>Enter a number as the suppress threshold, the penalty value above which the interface state is changed to “error disabled”. Range: 1 to 20000 Default: 2500</td>
</tr>
<tr>
<td><strong>max-suppress-time</strong></td>
<td>Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. Range: 1 to 86400 Default: 20 seconds</td>
</tr>
</tbody>
</table>

### Defaults

Disabled

### Command Modes

INTERFACE (conf-if-)

### Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

### Example

**Figure 20-5.  dampening Command Example**

```
FTOS(conf-if-tengig-3/2)#dampening 20 800 4500 120
FTOS(conf-if-tengig-3/2)#
```

### Usage Information

With each flap, FTOS penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the configured half-life. After the accumulated penalty exceeds the suppress threshold value, the interface is moved to the Error-Disabled state. This interface state is deemed as “down” by all static/dynamic Layer 2 and Layer 3 protocols. The penalty is exponentially decayed based on the half-life timer. Once the penalty decays below the reuse threshold, the interface is enabled. The configured parameters should follow:

- **suppress-threshold** should be greater than **reuse-threshold**
- **max-suppress-time** should be at least four times **half-life**

**Note:** Dampening cannot be applied on an interface that is monitoring traffic for other interfaces.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dampening</td>
<td>Clears the dampening counters on all the interfaces or just the specified interface.</td>
</tr>
<tr>
<td>show interfaces dampening</td>
<td>Displays interface dampening information.</td>
</tr>
</tbody>
</table>
**description**

Assign a descriptive text string to the interface.

**Syntax**

```
description desc_text
```

To delete a description, enter `no description`.

**Parameters**

- `desc_text` Enter a text string up to 240 characters long. To use special characters as a part of the description string, you must enclose the whole string in double quotes.

**Defaults**

No description is defined.

**Command Modes**

INTERFACE

**Command History**

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks ("desc_text").
- Entering a text string after the `description` command overwrites any previous text string configured as the description.
- The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the `show interfaces description` command to display descriptions configured for each interface.

**Related Commands**

- `show interfaces description` Displays the description field of interfaces.

**duplex (1000/10000 Interfaces)**

Configure duplex mode on any physical interfaces where the speed is set to 1000/10000.

**Syntax**

```
duplex {half | full}
```

To return to the default setting, use the `no duplex` command.

**Parameters**

- `half` Enter the keyword `half` to set the physical interface to transmit only in one direction.
- `full` Enter the keyword `full` to set the physical interface to transmit in both directions.

**Defaults**

Not configured

**Command Modes**

INTERFACE

**Command History**

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.
This command applies to any physical interface with speed set to 1000/10000.

**Note:** Starting with FTOS 7.8.1.0, when a copper SFP2 module with catalog number GP-SFP2-1T is used, its speed can be manually set with the `speed` command. When the speed is set to 10 or 100 Mbps, the `duplex` command can also be executed.

---

```
Related Commands
---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>speed (for 1000/10000/auto interfaces)</code></td>
<td>Sets the speed on the Base-T Ethernet interface.</td>
</tr>
<tr>
<td><code>negotiation auto</code></td>
<td>Enables or disables auto-negotiation on an interface.</td>
</tr>
</tbody>
</table>
```

---

**flowcontrol**

Control how the system responds to and generates 802.3x pause frames on 10G and 40G stack units.

**Syntax**

```
flowcontrol rx {off | on} tx {off | on} threshold
```

**Parameters**

- `rx on`: Enter the keywords `rx on` to process the received flow control frames on this port. This is the default value for the receive side.
- `rx off`: Enter the keywords `rx off` to ignore the received flow control frames on this port.
- `tx on`: Enter the keywords `tx on` to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.
- `tx off`: Enter the keywords `tx off` so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.

**Defaults**

```
rx off tx off
```

**Command Modes**

```
INTERFACE
```

**Command History**

```
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
```

---

**Usage Information**

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full duplex flow control, stations implementing the pause operation instruct the MAC to enable reception of frames with a destination address equal to this multicast address.

The pause:

- Starts when *either* the packet pointer or the buffer threshold is met (whichever is met first). When the discard threshold is met, packets are dropped.
- Ends when *both* the packet pointer and the buffer threshold fall below 50% of the threshold settings.

The *discard threshold* defines when the interface starts dropping the packet on the interface. This may be necessary when a connected device does not honor the flow control frame sent by the MXL Switch. The discard threshold should be larger than the *buffer threshold* so that the buffer holds at least hold at least 3 packets.

**On 4-port 10G stack units:** Changes in the flow-control values are not reflected automatically in the `show interface` output for 10G interfaces. This issue results from the fact that 10G interfaces do not support auto-negotiation per-se.

---

**Important Points to Remember**

- `speed (for 1000/10000/auto interfaces)`
- `negotiation auto`
- Do not enable tx pause when buffer carving is enabled. Consult Dell Networking TAC for information and assistance.
- Asymmetric flow control (rx on tx off or rx off tx on) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

  Cannot configure Asymmetric flowcontrol when speed <1G, config ignored
- The only configuration applicable to half duplex ports is rx off tx off. The following error is returned:

  Cannot configure flowcontrol when half duplex is configure, config ignored
- Half duplex cannot be configured when the flow control configuration is on (default is rx on tx on). The following error is returned:

  Cannot configure half duplex when flowcontrol is on, config ignored

**Note:** The flow control must be off (rx off tx off) before configuring the half duplex.

**Example Figure 20-6. show running config (partial) Command Example**

```
FTOS(conf-if-tengig-0/1)#show config
!
interface TenGigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
```

Table 20-1 lists how FTOS negotiates the flow control values between two Dell Networking chassis connected back-to-back using 10G copper ports.

**Table 20-1. Negotiated Flow Control Values**

<table>
<thead>
<tr>
<th>Configured</th>
<th>Negotiated</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocRxConf</td>
<td>LocTxConf</td>
</tr>
<tr>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>off</td>
<td>on</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
</tr>
</tbody>
</table>
### Table 20-1. Negotiated Flow Control Values

<table>
<thead>
<tr>
<th>Configured</th>
<th>Negotiated</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocRxConf</td>
<td>LocTxConf</td>
</tr>
<tr>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>off</td>
<td>on</td>
</tr>
<tr>
<td>off</td>
<td>on</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays the flow configuration parameters (non-default values only).</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Display information on a specific physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

### interface

Configure a physical interface on the switch.

**Syntax**

```
interface interface
```

**Parameters**

- `interface`: Enter one of the following keywords and slot/port or number information:
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

**Figure 20-7. interface Command Example**

```
FTOS(conf)#interface tengig 0/0
FTOS(conf-if-tengig-0/0)#exit#
```

**Usage Information**

- You cannot delete a physical interface.

By default, physical interfaces are disabled (shutdown) and are in Layer 3 mode. To place an interface in mode, ensure that the interface’s configuration does not contain an IP address and enter the Port Channel Commands command.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface loopback</code></td>
<td>Configures a Loopback interface.</td>
</tr>
<tr>
<td><code>interface null</code></td>
<td>Configures a Null interface.</td>
</tr>
<tr>
<td><code>interface port-channel</code></td>
<td>Configures a port channel.</td>
</tr>
<tr>
<td><code>interface vlan</code></td>
<td>Configures a VLAN.</td>
</tr>
<tr>
<td><code>show interfaces</code></td>
<td>Displays interface configuration.</td>
</tr>
</tbody>
</table>
interface loopback

Configure a Loopback interface.

Syntax

```
interface loopback number
```

To remove a loopback interface, use the no interface loopback number command.

Parameters

```
number
```
Enter a number as the interface number.
Range: 0 to 16383.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Figure 20-8.  interface loopback Command Example

FTOS(conf)#interface loopback 1655
FTOS(conf-if-lo-1655)#
```

Related Commands

- `interface` - Configures a physical interface.
- `interface null` - Configures a Null interface.
- `interface port-channel` - Configures a port channel.
- `interface vlan` - Configures a VLAN.

interface ManagementEthernet

Configure the Management port on the system.

Syntax

```
interface ManagementEthernet slot/port
```

Parameters

```
slot/port
```
Enter the keyword ManagementEthernet followed by slot number (0-1) and port number zero (0).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Figure 20-9.  interface ManagementEthernet Command Example

FTOS(conf)#interface managementethernet 0/0
FTOS(conf-if-ma-0/0)#
```

Usage Information

You cannot delete a Management port.
The Management port is enabled by default (no shutdown). Use the ip address command to assign an IP address to the Management port.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>management route</td>
<td>Configure a static route that points to the Management interface or a forwarding router.</td>
</tr>
<tr>
<td>duplex (1000/10000 Interfaces)</td>
<td>Configure duplex mode on any physical interfaces where the speed is set to 1000/10000</td>
</tr>
</tbody>
</table>

## interface null

Configure a Null interface on the switch.

### Syntax

```
interface null number
```

### Parameters

- **number**
  - Enter zero (0) as the Null interface number.

### Defaults

Not configured; `number = 0`

### Command Modes

CONFIGURATION

### Command History

- Introduced in 8.3.16.1 on the MXL 10/40GbE Switch IO Module.

### Example

```
FTOS(conf)#interface null 0
FTOS(conf-if-nu-0)#
```

### Usage Information

You cannot delete the Null interface. The only configuration command possible in a Null interface is `ip unreachables`.

### Related Commands

- interface
- interface loopback
- interface port-channel
- interface vlan
- ip unreachables

## interface range

This command permits configuration of a range of interfaces to which subsequent commands are applied (bulk configuration). Using the `interface range` command, you can enter identical commands for a range of interface.

### Syntax

```
interface range interface, interface,...
```
Enter the keyword `interface range` and one of the interfaces — slot/port, port-channel or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma separated ranges—spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels and physical interfaces.

Slot/Port information must contain a space before and after the dash. For example, `interface range tengigabitethernet 0/1 - 5` is valid; `interface range tengigabitethernet 0/1-5` is not valid.

- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  Range: 1 to 128
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical). Important things to remember:

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The interface range prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis ( ... ).
- When the interface range prompt has multiple port ranges, the smaller port range is excluded from the prompt.
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port.
Only VLAN and port-channel interfaces created using the `interface vlan` and `interface port-channel` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command cannot be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.

**Note:** If a range has VLAN, physical, and port-channel interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN or port-channel, only those respective interfaces should be configured in a particular range.

**Example**

**Figure 20-13. Interface Range prompt Overlapping Port Ranges**

```
FTOS(conf)#interface range tengig 2/1 - 11 , tengig 2/1 - 23
FTOS(conf-if-range-tengig-2/1-23#)
```

**Example**

**Figure 20-14. Single Range Bulk Configuration**

```
FTOS(conf)# interface range tengigabitethernet 5/1 - 23
FTOS(conf-if-range)# no shutdown
FTOS(conf-if-range)#
```

**Example**

**Figure 20-15. Multiple Range Bulk Configuration Gigabit Ethernet and Ten Gigabit Ethernet**

```
FTOS(conf-if)# interface range tengigabitethernet 5/1 - 23, tengigabitethernet 1/1 - 2
FTOS(conf-if-range)# no shutdown
FTOS(conf-if-range)#
```

**Example**

**Figure 20-16. Multiple Range Bulk Configuration with VLAN and port channel**

```
FTOS(conf-if)# interface range tengigabitethernet 5/1 - 23, tengigabitethernet 1/1 - 2,
Vlan 2 - 100 , Port 1 - 25
FTOS(conf-if-range)# no shutdown
FTOS(conf-if-range)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface port-channel</code></td>
<td>Configures a port channel group.</td>
</tr>
<tr>
<td><code>interface vlan</code></td>
<td>Configures a VLAN interface.</td>
</tr>
<tr>
<td><code>show config (from INTERFACE RANGE mode)</code></td>
<td>Shows the bulk configuration interfaces.</td>
</tr>
<tr>
<td><code>show range</code></td>
<td>Shows the bulk configuration ranges.</td>
</tr>
<tr>
<td><code>interface range macro (define)</code></td>
<td>Defines a macro for an interface-range.</td>
</tr>
</tbody>
</table>
**interface range macro (define)**

Defines a macro for an interface range and then saves the macro in the running configuration.

**Syntax**

```plaintext
define interface range macro name interface , interface , ...
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Enter up to 16 characters for the macro name.</td>
</tr>
<tr>
<td>interface , interface , ...</td>
<td>Enter the interface keyword (see below) and one of the interfaces slot/port, port-channel or VLAN numbers. Select the range of interfaces for bulk configuration. You can enter up to six comma separated ranges—spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, interface range tengigabitethernet 0/1 - 5 is valid; interface range tengigabitethernet 0/1-5 is not valid.</td>
</tr>
</tbody>
</table>

- For a Port Channel interface, enter the keyword port-channel followed by a number:
  Range: 1-128
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.
- For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Example**

**Figure 20-17.  define interface-range macro Command Example**

```plaintext
FTOS(conf)# define interface-range test tengigabitethernet 0/0 - 3 , tengigabitethernet 5/0 - 47 , tengigabitethernet 13/0 - 89

FTOS(conf)# show running-config | grep define
define interface-range test tengigabitethernet 0/0 - 3 , tengigabitethernet 5/0 - 47 , tengigabitethernet 13/0 - 89
define interface-range test tengigabitethernet 0/0 - 3 , tengigabitethernet 5/0 - 47 , tengigabitethernet 13/0 - 89

FTOS(conf)#interface range macro test
FTOS(conf-if-range-te-0/0-3,tengig-5/0-47,tengig-13/0-89)#
```

**Usage Information**

Figure 20-17 is an example of how to define an interface range macro named test. To display the macro definition, execute the show running-config command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface range</td>
<td>Configures a range of command (bulk configuration)</td>
</tr>
<tr>
<td>interface range macro name</td>
<td>Runs an interface range macro.</td>
</tr>
</tbody>
</table>
**interface range macro name**

Run the interface-range macro to automatically configure the pre-defined range of interfaces.

**Syntax**

```
interface range macro name
```

**Parameters**

- **name**: Enter the name of an existing macro.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Figure 20-18 runs the macro named `test` that was defined earlier.

**Example**

```
Example Figure 20-18. interface-range macro Command Example
FTOS(conf)#interface range macro test
FTOS(conf-if-range-te-0/0-3,tengig-5/0-47,tengig-13/0-89)#
```

**Related Commands**

- `interface range` Configures a range of command (bulk configuration)
- `interface range macro (define)` Defines a macro for an interface range (bulk configuration)

---

**interface vlan**

Configure a VLAN. You can configure up to 4094 VLANs.

**Syntax**

```
interface vlan vlan-id
```

To delete a VLAN, use the `no interface vlan vlan-id` command.

**Parameters**

- **vlan-id**: Enter a number as the VLAN Identifier. Range: 1 to 4094.

**Defaults**

Not configured, except for the Default VLAN, which is configured as VLAN 1.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Example Figure 20-19. interface vlan Command Example
FTOS(conf)#int vlan 3
FTOS(conf-if-vl-3)#
```

**Usage Information**

For more information about VLANs and the commands to configure them, refer to Virtual LAN (VLAN) Commands.
FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC ACLs are not supported in VLANs. IP ACLs are supported. Refer to Chapter 6, Access Control Lists (ACL).

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configures a physical interface.</td>
</tr>
<tr>
<td>interface loopback</td>
<td>Configures a loopback interface.</td>
</tr>
<tr>
<td>interface null</td>
<td>Configures a null interface.</td>
</tr>
<tr>
<td>interface port-channel</td>
<td>Configures a port channel group.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays the current VLAN configuration on the switch.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables/Enables the VLAN.</td>
</tr>
<tr>
<td>tagged</td>
<td>Adds a Layer 2 interface to a VLAN as a tagged interface.</td>
</tr>
<tr>
<td>untagged</td>
<td>Adds a Layer 2 interface to a VLAN as an untagged interface.</td>
</tr>
</tbody>
</table>

### intf-type cr4 autoneg

Set the interface type as CR4 with auto-negotiation enabled.

**Syntax**

```plaintext
intf-type cr4 autoneg
```

If intf-type cr4 autoneg is configured, use the **no intf-type cr4 autoneg** command to set the interface type as cr4 with autonegotiation disabled.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If interface type is configured as CR4 with auto-negotiation enabled, then the peer should also be configured as CR4 with auto-negotiation. Many DAC cable link issues can be resolved by setting the interface type as CR4.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configures a physical interface.</td>
</tr>
<tr>
<td>interface loopback</td>
<td>Configures a loopback interface.</td>
</tr>
<tr>
<td>interface null</td>
<td>Configures a null interface.</td>
</tr>
<tr>
<td>interface port-channel</td>
<td>Configures a port channel group.</td>
</tr>
</tbody>
</table>

### keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

**Syntax**

```plaintext
keepalive [seconds]
```

To stop sending keepalive packets, use the **no keepalive** command.
### keepalive

When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>(OPTIONAL) For interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. Range: 0 to 23767. Default: 10 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Enabled</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>INTERFACE</th>
</tr>
</thead>
</table>

| Command History | Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module. |

### monitor interface

Monitor counters on a single interface or all interfaces on a stack unit. The screen is refreshed every 5 seconds and the CLI prompt disappears.

**Syntax**

```
monitor interface [interface]
```

To disable monitoring and return to the CLI prompt, press the `q` key.

**Parameters**

<table>
<thead>
<tr>
<th><code>interface</code></th>
<th>(OPTIONAL) Enter the following keywords and slot/port or number information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For the management port, enter the keyword <code>managementethernet</code> followed by the slot (0-1) and the port (0).</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>EXEC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EXEC Privilege</td>
</tr>
</tbody>
</table>

| Command History | Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module. |

| Usage Information | The delta column displays changes since the last screen refresh. |
mtu

Set the Maximum Link MTU (frame size) for an Ethernet interface.

**Syntax**

```
mtu value
```

To return to the default MTU value, use the `no mtu` command.
**Parameters**

<table>
<thead>
<tr>
<th>value</th>
<th>Enter a maximum frame size in bytes.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range: 594 to 9252</td>
</tr>
<tr>
<td></td>
<td>MXL Switch Range: 594 to 12000</td>
</tr>
<tr>
<td></td>
<td>Default: 1554</td>
</tr>
</tbody>
</table>

**Defaults**

1554

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (ip mtu command) must be enough bytes to include the Layer 2 header:

- The IP MTU will get adjusted automatically when the Layer 2 MTU is configured with the mtu command.

When you enter the no mtu command, FTOS reduces the IP MTU value to 1536 bytes.

Link MTU and IP MTU considerations for port channels and VLANs are as follows.

**port channels:**

- All members must have the same link MTU value and the same IP MTU value.
- The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members.

Example: if the members have a link MTU of 2100 and an IP MTU 2000, the port channel’s MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

**VLANs:**

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members.

Example: the VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN’s Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

**Table 20-3. Difference between Link MTU and IP MTU**

<table>
<thead>
<tr>
<th>Layer 2 Overhead</th>
<th>Link MTU and IP MTU Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet (untagged)</td>
<td>18 bytes</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>22 bytes</td>
</tr>
<tr>
<td>Untagged Packet with VLAN-Stack Header</td>
<td>22 bytes</td>
</tr>
<tr>
<td>Tagged Packet with VLAN-Stack Header</td>
<td>26 bytes</td>
</tr>
</tbody>
</table>
negotiation auto

Enable auto-negotiation on an interface.

Syntax

negotiation auto

To disable auto-negotiation, enter no negotiation auto.

Defaults

Enabled

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The no negotiation auto command is only available if you first manually set the speed of a port to 10Mbits or 100Mbits.

The negotiation auto command provides a mode option for configuring an individual port to forced-master/forced slave once auto-negotiation is enabled.

Figure 20-21. negotiation auto Master/Slave Example

If the mode option is not used, the default setting is slave. If you do not configure forced-master or forced slave on a port, the port negotiates to either a master or a slave state. Port status is one of the following:

- Forced-master
- Force-slave
- Master
- Slave
- Auto-neg Error—typically indicates that both ends of the node are configured with forced-master or forced-slave.

⚠️ Caution: Ensure that one end of your node is configured as forced-master and one is configured as forced-slave. If both are configured the same (that is forced-master or forced-slave), the show interfaces command will flap between an auto-neg-error and forced-master/slave states.

You can display master/slave settings with the show interfaces command.
Both sides of the link must have auto-negotiation enabled or disabled for the link to come up.

The following table details the possible speed and auto-negotiation combinations for a line between two 100/1000 Base-T Ethernet interfaces.

Table 20-4. Auto-negotiation and Link Speed Combinations

<table>
<thead>
<tr>
<th>Port 0</th>
<th>Port 1</th>
<th>Link Status between Port 1 and Port 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-negotiation enabled* speed 1000 or auto</td>
<td>auto-negotiation enabled* speed 1000 or auto</td>
<td>Up at 1000 Mb/s</td>
</tr>
<tr>
<td>auto-negotiation enabled speed 100</td>
<td>auto-negotiation enabled speed 100</td>
<td>Up at 100 Mb/s</td>
</tr>
<tr>
<td>auto-negotiation disabled speed 100</td>
<td>auto-negotiation disabled speed 100</td>
<td>Up at 100 Mb/s</td>
</tr>
<tr>
<td>auto-negotiation disabled speed 100</td>
<td>auto-negotiation disabled speed 100</td>
<td>Down</td>
</tr>
<tr>
<td>auto-negotiation enabled* speed 1000 or auto</td>
<td>auto-negotiation disabled speed 100</td>
<td>Down</td>
</tr>
</tbody>
</table>

* You cannot disable auto-negotiation when the speed is set to 1000 or auto.

Related Commands

- **speed (for 1000/10000/auto interfaces)**
  - Set the link speed to 1000, 10000, or auto-negotiate the speed.

**portmode hybrid**

Set a physical port or port-channel to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.

**Syntax**

```
portmode hybrid
```

To return a port to accept either tagged or untagged frames (non-hybrid), use the `no portmode hybrid` command.

**Defaults**

non-hybrid

**Command Modes**

INTERFACE (conf-if-`interface-slot/port`)
Figure 20-23. portmode hybrid Configuration Example

```
FTOS(conf)#interface tengig 0/20
FTOS(conf-if-te-0/20)#no shut
FTOS(conf-if-te-0/20)#portmode hybrid
FTOS(conf-if-te-0/20)#sw
FTOS(conf-if-te-0/20)#int vlan 10
FTOS(conf-if-vl-10)#tag tengig 0/20
FTOS(conf-if-vl-10)#int vlan 20
FTOS(conf-if-vl-20)#untag tengig 0/20
FTOS(conf-if-vl-20)#
```

Figure 20-23 sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10, which becomes the native VLAN of the port. The port will now accept:

- untagged frames and classify them as VLAN 10 frames
- VLAN 20 tagged frames

The next figure is an example show output with “Hybrid” as the newly added value for 802.1QTagged. The options for this field are:

- True—port is tagged
- False—port is untagged
- Hybrid—port accepts both tagged and untagged frames
**Example**

**Figure 20-24. Display the Tagged Hybrid Interface**

```
FTOS(conf)#interface tengig 0/20
FTOS(conf-if-te-0/20)#no shut
FTOS(conf-if-te-0/20)#portmode hybrid
FTOS(conf-if-te-0/20)#int vlan 10
FTOS(conf-if-vl-10)#int tengig 0/20
FTOS(conf-if-vl-20)# untag tengig 0/20

FTOS (conf-if-vl-20)#

FTOS (conf)#do show interfaces switchport tengigabitethernet 3/20
```

Codes:  U - Untagged, T - Tagged
x - Dot1x untagged, X - Dot1x tagged
G - GVRP tagged, M - Trunk, H - VSN tagged
i - Internal untagged, I - Internal tagged, v - VLT untagged,
V - VLT tagged

Name: TenGigabitEthernet 3/20
802.1QTagged: Hybrid
Vlan membership:
Q       Vlans
U       20
T       10
Native VlanId:    20.

```
FTOS(conf)#
```

**Figure 20-25** is an example of unconfiguration of the hybrid port using the `no portmode hybrid` command.

**Note:** You must remove all other configurations on the port before you can remove the hybrid configuration from the port.

**Example**

**Figure 20-25. Unconfigure the hybrid port**

```
FTOS(conf-if-vl-20)#interface vlan 10
FTOS(conf-if-vl-10)#no untagged tengig 0/20
FTOS(conf-if-vl-10)#interface vlan 20
FTOS(conf-if-vl-20)#no tagged tengig 0/20
FTOS(conf-if-vl-20)#interface tengig 0/20
FTOS(conf-if-te-0/20)#no portmode hybrid
FTOS(conf-if-vl-20)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces switchport</code></td>
<td>Displays the configuration of switchport (Layer 2) interfaces on the switch.</td>
</tr>
<tr>
<td><code>vlan-stack trunk</code></td>
<td>Specifies an interface as a trunk port to the Stackable VLAN network.</td>
</tr>
</tbody>
</table>
rate-interval

Configure the traffic sampling interval on the selected interface.

Syntax

rate-interval seconds

Parameters

seconds Enter the number of seconds for which to collect traffic data.
Range: 5 to 299 seconds

Note: For 0-5 seconds, polling occurs every 5 seconds. For 6-10 seconds, polling occurs every 10 seconds. For any other value, polling occurs every 15 seconds.

Defaults

299 seconds

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The configured rate interval is displayed, along with the collected traffic data, in the output of show interfaces commands.

Related Commands

show interfaces Displays information on physical and virtual interfaces.

show config

Display the interface configuration.

Syntax

show config

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 20-26. show config Command Example for the INTERFACE Mode

```
FTOS(conf-if)#show conf
!
interface TenGigabitEthernet 1/7
  no ip address
  switchport
  no shutdown
FTOS(conf-if)#
```
show interfaces

Display information on a specific physical interface or virtual interface.

**Syntax**

show interfaces interface

**Parameters**

- **interface**: Enter one of the following keywords and slot/port or number information:
  - For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For the management interface, enter the keyword `ManagementEthernet` followed by the slot/port information. The slot range is 0 to 1 and the port range is 0.
  - For a Null interface, enter the keywords `null 0`.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number: Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage**

Use this `show interfaces` command for details on a specific interface. Use the `show interfaces stack-unit` command for details on all interfaces on the designated stack unit.

On the MXL Switch, the show interface output displays incorrect rate information details over time for link monitoring when the rate-interval is configured for 5 seconds. Dell Networking recommends using higher rate-intervals such as 15 to 299 seconds to minimize the errors seen.

**Note:** In the CLI output, the power value will be rounded to a 3-digit value. For receive/transmit power that is less than 0.000, an snmp query will return the corresponding dbm value even though the CLI displays as 0.000.
Note: After the counters are cleared, the line-rate continues to increase until it reaches the maximum line rate. When the maximum line rate is reached, there will be no change in the line-rate.

**Example**  Figure 20-28. show interfaces Command Example for 10G Port

```
FTOS#show interfaces tengigabitethernet 2/0
TenGigabitEthernet 2/0 is up, line protocol is up
Hardware is Dell Force10Eth, address is 00:01:e8:05:f7:3a
Interface index is 100990998
Internet address is 213.121.22.45/28
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 02:31:45
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  Input 0 IP Packets, 0 Vlans 0 MPLS
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 symbol errors, 0 runts, 0 giants, 0 throttles
  0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
Output Statistics:
  1 packets, 64 bytes, 0 underruns
  0 Multicasts, 2 Broadcasts, 0 Unicasts
  0 IP Packets, 0 Vlans, 0 MPLS
  0 throttles, 0 discarded
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:00:27
```

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet 2/0...</td>
<td>Displays the interface’s type, slot/port, and administrative and line protocol status.</td>
</tr>
<tr>
<td>Hardware is...</td>
<td>Displays the interface’s hardware information and its assigned MAC address.</td>
</tr>
<tr>
<td>Interface index...</td>
<td>Displays the interface index number used by SNMP to identify the interface.</td>
</tr>
<tr>
<td>Internet address...</td>
<td>States whether an IP address is assigned to the interface. If one is, that address is displayed.</td>
</tr>
<tr>
<td>MTU 1554...</td>
<td>Displays link and IP MTU information. If the chassis is in Jumbo mode, this number can range from 576 to 9252.</td>
</tr>
<tr>
<td>LineSpeed</td>
<td>Displays the interface’s line speed.</td>
</tr>
<tr>
<td>ARP type:...</td>
<td>Displays the ARP type and the ARP timeout value for the interface.</td>
</tr>
<tr>
<td>Last clearing...</td>
<td>Displays the time when the show interfaces counters were cleared.</td>
</tr>
<tr>
<td>Queuing strategy...</td>
<td>States the packet queuing strategy. FIFO means first in first out.</td>
</tr>
</tbody>
</table>

Table 20-5. Lines in show interfaces Command Example
<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
</table>
| Input Statistics: | Displays all the input statistics including:  
  • Number of packets and bytes into the interface  
  • Number of packets with IP headers and VLAN tagged headers.  
  **Note:** The sum of the number of packets may not be as expected since a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.  
  • Packet size and the number of those packets inbound to the interface  
  • Number of symbol errors, runts, giants, and throttles packets:  
    symbol errors = number packets containing bad data. That is, the port MAC detected a physical coding error in the packet.  
    runts = number of packets that are less than 64B  
    giants = packets that are greater than the MTU size  
    throttles = packets containing PAUSE frames  
  • Number of CRC, IP Checksum, overrun, and discarded packets:  
    CRC = packets with CRC/FCS errors  
    IP Checksum = packets with IP Checksum errors  
    overrun = number of packets discarded due to FIFO overrun conditions  
    discarded = the sum of input symbol errors, runts, giants, CRC, IP Checksum, and overrun packets discarded without any processing |
| Output Statistics: | Displays output statistics sent out of the interface including:  
  • Number of packets, bytes and underruns out of the interface  
    packets = total number of packets  
    bytes = total number of bytes  
    underruns = number of packets with FIFO underrun conditions  
  • Number of Multicast, Broadcast and Unicast packets:  
    Multicasts = number of MAC multicast packets  
    Broadcasts = number of MAC broadcast packets  
    Unicasts = number of MAC unicast packets  
  • Number of throttles and discards packets:  
    throttles = packets containing PAUSE frames  
    discarded = number of packets discarded without any processing |
| Rate information... | Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds).  
  Traffic rate is displayed in bits, packets per second, and percent of line rate. |
| Time since... | Elapsed time since the last interface status change (hh:mm:ss format). |
Example

Figure 20-29.  show interfaces Command Example for 1G SFP Interface

```
FTOS#show interfaces tengigabitethernet 0/44
TenGigabitEthernet 0/44 is up, line protocol is up
Hardware is DellForce10Eth, address is 00:01:e8:43:00:01
Current address is 00:01:e8:43:00:01
Port is present
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
SFP+ receive power reading is -3.6041dBm
Interface index is 45420801
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :tenG1730001e8430001
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 21:14:32
Queueing strategy: fifo
Input Statistics:
  94322888 packets, 603664832 bytes
  94322888 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 94322888 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  180384 packets, 11926850 bytes, 0 underruns
  172622 64-byte pkts, 7762 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  7762 Multicasts, 87726 Broadcasts, 84896 Unicasts
  0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 21:13:36
```

Figure 20-30.  show interfaces ManagementEthernet Command Example

```
FTOS#show interface managementethernet ?
0/0                     Management Ethernet interface number
FTOS#show interface managementethernet 0/0
ManagementEthernet 0/0 is up, line protocol is up
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:05
    Current address is 00:1e:c9:f1:00:05
    Pluggable media not present
    Interface index is 235159752
    Internet address is 10.11.209.87/16
    Mode of IP Address Assignment : MANUAL
    DHCP Client-ID: mgmt001ec9f10005
    Virtual-IP is not set
    Virtual-IP IPv6 address is not set
    MTU 1554 bytes, IP MTU 1500 bytes
    LineSpeed 100 Mbit, Mode full duplex
    ARP type: ARPA, ARP Timeout 04:00:00
    Last clearing of "show interface" counters 5d4h57m
    Queueing strategy: fifo
    Input 3448753 packets, 950008323 bytes, 0 errors, 0 discarded
    Output 8627 packets, 814226 bytes, 0 multicast
    Output 8627 errors, 0 invalid protocol
```

Usage Information

The interface counter “over 1023-byte pkts” does not increment for packets in the range 9216 > x < 1023.

The Management port is enabled by default (no shutdown). If necessary, use the ip address command to assign an IP address to the Management port.
## show interfaces configured

Display any interface with a non-default configuration.

### Syntax

```
show interfaces configured
```

### Command Modes

- EXEC
- EXEC Privilege

### Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
FTOS#show interfaces configured
TenGigabitEthernet 13/18 is up, line protocol is up
  Hardware is DellForce10Eth, address is 00:01:e8:05:f7:fc
  Current address is 00:01:e8:05:f7:fc
  Interface index is 474791997
  Internet address is 1.1.1.1/24
  MTU 1554 bytes, IP MTU 1500 bytes
  LineSpeed 1000 Mbit, Mode full duplex, Master
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interfaces" counters 00:12:42
  Queueing strategy: fifo
  Input Statistics:
    10 packets, 10000 bytes
    0 Vlans
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 10 over 511-byte pkts, 0 over 1023-byte pkts
    0 Multicasts, 0 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
  Output Statistics:
    1 packets, 64 bytes, 0 underruns
    1 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
    0 Multicasts, 1 Broadcasts, 0 Unicasts
    0 Vlans, 0 throttles, 0 discarded, 0 collisions
  Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Time since last interface status change: 00:04:59

FTOS#
```

### Related Commands

- `show interfaces switchport`: Displays Layer 2 information about the interfaces.
- `show inventory`: Displays the MXL switch type, components (including media), FTOS version including hardware identification numbers and configured protocols.
- `strict-priority unicast`: Displays information of either rate limiting or rate policing on the interface.
- `show interfaces stack-unit`: Displays information on all interfaces on a specific stack unit.
- `show interfaces configured`: Displays any interface with a non-default configuration.
- `show range`: Displays all interfaces configured using the interface range command.
- `show interfaces`: Displays information on a specific physical interface or virtual interface.
- `show memory`: Displays the stack unit(s) status.
- `show ip interface`: Displays Layer 3 information about the interfaces.
- `show interfaces switchport`: Displays Layer 3 information about the interfaces.
- `show interfaces switchport`: Displays the stack unit(s) status.
- `show interfaces configured`: Displays any interface with a non-default configuration.
- `show interfaces configured`: Displays any interface with a non-default configuration.
show interfaces dampening

Display interface dampening information.

**Syntax**

```
show interfaces dampening [[interface] [summary] [detail]]
```

**Parameters**

- **interface** (OPTIONAL) Enter one of the following keywords and slot/port or number information:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
- **summary** (OPTIONAL) Enter the keyword `summary` to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.
- **detail** (OPTIONAL) Enter the keyword `detail` to display detailed interface dampening data.

**Defaults**

`none`

**Command Modes**

EXEC

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
FTOS#show interfaces dampening
Interface     Supp     Flaps     Penalty     Half-Life    Reuse     Suppress    Max-Sup
State
tengig 3/2        Up       0         0           20           800       4500        120
tengig 3/10       Up       0         0           5            750       2500        20
FTOS#
```

**Related Commands**

- `dampening` Configures dampening on an interface
- `show interfaces` Displays information on a specific physical interface or virtual interface.
- `show interfaces configured` Displays any interface with a non-default configuration.
show interfaces description

Display the descriptions configured on the interface.

**Syntax**

```
show interfaces [interface] description
```

**Parameters**

- `interface` Enter one of the following keywords and slot/port or number information:
  - For Loopback interfaces, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For the management interface on the stack unit enter the keyword `ManagementEthernet` followed by the slot/port information. The slot range is 0-0 and the port range is 0.
  - For the Null interface, enter the keywords `null 0`.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For VLAN interfaces, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
FTOS#show interface description

Interface          OK Status  Protocol  Description
TenGigabitEthernet 0/1      NO  admin down  down
TenGigabitEthernet 0/2      NO  admin down  down
TenGigabitEthernet 0/3      NO  admin down  down
TenGigabitEthernet 0/4      NO  admin down  down
TenGigabitEthernet 0/5      NO  admin down  down
TenGigabitEthernet 0/6      NO  admin down  down
TenGigabitEthernet 0/7      NO  up         down
TenGigabitEthernet 0/8      YES up         up
TenGigabitEthernet 0/9      NO  admin down  down
TenGigabitEthernet 0/10     NO  admin down  down
TenGigabitEthernet 0/11     NO  admin down  down
TenGigabitEthernet 0/12     NO  admin down  down
TenGigabitEthernet 0/13     NO  admin down  down
TenGigabitEthernet 0/14     NO  admin down  down
TenGigabitEthernet 0/15     NO  admin down  down
TenGigabitEthernet 0/16     YES up         up
TenGigabitEthernet 0/17     NO  admin down  down
TenGigabitEthernet 0/18     NO  admin down  down
TenGigabitEthernet 0/19     NO  admin down  down
TenGigabitEthernet 0/20     NO  admin down  down
TenGigabitEthernet 0/21     NO  admin down  down
```

**Table 20-6. show interfaces description Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays type of interface and associated slot and port number.</td>
</tr>
<tr>
<td>OK?</td>
<td>Indicates if the hardware is functioning properly.</td>
</tr>
<tr>
<td>Status</td>
<td>States whether the interface is enabled (up) or disabled (administratively down).</td>
</tr>
</tbody>
</table>
show interfaces

Display information on all interfaces on a specific MXL Switch stack member.

Syntax

show interfaces stack-unit unit-number

Parameters

- `unit-number`: Enter the stack member number (0 to 5).

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
FTOS#show interfaces stack-unit 0
TenGigabitEthernet 0/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:05
  Current address is 00:1e:c9:f1:00:05
  Server Port AdminState is Down
  Pluggable media not present
  Interface index is 34148609
  Internet address is not set
  Mode of IP Address Assignment : NONE
  DHCP Client-ID :tenG130001ec9f10005
  MTU 1554 bytes, IP MTU 1500 bytes
  LineSpeed auto
  Flowcontrol rx off tx off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters 5d5h23m
  Queueing strategy: fifo
  Input Statistics:
  0 packets, 0 bytes
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
  Output Statistics:
  0 packets, 0 bytes, 0 underruns
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 collisions
  Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Time since last interface status change: 5d5h23m

!----------------output truncated ------------------!
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show hardware stack-unit</td>
<td>Displays data plane and management plane input/output statistics.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays information on a specific physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**show interfaces status**

Display a summary of interface information or specify a stack unit and interface to display status information for that specific interface only.

**Syntax**

```
show interfaces [interface | stack-unit unit-number] status
```

**Parameters**

- **interface**
  - (OPTIONAL) Enter one of the following keywords and slot/port or number information:
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Figure 20-35. show interfaces status Command Example

FTOS#show interface status
Port    Description  Status    Speed    Duplex Vlan
Te 0/1    Down        Auto      Auto    --
Te 0/2    Down        Auto      Auto    --
Te 0/3    Down        Auto      Auto    --
Te 0/4    Down        Auto      Auto    --
Te 0/5    Down        Auto      Auto    --
Te 0/6    Down        Auto      Auto    --
Te 0/7    Down        Auto      Auto    --
Te 0/8    Up          10000 Mbit Full --
Te 0/9    Down        Auto      Auto    --
Te 0/10   Down        Auto      Auto    --
Te 0/11   Down        Auto      Auto    --
Te 0/12   Down        Auto      Auto    --
Te 0/13   Down        Auto      Auto    --
Te 0/14   Down        Auto      Auto    --
Te 0/15   Down        Auto      Auto    --
Te 0/16   Up          10000 Mbit Full --
FTOS#
```

**Related Commands**

- show interfaces - Displays information on a specific physical interface or virtual interface.
show interfaces switchport

Display only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces’ IEEE 802.1Q tag status and VLAN membership.

Syntax

`show interfaces switchport [interface | stack-unit unit-id ]`

Parameters

- **interface**: Enter one of the following keywords and slot/port or number information:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - Enter the keyword `backup` to view the backup interface for this interface.

- **stack-unit unit-id**: (OPTIONAL) Enter the keyword `stack-unit` followed by the stack member number.
  Range: 0 to 5

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.
Example

### Figure 20-36. show interfaces switchport Command Example

```
FTOS#show interfaces switchport
Codes:  U - Untagged, T - Tagged
       x - Dot1x untagged, X - Dot1x tagged
       G - GVRP tagged, M - Trunk, H - VSN tagged
       i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT

Name: TenGigabitEthernet 3/20
  802.1QTagged: Hybrid
  Vlan membership:
    Q: Vlans
    U: 20
    T: 10
  Native VlanId: 20.
Name: TenGigabitEthernet 5/20
  802.1QTagged: False
  Vlan membership:
    Q: Vlans
    U: 1
Name: TenGigabitEthernet 5/21
  802.1QTagged: False
  Vlan membership:
    Q: Vlans
    U: 1
Name: TenGigabitEthernet 5/49 (Port-channel 128)
  802.1QTagged: True
  Vlan membership:
    Q: Vlans
    G: 10
Name: Port-channel 128
  802.1QTagged: True
  Vlan membership:
    Q: Vlans
FTOS#
```

### Table 20-7. Items in show interfaces switchport Command Example

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the interface’s type, slot and port number.</td>
</tr>
<tr>
<td>802.1QTagged</td>
<td>Displays whether if the VLAN tagged (“True”), untagged (“False”), or hybrid (“Hybrid”), which supports both untagged and tagged VLANs by port 13/0.</td>
</tr>
<tr>
<td>Vlan membership</td>
<td>Lists the VLANs to which the interface is a member. Starting with FTOS 7.6.1, this field can display native VLAN membership by port 13/0.</td>
</tr>
</tbody>
</table>

### Related Commands

- `interface` Configures a physical interface on the switch.
- `show ip interface` Displays Layer 3 information about the interfaces.
- `show interfaces` Displays information on a specific physical interface or virtual interface.
- `show interfaces transceiver` Displays the physical status and operational status of an installed transceiver. The output also displays the transceiver’s serial number.
show interfaces transceiver

Display the physical status and operational status of an installed transceiver. The output also displays the transceiver’s serial number.

**Syntax**

```
show interfaces [tengigabitethernet slot/port | fortyGigE slot/port] transceiver
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tengigabitethernet</td>
<td>For a 10G interface, enter the keyword tengigabitethernet followed by the slot/port information.</td>
</tr>
<tr>
<td>fortyGigE</td>
<td>For a 40G interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage**

See Figure 20-37 for an command example and see Table 20-8 for a description of the output fields.
Figure 20-37. show interfaces tengigabitethernet transceiver Command Example

Example

```
FTOS#show interfaces tengigabitethernet 1/0 transceiver
SFP is present.
SFP 0 Serial Base ID fields
  SFP 0 Id = 0x03
  SFP 0 Ext Id = 0x04
  SFP 0 Connector = 0x07
  SFP 0 Transceiver Code = 0x20 0x00 0x00 0x01 0x20 0x40 0x0c 0x05
  SFP 0 Encoding = 0x01
  SFP 0 BR Nominal = 0x15
  SFP 0 Length(9um) Km = 0x00
  SFP 0 Length(9um) 100m = 0x00
  SFP 0 Length(50um) 10m = 0x1e
  SFP 0 Length(62.5um) 10m = 0x0f
  SFP 0 Length(Copper) 10m = 0x00
  SFP 0 Vendor Rev = A
  SFP 0 Laser Wavelength = 850 nm
  SFP 0 CheckCodeBase = 0x66
  SFP 0 Serial Extended ID fields
  SFP 0 Options= 0x00 0x12
  SFP 0 BR max= 0
  SFP 0 BR min= 0
  SFP 0 Vendor SN= P5N1ACE
  SFP 0 Datecode = 040528
  SFP 0 CheckCodeExt = 0x5b
SFP 1 Diagnostic Information
SFP 1 Rx Power measurement type = Average
-------------------------------------
  SFP 1 Temp High Alarm threshold = 95.000C
  SFP 1 Voltage High Alarm threshold = 3.900V
  SFP 1 Bias High Alarm threshold = 17.000mA
  SFP 1 TX Power High Alarm threshold = 0.631mW
  SFP 1 RX Power High Alarm threshold = 1.259mW
  SFP 1 Temp Low Alarm threshold = -25.000C
  SFP 1 Voltage Low Alarm threshold = 2.700V
  SFP 1 Bias Low Alarm threshold = 1.000mA
  SFP 1 TX Power Low Alarm threshold = 0.067mW
  SFP 1 RX Power Low Alarm threshold = 0.010mW
-------------------------------------
  SFP 1 Temp High Warning threshold = 90.000C
  SFP 1 Voltage High Warning threshold = 3.700V
  SFP 1 Bias High Warning threshold = 14.000mA
  SFP 1 TX Power High Warning threshold = 0.631mW
  SFP 1 RX Power High Warning threshold = 0.794mW
  SFP 1 Temp Low Warning threshold = 2.900V
  SFP 1 Voltage Low Warning threshold = 2.000mA
  SFP 1 TX Power Low Warning threshold = 0.079mW
  SFP 1 RX Power Low Warning threshold = 0.016mW
-------------------------------------
  SFP 1 Temperature = 39.930C
  SFP 1 Voltage = 3.293V
  SFP 1 Tx Bias Current = 6.894mA
  SFP 1 Tx Power = 0.328mW
  SFP 1 Rx Power = 0.000mW
-------------------------------------
  SFP 1 Data Ready state Bar = False
  SFP 1 Rx LOS state = True
  SFP 1 Tx Fault state = False
  SFP 1 Rate Select state = False
  SFP 1 RS state = False
  SFP 1 Tx Disable state = False
-------------------------------------
  SFP 1 Temperature High Alarm Flag = False
  SFP 1 Voltage High Alarm Flag = False
  SFP 1 Tx Bias High Alarm Flag = False
  SFP 1 Tx Power High Alarm Flag = False
  SFP 1 Rx Power High Alarm Flag = False
  SFP 1 Temperature Low Alarm Flag = False
  SFP 1 Voltage Low Alarm Flag = False
  SFP 1 Tx Bias Low Alarm Flag = False
  SFP 1 Tx Power Low Alarm Flag = False
  SFP 1 Rx Power Low Alarm Flag = True
```

!-------output truncated -------------------------!
<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Power measurement type</td>
<td>Output depends on the vendor, typically either “Average” or “OMA” (Receiver optical modulation amplitude).</td>
</tr>
<tr>
<td>Temp High Alarm threshold</td>
<td>Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.</td>
</tr>
<tr>
<td>Voltage High Alarm threshold</td>
<td>Displays the interface index number used by SNMP to identify the interface.</td>
</tr>
<tr>
<td>Bias High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Power Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Current temperature of the SFPs. If this temperature crosses Temp High alarm/warning thresholds, then the temperature high alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Voltage</td>
<td>Current voltage of the SFPs. If this voltage crosses voltage high alarm/warning thresholds, then the voltage high alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Tx Bias Current</td>
<td>Present Tx bias current of the SFP. If this crosses bias high alarm/warning thresholds, then the tx bias high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, then the tx bias low alarm/warning flag is set to true.</td>
</tr>
</tbody>
</table>
Table 20-8. Diagnostic Data in show interfaces transceiver (continued)

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Power</td>
<td>Present Tx power of the SFP. If this crosses Tx power alarm/warning thresholds, then the Tx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, then the Tx power low alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Rx Power</td>
<td>Present Rx power of the SFP. This value is either average Rx power or OMA. This depends upon on the Rx Power measurement type displayed above. If this crosses Rx power alarm/warning thresholds, then the Rx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, then the Rx power low alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Data Ready state Bar</td>
<td>This field indicates that the transceiver has achieved power up and data is ready. This is set to true if data is ready to be sent, false if data is being transmitted.</td>
</tr>
<tr>
<td>Rx LOS state</td>
<td>This is the digital state of the Rx_LOS output pin. This is set to true if the operating status is down.</td>
</tr>
<tr>
<td>Tx Fault state</td>
<td>This is the digital state of the Tx Fault output pin.</td>
</tr>
<tr>
<td>Rate Select state</td>
<td>This is the digital state of the SFP rate_select input pin.</td>
</tr>
<tr>
<td>RS state</td>
<td>This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.</td>
</tr>
<tr>
<td>Tx Disable state</td>
<td>If the admin status of the port is down then this flag will be set to true.</td>
</tr>
<tr>
<td>Temperature High Alarm Flag</td>
<td>This can be either true/False and it depends on the Current Temperature value displayed above.</td>
</tr>
<tr>
<td>Voltage High Alarm Flag</td>
<td>This can be either true or false, depending on the Current voltage value displayed above.</td>
</tr>
<tr>
<td>Tx Bias High Alarm Flag</td>
<td>This can be either true or false, depending on the present Tx bias current value displayed above.</td>
</tr>
<tr>
<td>Tx Power High Alarm Flag</td>
<td>This can be either true or false, depending on the Current Tx power value displayed above.</td>
</tr>
<tr>
<td>Rx Power High Alarm Flag</td>
<td>This can be either true or false, depending on the Current Rx power value displayed above.</td>
</tr>
<tr>
<td>Temperature Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current Temperature value displayed above.</td>
</tr>
<tr>
<td>Voltage Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current voltage value displayed above.</td>
</tr>
<tr>
<td>Tx Bias Low Alarm Flag</td>
<td>This can be either true or false, depending on the Tx bias current value displayed above.</td>
</tr>
<tr>
<td>Tx Power Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current Tx power value displayed above.</td>
</tr>
<tr>
<td>Rx Power Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current Rx power value displayed above.</td>
</tr>
<tr>
<td>Temperature High Warning Flag</td>
<td>This can be either true or false, depending on the Current Temperature value displayed above.</td>
</tr>
<tr>
<td>Voltage High Warning Flag</td>
<td>This can be either true or false, depending on the Current voltage value displayed above.</td>
</tr>
<tr>
<td>Tx Bias High Warning Flag</td>
<td>This can be either true or false, depending on the Tx bias current value displayed above.</td>
</tr>
</tbody>
</table>
### show range

Display all interfaces configured using the **interface range** command.

**Syntax**

```
show range
```

**Command Mode**

INTERFACE RANGE (config-if-range)

**Command History**

- **Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

**Figure 20-38. show range Command Example**

```
FTOS(conf-if-range-te-0/16)#show range
interface tengigabitethernet 0/16
FTOS(conf-if-range-te-0/16)#
```

**Related Commands**

- **interface** Configures a physical interface on the switch.
- **show ip interface** Displays Layer 3 information about the interfaces.
- **show interfaces** Displays information on a specific physical interface or virtual interface.
- **show inventory** Displays the switch type, FTOS version including hardware identification numbers and configured protocols.
shutdown

Disable an interface.

Syntax

shutdown

To activate an interface, enter no shutdown.

Defaults

The interface is disabled.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The shutdown command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the show ip interface brief command. Disabled interfaces are listed as down.

Disabling a VLAN or a port channel causes different behavior. When a VLAN is disabled, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the shutdown command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, you must enter no shutdown on the port channel interface and at least one interface within that port channel.

The shutdown and description commands are the only commands that you can configure on an interface that is a member of a port channel.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel</td>
<td>Creates a port channel interface.</td>
</tr>
<tr>
<td>interface vlan</td>
<td>Creates a VLAN.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays the interface routing status. Add the keyword brief to display a table of interfaces and their status.</td>
</tr>
</tbody>
</table>

speed (for 1000/10000/auto interfaces)

Set the speed for 1000/10000 Base-T Ethernet interfaces. Both sides of a link must be set to the same speed (1000/10000) or to auto or the link may not come up.

Syntax

speed {1000 | 10000 | auto}

To return to the default setting, use the no speed {1000 | 10000 | auto} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>Enter the keyword 1000 to set the interface’s speed to 1000 Mb/s.</td>
</tr>
<tr>
<td>10000</td>
<td>Enter the keyword 10000 to set the interface’s speed to 10000 Mb/s. (Auto-negotiation is enabled. See negotiation auto for more information)</td>
</tr>
<tr>
<td>auto</td>
<td>Enter the keyword auto to set the interface to auto-negotiate its speed. (Auto-negotiation is enabled. See negotiation auto for more information)</td>
</tr>
</tbody>
</table>

Defaults

auto

Command Modes

INTERFACE
This command is found on the 1000/10000 Base-T Ethernet interfaces.

When you enable auto, the system performs and automatic discovery to determine the optics installed and configure the appropriate speed.

When you configure a speed for the 1000/10000 interface, you should confirm negotiation auto command setting. Both sides of the link should have auto-negotiation either enabled or disabled. For speed settings of 1000 or auto, the software sets the link to auto-negotiation and you cannot change that setting.

In FTOS, the command speed 1000 is an exact equivalent of speed auto 1000 in IOS.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>duplex (1000/10000 Interfaces)</td>
<td>Configures duplex mode on physical interfaces with the speed set to 1000/1000.</td>
</tr>
<tr>
<td>negotiation auto</td>
<td>Enables or disables auto-negotiation on an interface.</td>
</tr>
</tbody>
</table>

stack-unit portmode

Split a single 40G port into 4x10G ports on the MXL Switch.

Syntax

```
stack-unit stack-unit port number portmode quad
```

Parameters

- `stack-unit`: Enter the stack member unit identifier of the stack member to reset.
  - **MXL Switch range**: 0 to 5
    - **Note**: The MXL Switch commands accept Unit ID numbers 0-5, though MXL Switch supports stacking up to 3 units only with FTOS version 8.3.7.1.
  - `port`: Enter the port number of the 40G port to be split.
  - **MXL Switch range**: Enter one of the following port numbers: 48, 52, 56, or 60.

Defaults

Disabled

Command Modes

- **CONFIGURATION**

Command History

- **Version 8.3.16.1**: Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- Splitting a 40G port into 4x10G port is supported only on a standalone unit.
  - Split ports cannot be used as stack-link to stack an MXL Switch.
  - Split ports MXL Switch unit cannot be a part of any stacked system.
  - The unit number with the split ports must be the default (stack-unit 0)
  - This can be verified using CLI “show system brief”. If the unit ID is different than 0, then it must be renumbered to 0 before ports are split. By using the stack unit id renumber 0 command in EXEC mode.

The quad port must be in a default configuration before it can be split into 4x10G ports. The 40G port is lost in the config when the port is split, so be sure the port is also removed from other L2/L3 feature configurations. The system must be reloaded after issuing the CLI for the change to take effect.
Port Channel Commands

A link aggregation group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In FTOS, a LAG is referred to as a Port Channel.

Table 20-9. Port Channel Limits

<table>
<thead>
<tr>
<th>Platform</th>
<th>Maximum Port Channel IDs</th>
<th>Maximum Members per Port Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>MXL Switch</td>
<td>128</td>
<td>16</td>
</tr>
</tbody>
</table>

Because each port can be assigned to only one Port Channel, and each Port Channel must have at least one port, some of those nominally available Port Channels might have no function because they could have no members if there are not enough ports installed. In the MXL 10/40GbE Switch IO Module, those ports could be provided by stack members.

The commands in this section are specific to Port Channel interfaces:

- channel-member
- group
- interface port-channel
- minimum-links
- port-channel failover-group
- show config
- show interfaces port-channel

Note: The FTOS implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information on FTOS Link Aggregation Control Protocol (LACP) for dynamic LAGs, refer to Chapter 27, Link Aggregation Control Protocol (LACP).

For more information on configuring and using Port Channels, refer to the FTOS Configuration Guide.

channel-member

Add an interface to the Port Channel, while in the INTERFACE PORTCHANNEL mode.

Syntax

```
channel-member interface
```

To delete an interface from a Port Channel, use the no channel-member interface command.

Parameters

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a Ten Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

Defaults

Not configured.

Command Modes

INTERFACE PORTCHANNEL

Command History

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Use the `interface port-channel` command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration.

Link MTU and IP MTU considerations for Port Channels are:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members.

For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel’s MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the `no channel-member` command syntax, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

You can have sixteen interfaces per Port Channel on the MXL Switch. The interfaces can be located on different stack units but must be the same physical type and speed (for example, all 10-Gigabit Ethernet interfaces). However, you can combine 100/1000 interfaces and GE interfaces in the same Port Channel.

If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; you must disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. Refer to the `FTOS Configuration Guide` for more information on Port Channels.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Assigns a descriptive text string to the interface.</td>
</tr>
<tr>
<td>interface port-channel</td>
<td>Creates a Port Channel interface.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables/Enables the port channel.</td>
</tr>
</tbody>
</table>

### group

Group two LAGs in a supergroup (“fate-sharing group” or “failover group”).

#### Syntax

`group group_number port-channel number port-channel number`

To remove an existing LAG supergroup, use the `no group group_number` command.

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_number</td>
<td>Enter an integer from 1 to 32 that will uniquely identify this LAG fate-sharing group.</td>
</tr>
<tr>
<td>port-channel number</td>
<td>Enter the keyword <code>port-channel</code> followed by an existing LAG <code>number</code>. Enter this keyword/variable combination twice, identifying the two LAGs to be paired.</td>
</tr>
</tbody>
</table>

#### Defaults

`none`
interface port-channel

Create a Port Channel interface, which is a link aggregation group containing up to 16 physical interfaces on an MXL Switch.

Syntax

```
interface port-channel channel-number
```

To delete a Port Channel, use the `no interface port-channel channel-number` command.

Parameters

- **channel-number**: For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - Range: 1-128

Defaults

Not configured.

Command Modes

- **CONFIGURATION**

Command History

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example

**Figure 20-40.  interface port-channel Command Example**

```
FTOS(conf)#int port-channel 2
FTOS(conf-if-po-2)#
```

Usage Information

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by configuring `port-channel with switchport command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, FTOS determines if the Port Channel uses 100 Mb/s or 1000 Mb/s as the common speed. Refer to `channel-member` for more information.

If the stack unit is in a Jumbo mode chassis, then the `mtu` and `ip mtu` commands can also be configured. The Link MTU and IP MTU values configured on the channel members must be greater than the Link MTU and IP MTU values configured on the Port Channel interface.

**Note:** In a Jumbo-enabled system, all members of a Port Channel must be configured with the same link MTU values and the same IP MTU values.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-member</td>
<td>Adds a physical interface to the LAG.</td>
</tr>
<tr>
<td>interface</td>
<td>Configures a physical interface.</td>
</tr>
<tr>
<td>interface loopback</td>
<td>Configures a Loopback interface.</td>
</tr>
<tr>
<td>interface null</td>
<td>Configures a null interface.</td>
</tr>
<tr>
<td>interface vlan</td>
<td>Configures a VLAN.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Disables/Enables the port channel.</td>
</tr>
</tbody>
</table>

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in “oper up” status for the LAG to be also in “oper up” status.

Syntax

minimum-links number

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the number of links in a LAG that must be in “oper up” status. Range: 1 to 16 Default: 1</td>
</tr>
</tbody>
</table>

Defaults

1

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you use this command to configure the minimum number of links in a LAG that must be in “oper up” status, the LAG must have at least that number of “oper up” links before it can be declared as up.

For example, if the required minimum is four, and only three are up, then the LAG is considered down.

port-channel failover-group

Access the PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

Syntax

port-channel failover-group

To remove all LAG failover groups, use the no port-channel failover-group command.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This feature groups two LAGs to work in tandem as a supergroup, so that, if one LAG goes down, the other LAG is taken down automatically, providing an alternate path to reroute traffic, avoiding oversubscription on the other LAG. You can use both static and dynamic (LACP) LAGs to configure failover groups. For details, refer to the Port Channel chapter in the FTOS Configuration Guide.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group</code></td>
<td>Groups two LAGs in a supergroup (“fate-sharing group”).</td>
</tr>
<tr>
<td><code>show interfaces port-channel</code></td>
<td>Displays information on configured Port Channel groups.</td>
</tr>
</tbody>
</table>

**show config**

Display the current configuration of the selected LAG.

**Syntax**

```
show config
```

**Command Modes**

INTERFACE PORTCHANNEL

**Example**

Figure 20-41. show config Command Sample Output for a Selected LAG

```
FTOS(conf-if-po-1)#show config
!
interface Port-channel 1
no ip address
shutdown
FTOS(conf-if-po-1)#
```

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**show interfaces port-channel**

Display information on configured Port Channel groups.

**Syntax**

```
show interfaces port-channel [channel-number] [brief]
```

**Parameters**

- `channel-number`: For a Port Channel interface, enter the keyword `port-channel` followed by a number:  
  - Range: 1-128
- `brief`: (OPTIONAL) Enter the keyword `brief` to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
### Table 20-10. show interfaces port-channel Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-Channel 1...</td>
<td>Displays the LAG’s status. In the example, the status of the LAG’s LAG fate-sharing group (“Failover-group”) is listed.</td>
</tr>
<tr>
<td>Hardware is...</td>
<td>Displays the interface’s hardware information and its assigned MAC address.</td>
</tr>
<tr>
<td>Port-channel is part...</td>
<td>Indicates whether the LAG is part of a LAG fate-sharing group (“Failover-group”).</td>
</tr>
<tr>
<td>Internet address...</td>
<td>States whether an IP address is assigned to the interface. If one is, that address is displayed.</td>
</tr>
<tr>
<td>MTU 1554...</td>
<td>Displays link and IP MTU.</td>
</tr>
<tr>
<td>LineSpeed</td>
<td>Displays the interface’s line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.</td>
</tr>
<tr>
<td>Members in this...</td>
<td>Displays the interfaces belonging to this port channel.</td>
</tr>
<tr>
<td>ARP type...</td>
<td>Displays the ARP type and the ARP timeout value for the interface.</td>
</tr>
<tr>
<td>Last clearing...</td>
<td>Displays the time when the <code>show interfaces</code> counters were cleared.</td>
</tr>
<tr>
<td>Queueing strategy.</td>
<td>States the packet queuing strategy. FIFO means first in first out.</td>
</tr>
<tr>
<td>packets input...</td>
<td>Displays the number of packets and bytes into the interface.</td>
</tr>
<tr>
<td>Input 0 IP packets...</td>
<td>Displays the number of packets with IP headers, VLAN tagged headers and MPLS headers. The number of packets may not add correctly because a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.</td>
</tr>
<tr>
<td>0 64-byte...</td>
<td>Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.</td>
</tr>
<tr>
<td>Received 0...</td>
<td>Displays the type and number of errors or other specific packets received. This information is displayed over three lines.</td>
</tr>
</tbody>
</table>
Table 20-10.  show interfaces port-channel Command Example Fields  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output 0...</td>
<td>Displays the type and number of packets sent out the interface. This information is displayed over three lines.</td>
</tr>
<tr>
<td>Rate information...</td>
<td>Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.</td>
</tr>
<tr>
<td>Time since...</td>
<td>Displays the time since the last change in the configuration of this interface.</td>
</tr>
</tbody>
</table>

Figure 20-43.  show interfaces port-channel brief Command Example

```
FTOS#show int po 1 brief
Codes: L - LACP Port-channel

LAG  Mode  Status       Uptime      Ports
1    L3    down         00:00:00    Te 0/16    (Down)
FTOS#
```

Table 20-11.  show interfaces port-channel brief Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAG</td>
<td>Lists the port channel number.</td>
</tr>
<tr>
<td>Mode</td>
<td>Lists the mode:</td>
</tr>
<tr>
<td></td>
<td>• L3 - for Layer 3</td>
</tr>
<tr>
<td></td>
<td>• L2 - for Layer 2</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the port channel.</td>
</tr>
<tr>
<td></td>
<td>• down - if the port channel is disabled (shutdown)</td>
</tr>
<tr>
<td></td>
<td>• up - if the port channel is enabled (no shutdown)</td>
</tr>
<tr>
<td>Uptime</td>
<td>Displays the age of the port channel in hours:minutes:seconds.</td>
</tr>
<tr>
<td>Ports</td>
<td>Lists the interfaces assigned to this port channel.</td>
</tr>
<tr>
<td>(untitled)</td>
<td>Displays the status of the physical interfaces (up or down).</td>
</tr>
<tr>
<td></td>
<td>In Layer 2 port channels, an * (asterisk) indicates which interface is the</td>
</tr>
<tr>
<td></td>
<td>primary port of the port channel. The primary port sends out interface</td>
</tr>
<tr>
<td></td>
<td>PDU.</td>
</tr>
<tr>
<td></td>
<td>In Layer 3 port channels, the primary port is not indicated.</td>
</tr>
</tbody>
</table>

Related Commands

`show lacp` Displays the LACP matrix.
Time Domain Reflectometer (TDR)

Time domain reflectometer (TDR) is useful for troubleshooting an interface that is not establishing a link; either it is flapping or not coming up at all. TDR detects open or short conditions of copper cables on 100/1000 Base-T modules.

- tdr-cable-test
- show tdr

Important Points to Remember

- The interface and port must be enabled (configured—see the `interface` command) before running TDR. An error message is generated if you have not enabled the interface.
- The interface on the far-end device must be shut down before running TDR.
- Because TDR is an intrusive test on an interface that is not establishing a link, do not run TDR on an interface that is passing traffic.
- When testing between two devices, do not run the test on both ends of the cable.

tdr-cable-test

Test the condition of copper cables on 100/1000 Base-T modules.

```
Syntax tdr-cable-test interface
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information for the 100/1000 Ethernet interface.</td>
</tr>
</tbody>
</table>

| Defaults | none |
| Command Modes | EXEC |

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The interface must be enabled to run the test or an error message is generated:

```
FTOS#tdr-cable-test tengigabitethernet 5/2
%Error: Interface is disabled TenGIG 5/2
```

Related Commands

- `show tdr` Displays the results of the TDR test.

show tdr

Display the TDR test results.

```
Syntax show tdr interface
```

Interfaces | 425
**Parameters**

- **interface**: Enter the keyword `TenGigabitEthernet` followed by the slot/port information for the 100/1000 Ethernet interface.

**Defaults**

- none

**Command Modes**

- EXEC

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

**Figure 20-44. show tdr tengigabitethernet Command Example**

```plaintext
FTOS#show tdr tengigabitethernet 10/47
Time since last test: 00:00:02
  Pair A, Length: OK Status: Terminated
  Pair B, Length: 92 (+/- 1) meters, Status: Short
  Pair C, Length: 93 (+/- 1) meters, Status: Open
  Pair D, Length: 0 (+/- 1) meters, Status: Impedance Mismatch
```

**Table 20-12. TDR Test Status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OK Status: Terminated</strong></td>
<td>TDR test is complete, no fault is detected on the cable, and the test is terminated</td>
</tr>
<tr>
<td>Length: 92 (+/- 1) meters, Status: Shorted</td>
<td>A short is detected on the cable. The location, in this example is 92 meters, of the short is accurate to plus or minus one meter.</td>
</tr>
<tr>
<td>Length: 93 (+/- 1) meters, Status: Open</td>
<td>An opening is detected on the cable. The location, in this example is 93 meters, of the open is accurate to plus or minus one meter.</td>
</tr>
<tr>
<td>Status: Impedance Mismatch</td>
<td>There is an impedance mismatch in the cables.</td>
</tr>
</tbody>
</table>

**Usage Information**

If the TDR test has not been run, an error messages is generated:

```
%Error: Please run the TDR test first
```

**Related Commands**

- `tdr-cable-test` Runs the TDR test.
UDP Broadcast

The user datagram protocol (UDP) broadcast feature is a software-based method to forward low throughput (not to exceed 200 pps) IP/UDP broadcast traffic arriving on a physical or VLAN interface.

Important Points to Remember

- Routing information protocol (RIP) is not supported with the UDP broadcast feature.
- If this feature is configured on an interface using `ip udp-helper udp-port`, the `ip directed-broadcast` command becomes ineffective on that interface.
- The existing command `show interface` has been modified to display the configured broadcast address.

The commands for UDP Broadcast are:

- `debug ip udp-helper`
- `ip udp-broadcast-address`
- `ip udp-helper udp-port`
- `show ip udp-helper`

**debug ip udp-helper**

Enable UDP debug and display the debug information on a console.

**Syntax**

```
debug ip udp-helper
```

To disable debug information, use the `no debug ip udp-helper` command.

**Defaults**

Debug disabled

**Command Modes**

EXEC

EXEC Privilege

**Example**

```
Figure 20-45. Debug Output Command Example

FTOS#debug ip udp-helper
UDP helper debugging is on

01:20:22: Pkt rcvd on TenGig 5/0 with IP DA (0xffffffff) will be sent on TenGig 5/1
TenGig 5/2 Vlan 3

01:44:54: Pkt rcvd on TenGig 7/0 is handed over for DHCP processing.
```

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `ip udp-broadcast-address` Configures a UDP IP address for broadcast
- `ip udp-helper udp-port` Enables the UDP broadcast feature on an interface.
- `show ip udp-helper` Displays the configured UDP helper(s) on all interfaces.
ip udp-broadcast-address

Configure an IP UDP address for broadcast.

**Syntax**

```plaintext
ip udp-broadcast-address address
```

To delete the configuration, use the `no ip udp-broadcast-address address` command.

**Parameters**

- `address` Enter an IP broadcast address in dotted decimal format (A.B.C.D).

**Defaults**

Not Configured

**Command Modes**

INTERFACE (config-if)

**Usage Information**

When a UDP broadcast packet is flooded out of an interface, and the outgoing interface is configured using this command, the outgoing packet’s IP destination address is replaced with the configured broadcast address.

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `debug ip udp-helper` Enables debug and display the debug information on a console.
- `show ip udp-helper` Displays the configured UDP helper(s) on all interfaces.

---

ip udp-helper udp-port

Enable the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

**Syntax**

```plaintext
ip udp-helper udp-port [udp-port-list]
```

To disable the UDP broadcast on a port, use the `no ip udp-helper udp-port [udp-port-list]` command.

**Parameters**

- `udp-port-list` (OPTIONAL) Enter up to 16 comma separated UDP port numbers.

  **Note:** If this option is not used, all UDP Ports are considered by default.

**Defaults**

none

**Command Modes**

INTERFACE (config-if)

**Usage Information**

If you configure the `ip helper-address` command and `ip udp-helper udp-port` command, the behavior is that the UDP broadcast traffic with port numbers 67/68 is unicast relayed to the DHCP server as per the `ip helper-address` configuration. This occurs regardless of whether the `ip udp-helper udp-port` command contains port numbers 67/68 or not.

If you only configure the `ip udp-helper udp-port` command, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the `udp-port-list`.

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
show ip udp-helper

Display the configured UDP helper(s) on all interfaces.

Syntax

show ip udp-helper

Defaults

none

Command Modes

EXEC

Example

Figure 20-46.  show ip udp-helper Command Example

FTOS#show ip udp-helper
-------------------------------
Port   UDP port list
-------------------------------
TenGig 10/0   656, 658
TenGig 10/1   All

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip helper-address</td>
<td>Configures the destination broadcast or host address for DHCP server.</td>
</tr>
<tr>
<td>debug ip udp-helper</td>
<td>Enables debug and display the debug information on a console.</td>
</tr>
<tr>
<td>show ip udp-helper</td>
<td>Displays the configured UDP helper(s) on all interfaces.</td>
</tr>
<tr>
<td>ip udp-broadcast-address</td>
<td>Configures a UDP IP address for broadcast.</td>
</tr>
<tr>
<td>ip udp-helper udp-port</td>
<td>Enables the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.</td>
</tr>
</tbody>
</table>
IPv4 Routing

Commands

This chapter describes the IPv4-related commands. They are:

- arp
- arp learn-enable
- arp retries
- arp timeout
- clear arp-cache
- clear host
- clear ip fib stack-unit
- clear ip route
- clear tcp statistics
- debug arp
- debug ip dhcp
- debug ip icmp
- debug ip packet
- ip address
- ip directed-broadcast
- ip domain-list
- ip domain-lookup
- ip domain-name
- ip helper-address
- ip helper-address hop-count disable
- ip host
- ip max-frag-count
- ip name-server
- ip proxy-arp
- ip route
- ip source-route
- ip unreachable
- management route
- show arp
- show arp retries
- show hosts
- show ip cam stack-unit
- show ip fib stack-unit
- show ip interface
arp

Use the address resolution protocol (ARP) to associate an IP address with a MAC address in the switch.

**Syntax**
```
arp ip-address mac-address interface
```

To remove an ARP address, use the `no arp ip-address` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>Enter an IP address in dotted decimal format.</td>
</tr>
<tr>
<td><strong>mac-address</strong></td>
<td>Enter a MAC address in nnnn.nnnn.nnnn format.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>Enter the following keywords and slot/port or number information:</td>
</tr>
</tbody>
</table>

  - For the Management interface, enter the keyword `ManagementEthernet` followed by the slot/port information. The slot range is 0-1 and the port range is 0.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**
You cannot use Class D or Class E IP addresses or zero IP address (0.0.0.0) when creating a static ARP. Zero MAC addresses (00:00:00:00:00:00) are also invalid.

**Related Commands**

- `clear arp-cache` — Clears dynamic ARP entries from the ARP table.
- `show arp` — Displays the ARP table.

arp learn-enable

Enable ARP learning via Gratuitous ARP.

**Syntax**
```
arp learn-enable
```
Defaults
Disabled

Command Modes
CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

arp retries
Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

Syntax
arp retries number

Parameters

| number   | Enter the number of retries.  
|----------|------------------------------
| Range: 5 to 20.  
| Default: 5 |

Defaults
5

Command Modes
CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
Retries are 20 seconds apart.

Related Commands
show arp retries Displays the configured number of ARP retries.

arp timeout
Set the time interval for an ARP entry to remain in the ARP cache.

Syntax
arp timeout minutes

Parameters

| seconds   | Enter the number of minutes.  
|-----------|------------------------------
| Range: 0 to 35790  
| Default: 240 minutes |

Defaults
240 minutes (4 hours)

Command Modes
INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands
show interfaces Displays the ARP timeout value for all available interfaces.
### clear arp-cache

Clear the dynamic ARP entries from a specific interface or optionally delete (no-refresh) ARP entries from CAM.

**Syntax**
```
clear arp-cache [interface | ip ip-address] [no-refresh]
```

**Parameters**
- `interface` (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For the Management interface, enter the keyword `ManagementEthernet` followed by the slot/port information. The slot range is 0 and the port range is 0.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
- `ip ip-address` (OPTIONAL) Enter the keyword `ip` followed by the IP address of the ARP entry you wish to clear.
- `no-refresh` (OPTIONAL) Enter the keyword `no-refresh` to delete the ARP entry from CAM. Or use this option with `interface` or `ip ip-address` to specify which dynamic ARP entries you want to delete.

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### clear host

Remove one or all dynamically learnt host table entries.

**Syntax**
```
clear host name
```

**Parameters**
- `name` Enter the name of the host to delete.
  Enter `*` to delete all host table entries.

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### clear ip fib stack-unit

Clear all forwarding information base (fib) entries in the specified stack unit (use this command with caution, refer to Usage Information).

**Syntax**

```
clear ip fib stack-unit unit-number
```

**Parameters**

<table>
<thead>
<tr>
<th>unit-number</th>
<th>Enter the stack-unit number.</th>
</tr>
</thead>
</table>

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Use this command to clear Layer 3 CAM inconsistencies.

⚠️ **Caution:** Executing this command causes traffic disruption.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip fib stack-unit</td>
<td>Shows the FIB entries.</td>
</tr>
</tbody>
</table>

### clear ip route

Clear one or all routes in the routing table.

**Syntax**

```
clear ip route {* | ip-address mask}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Enter an asterisk (*) to clear all learned IP routes.</td>
</tr>
<tr>
<td>ip-address mask</td>
<td>Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route</td>
<td>Assigns an IP route to the switch.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Views the routing table.</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Views a summary of the routing table.</td>
</tr>
</tbody>
</table>

### clear tcp statistics

Clear TCP counters.

**Syntax**

```
clear tcp statistics
```

**Parameters**

None
debug arp

View information on ARP transactions.

Syntax
d debug arp [interface] [count value]

To stop debugging ARP transactions, use the no debug arp command.

Parameters

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For the Management interface, enter the keyword managementethernet followed by the slot/port information. The slot range is 0 and the port range is 0.
  - For a Port Channel interface, enter the keyword port-channel followed by a number: Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword tengigabitethernet followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.
  - For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

- **count value** (OPTIONAL) Enter the keyword count followed by the count value. Range: 1 to 65534

Defaults

- none

Command Modes

- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

- Use the count option to stop packets from flooding the user terminal when debugging is turned on.

debug ip dhcp

Enable debug information for DHCP relay transactions and display the information on the console.

Syntax
d debug ip dhcp

To disable debug, use the no debug ip dhcp command.

Defaults

- Debug disabled

Command Modes

- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### Example Figure 21-1. debug ip dhcp Command Example

```
FTOS#debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xbf05140f, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xbf05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
FTOS#
```
**debug ip packet**

View a log of IP packets sent and received.

**Syntax**

```
debug ip packet [access-group name] [count value] [interface]
```

To disable debugging, use the `no debug ip packet [access-group name] [count value] [interface]` command.

**Parameters**

- **access-group name**
  - Enter the keyword `access-group` followed by the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.

- **count value**
  - (OPTIONAL) Enter the keyword `count` followed by the count value.
  - Range: 1 to 65534
  - Default: Infinity

- **interface**
  - (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For the management interface, enter the keyword `managementethernet` followed by the slot/port information. The slot range is 0 and the port range is 0.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Mode**

EXEC Privilege

**Command History**

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

**Usage Information**

Use the `count` option to stop packets from flooding the user terminal when debugging is turned on.
Example

Figure 21-3. debug ip packet Command Example (Partial)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>s=</td>
<td>Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.</td>
</tr>
<tr>
<td>d=</td>
<td>Lists the destination address of the packet and the name of the interface (in parentheses) through which the packet is being sent out on the network.</td>
</tr>
<tr>
<td>len</td>
<td>Displays the packet’s length.</td>
</tr>
<tr>
<td>sending</td>
<td>The last part of each line lists the status of the packet.</td>
</tr>
<tr>
<td>rcvd</td>
<td></td>
</tr>
<tr>
<td>fragment</td>
<td></td>
</tr>
<tr>
<td>sending broad/multicast proto</td>
<td></td>
</tr>
<tr>
<td>unroutable</td>
<td></td>
</tr>
<tr>
<td>TCP src=</td>
<td>Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.</td>
</tr>
<tr>
<td>UDP src=</td>
<td>Displays the source and destination ports for the UDP packets.</td>
</tr>
<tr>
<td>ICMP type=</td>
<td>Displays the ICMP type and code.</td>
</tr>
<tr>
<td>IP Fragment</td>
<td>States that it is a fragment and displays the unique number identifying the fragment (Ident) and the offset (in 8-byte units) of this fragment (fragment offset) from the beginning of the original datagram.</td>
</tr>
</tbody>
</table>
Usage Information

Use the count option to stop packets from flooding the user terminal when debugging is turned on.

The access-group option supports only the equal to (eq) operator in TCP ACL rules. Port operators not equal to (neq), greater than (gt), less than (lt), or **range** are not supported in **access-group** option (see Figure 21-4). ARP packets (arp) and Ether-type (ether-type) are also not supported in **access-group** option. The entire rule is skipped to compose the filter.

The access-group option pertains to:

- **IP Protocol Number**
- Internet Control Message Protocol* (icmp)
  * but not the ICMP message type (0-255)
- Any Internet Protocol
- Transmission Control Protocol* (tcp)
  * but not on the rst, syn, or urg bit
- User Datagram Protocol

In the case of ambiguous access control list rules, the debug ip packet access-control command will be disabled. A message appears identifying the error (see Figure 21-4).

### Example

```
FTOS#debug ip packet access-group test
%Error: port operator GT not supported in access-list debug
%Error: port operator LT not supported in access-list debug
%Error: port operator RANGE not supported in access-list debug
%Error: port operator NEQ not supported in access-list debug
%IPMGR-3-DEBUG_IP_PACKET_ACL_AMBIGUOUS_EXP: Ambiguous rules not supported in access-list debug, access-list debugging is turned off
FTOS#
```

### ip address

Assign a primary and secondary IP address to the interface.

**Syntax**

```
ip address ip-address mask [secondary]
```

To delete an IP address from an interface, use the **no ip address** command.

**Parameters**

- **ip-address**
  
  Enter an IP address in dotted decimal format.

- **mask**
  
  Enter the mask of the IP address in slash prefix format (for example, /24).

- **secondary**
  
  (OPTIONAL) Enter the keyword **secondary** to designate the IP address as the secondary address.

**Defaults**

Not configured.

**Command Modes**

**INTERFACE**

**Command History**

- **Version 8.3.16.1**
  Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must be in INTERFACE mode before you add an IP address to an interface. Assign an IP address to an interface prior to entering ROUTER OSPF mode.
**ip directed-broadcast**

Enables the interface to receive directed broadcast packets.

**Syntax**

```
ip directed-broadcast
```

To disable the interface from receiving directed broadcast packets, use the `no ip directed-broadcast` command.

**Defaults**

Disabled (that is, the interface does not receive directed broadcast packets)

**Command Modes**

`INTERFACE`

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**ip domain-list**

Configure names to complete unqualified host names.

**Syntax**

```
ip domain-list name
```

To remove the name, use the `no ip domain-list name` command.

**Parameters**

- `name` Enter a domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

**Defaults**

Disabled.

**Command Modes**

`CONFIGURATION`

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**Usage Information**

Configure the `ip domain-list` command up to 6 times to configure a list of possible domain names.

If both the `ip domain-name` and `ip domain-list` commands are configured, the software will try to resolve the name using the `ip domain-name` command. If the name is not resolved, the software goes through the list of names configured with the `ip domain-list` command to find a match.

Use the following steps to enable dynamic resolution of hosts:

- specify a domain name server with the `ip name-server` command.
- enable DNS with the `ip domain-lookup` command.

To view current bindings, use the `show hosts` command. To view DNS related configuration, use the `show running-config resolve` command.

**Related Commands**

- `ip domain-name` Specifies a DNS server.
ip domain-lookup

Enable dynamic host-name to address resolution (that is, DNS).

Syntax

ip domain-lookup

To disable DNS lookup, use the no ip domain-lookup command.

Defaults

Disabled.

Command Mode

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

To fully enable DNS, also specify one or more domain name servers with the ip name-server command.

FTOS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

To view current bindings, use the show hosts command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip name-server</td>
<td>Specifies a DNS server.</td>
</tr>
<tr>
<td>show hosts</td>
<td>Views current bindings.</td>
</tr>
</tbody>
</table>
### ip helper-address

Specify the address of a DHCP server so that DHCP broadcast messages can be forwarded when the DHCP server is not on the same subnet as the client.

**Syntax**

```
ip helper-address ip-address
```

To remove a DHCP server address, use the `no ip helper-address` command.

**Parameters**

- **ip-address**: Enter an IP address in dotted decimal format (A.B.C.D).

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You can add multiple DHCP servers by entering the `ip helper-address` command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client.

FTOS uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and FTOS forwards to the client with source port=67, destination port=68.

### ip helper-address hop-count disable

Disable the hop-count increment for the DHCP relay agent.

**Syntax**

```
ip helper-address hop-count disable
```

To re-enable the hop-count increment, use the `no ip helper-address hop-count disable` command.

**Defaults**

Enabled; the hops field in the DHCP message header is incremented by default.

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through FTOS. If the incoming boot request already has a non-zero hops field, the message will be relayed with the same value for hops. However, the message is discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.
### ip host

Assign a name and IP address to be used by the host-to-IP address mapping table.

**Syntax**

```
ip host name ip-address
```

To remove an IP host, use the `no ip host name [ip-address]` command.

**Parameters**

- `name` Enter a text string to associate with one IP address.
- `ip-address` Enter an IP address, in dotted decimal format, to be mapped to the name.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

**Syntax**

```
ip max-frag-count count
```

To place no limit on the number of fragments allowed, use the `no ip max-frag-count` command.

**Parameters**

- `count` Enter a number for the number of fragments allowed for re-assembly.
  
  Range: 2 to 256

**Defaults**

No limit is set on number of fragments allowed.

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

To avoid denial of service (DOS) attacks, keep the number of fragments allowed for re-assembly low.

### ip name-server

Enter up to 6 IPv4 addresses of name servers. The order you enter the addresses determines the order of their use.

**Syntax**

```
ip name-server ipv4-address [ipv4-address2...ipv4-address6]
```

To remove a name server, use the `no ip name-server ip-address` command.
Parameters

| ipv4-address | Enter the IPv4 address, in dotted decimal format, of the name server to be used. |
| ipv4-address2...ipv4-address6 | (OPTIONAL) Enter up to five more IPv4 addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space. |

Defaults

No name servers are configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

FTOS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

**ip proxy-arp**

Enable Proxy ARP on an interface.

Syntax

ip proxy-arp

to disable Proxy ARP, enter no ip proxy-arp.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

show ip interface Displays the interface routing status and configuration.

**ip route**

Assign a static route to the switch.

Syntax

ip route destination mask ip-address | interface [ip-address] [distance] [permanent] [tag tag-value]

To delete a specific static route, use the no ip route destination mask [address | interface [ip-address]] command.

To delete all routes matching a certain route, use the no ip route destination mask command.

Parameters

| destination | Enter the IP address in dotted decimal format of the destination device. |
| mask | Enter the mask in slash prefix formation (/x) of the destination device’s IP address. |
| ip-address | Enter the IP address in dotted decimal format of the forwarding router. |
Using the following example of a static route:
\texttt{ip route 33.33.33.0 /24 tengigabitethernet 0/0 172.31.5.43}

- The software installs a next hop that is not on the directly connected subnet but which recursively resolves to a next hop on the interface’s configured subnet. In the example, if gig 0/0 has ip address on subnet 2.2.2.0 and if 172.31.5.43 recursively resolves to 2.2.2.0, FTOS installs the static route.
- When the interface goes down, FTOS withdraws the route.
- When the interface comes up, FTOS re-installs the route.
- When recursive resolution is “broken,” FTOS withdraws the route.
- When recursive resolution is satisfied, FTOS re-installs the route.

**Related Commands**

- \texttt{show ip route} Views the switch routing table.

---

**ip source-route**

Enable FTOS to forward IP packets with source route information in the header.

**Syntax**

\texttt{ip source-route}

To drop packets with source route information, use the \texttt{no ip route-source} command.
ip unreachables

Enable the generation of Internet Control Message Protocol (ICMP) unreachable messages.

Syntax

ip unreachables

To disable the generation of ICMP messages, use the no ip unreachables command.

Defaults

Disabled

Command Modes

INTERFACE

Related Commands

management route

Configure a static route that points to the Management interface or a forwarding router.

Syntax

management route {ipv4-address}/mask [forwarding-router-address | managementethernet}

Parameters

ipv4-address/mask Enter an IPv4 address (A.B.C.D) followed by the prefix-length for the IP address of the management interface.

forwarding-router-address Enter an IPv4 address of a forwarding router.

managementethernet Enter the keyword managementethernet for the Management interface.

Defaults

Not configured.

Command Modes

CONFIGURATION

Usage Information

When a static route (or a protocol route) overlaps with Management static route, the static route (or a protocol route) is preferred over the Management Static route. Also, Management static routes and the Management Connected prefix are not reflected in the hardware routing tables. Separate routing tables are maintained for IPv4 management routes. This command manages both tables.

Related Commands

interface ManagementEthernet  Configures the Management port on the system.
**show arp**

Display the ARP table.

**Syntax**

```
show arp [interface interface | ip ip-address [mask] | macaddress mac-address [mac-address mask]] [static | dynamic] [summary]
```

**Parameters**

- `interface interface` (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For the Management interface, enter the keyword `managementethernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

- `ip ip-address mask` (OPTIONAL) Enter the keyword `ip` followed by an IP address in the dotted decimal format. Enter the optional IP address mask in the slash prefix format (/x).


- `static` (OPTIONAL) Enter the keyword `static` to view entries entered manually.

- `dynamic` (OPTIONAL) Enter the keyword `dynamic` to view dynamic entries.

- `summary` (OPTIONAL) Enter the keyword `summary` to view a summary of ARP entries.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Figure 21-5 shows two VLANs that are associated with a private VLAN (PVLAN) (refer to Chapter 37, Private VLAN (PVLAN)).

**Example**

```
Figure 21-5. show arp Command Example (Partial)
```

```
Protocol Address Age(min) Hardware Address Interface VLAN
-----------------------------------------------------------------------------------------
  Internet    10.11.8.6 167 00:01:e9:45:00:03 Ma 0/0  -
    CP
  Internet    10.11.68.14 124 00:01:e9:45:00:03 Ma 0/0  -
     CP
  Internet    10.11.209.254 0 00:01:e9:45:00:03 Ma 0/0  -
     CP
```
Figure 21-6. show arp Command Example with Private VLAN data

FTOS#show arp

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age(min)</th>
<th>Hardware Address</th>
<th>Interface</th>
<th>VLAN</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>5.5.5.1</td>
<td>-</td>
<td>00:01:e8:43:96:5e</td>
<td>Vl 10 pv 200</td>
<td>CP</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>5.5.5.10</td>
<td>-</td>
<td>00:01:e8:44:99:55</td>
<td>Vl 10</td>
<td>CP</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>10.1.2.4</td>
<td>1</td>
<td>00:01:e8:d5:9e:e2</td>
<td>Ma 0/0</td>
<td>CP</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>10.10.10.4</td>
<td>1</td>
<td>00:01:e8:d5:9e:e2</td>
<td>Ma 0/0</td>
<td>CP</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>10.16.127.53</td>
<td>20</td>
<td>00:01:e8:d5:9e:e2</td>
<td>Ma 0/0</td>
<td>CP</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>10.16.134.254</td>
<td>20</td>
<td>00:01:e8:d5:9e:e2</td>
<td>Ma 0/0</td>
<td>CP</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>133.33.33.4</td>
<td>1</td>
<td>00:01:e8:d5:9e:e2</td>
<td>Ma 0/0</td>
<td>CP</td>
<td></td>
</tr>
</tbody>
</table>

Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN.
Line 2 shows primary VLAN 10.

Table 21-2. show arp Command Example Fields

<table>
<thead>
<tr>
<th>Row Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Displays the protocol type.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the IP address of the ARP entry.</td>
</tr>
<tr>
<td>Age(min)</td>
<td>Displays the age in minutes of the ARP entry.</td>
</tr>
<tr>
<td>Hardware Address</td>
<td>Displays the MAC address associated with the ARP entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the first two letters of the interfaces type and the slot/port</td>
</tr>
<tr>
<td></td>
<td>associated with the ARP entry.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Displays the VLAN ID, if any, associated with the ARP entry.</td>
</tr>
<tr>
<td>CPU</td>
<td>Lists which CPU the entries are stored on.</td>
</tr>
</tbody>
</table>

Figure 21-7. show arp summary Command Example

FTOS#show arp summary

<table>
<thead>
<tr>
<th>Total Entries</th>
<th>Static Entries</th>
<th>Dynamic Entries</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>CP</td>
</tr>
</tbody>
</table>

FTOS#

Table 21-3. show arp summary Command Example Fields

<table>
<thead>
<tr>
<th>Row Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Entries</td>
<td>Lists the total number of ARP entries in the ARP table.</td>
</tr>
<tr>
<td>Static Entries</td>
<td>Lists the total number of configured or static ARP entries.</td>
</tr>
<tr>
<td>Dynamic Entries</td>
<td>Lists the total number of learned or dynamic ARP entries.</td>
</tr>
<tr>
<td>CPU</td>
<td>Lists which CPU the entries are stored on.</td>
</tr>
</tbody>
</table>

Related Commands

- `ip local-proxy-arp`: Enables/disables Layer 3 communication in secondary VLANs.
- `switchport mode private-vlan`: Sets the PVLAN mode of the selected port.
show arp retries

Display the configured number of ARP retries.

Syntax

show arp retries

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.1.0 Introduced

Related Commands

arp retries Sets the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

show hosts

View the host table and DNS configuration.

Syntax

show hosts

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 21-8. show hosts Command Example

FTOS#show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set
Host Flags TTL Type Address
-------- ----- ---- ---- -------
ks (perm, OK) - IP 2.2.2.2
4200-1 (perm, OK) - IP 192.68.69.2
1230-3 (perm, OK) - IP 192.68.99.2
Zzr (perm, OK) - IP 192.71.18.2
Z10-3 (perm, OK) - IP 192.71.23.1
FTOS#

Table 21-4. show hosts Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default domain...</td>
<td>Displays the domain name (if configured).</td>
</tr>
<tr>
<td>Name/address lookup</td>
<td>States if DNS is enabled on the system. If DNS is enabled, the Name/Address lookup is domain service. If DNS is not enabled, the Name/Address lookup is static mapping.</td>
</tr>
<tr>
<td>Name servers are...</td>
<td>Lists the name servers, if configured.</td>
</tr>
<tr>
<td>Host</td>
<td>Displays the host name assigned to the IP address.</td>
</tr>
</tbody>
</table>
show ip cam stack-unit

Display content-addressable memory (CAM) entries.

Syntax

```
show ip cam stack-unit 0-5 port-set pipe-number [ip-address mask [longer-prefixes] | detail | member-info | summary]
```

Parameters

- **0-5**: Enter the stack-unit ID, from 0 to 5.
- **pipe-number**: Enter the number of the Port-Pipe number.
  Range: 0 to 0
- **ip-address mask [longer-prefix]**: (OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. Enter the keyword `longer-prefixes` to view routes with a common prefix.
- **detail**: Enter the keyword `detail` to display the group index ID used by the ecmp routes in the CAM.
- **member-info**: Enter the keyword `member-info` to display the group index used by the ecmp, the number of egress ports (members) for the ecmp, and the port details of each member. The detail information under `member-info` will give the MAC address, VLAN ID and gateway of every member port of the ecmp.
- **summary**: (OPTIONAL) Enter the keyword `summary` to view a table listing route prefixes and the total number routes which can be entered in to CAM.

Command Modes

- **EXEC**
- **EXEC Privilege**

Command History

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module
**Figure 21-9. show ip cam stack-unit Command Example**

```text
FTOS#show ip cam stack-unit 0 port-set 0 10.10.10.10/32 longer-prefixes

<table>
<thead>
<tr>
<th>Destination</th>
<th>EC</th>
<th>CG</th>
<th>V</th>
<th>C</th>
<th>VId</th>
<th>Mac-Addr</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.10</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>00:00:00:00:00:00</td>
<td>3f01 CP</td>
</tr>
</tbody>
</table>

FTOS#```

**Table 21-5. show ip cam Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Displays the destination route of the index.</td>
</tr>
<tr>
<td>CG</td>
<td>Displays 0.</td>
</tr>
<tr>
<td>V</td>
<td>Displays a 1 if the entry is valid and a 0 otherwise.</td>
</tr>
<tr>
<td>C</td>
<td>Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the control processor, depending on Egress port.</td>
</tr>
<tr>
<td>V Id</td>
<td>Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.</td>
</tr>
<tr>
<td>Mac Addr</td>
<td>Displays the next-hop router’s MAC address.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry 17cl CP, the CP is the pertinent portion. CP = control processor, Fo = 40 Gigabit Ethernet interface, Te = 10 Gigabit Ethernet interface</td>
</tr>
</tbody>
</table>

**Figure 21-10. show ip cam stack-unit ecmp-group detail Command Example**

```text
FTOS#show ip cam stack-unit 0 po 0 ecmp-group detail

<table>
<thead>
<tr>
<th>Destination</th>
<th>EC</th>
<th>CG</th>
<th>V</th>
<th>C</th>
<th>VId</th>
<th>Mac-Addr</th>
<th>Port</th>
<th>ECMP Group-Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>00:01:e8:8a:d6:58</td>
<td>Te 0/3</td>
<td>-</td>
</tr>
<tr>
<td>2.1.1.1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>00:01:e8:8a:d6:58</td>
<td>Te 0/8</td>
<td>-</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>00:00:00:00:00:00</td>
<td>3f01 CP</td>
<td>-</td>
</tr>
<tr>
<td>2.1.1.0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>00:00:00:00:00:00</td>
<td>3f01 CP</td>
<td>-</td>
</tr>
<tr>
<td>2.1.1.1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>00:00:00:00:00:00</td>
<td>3f01 CP</td>
<td>-</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>00:00:00:00:00:00</td>
<td>3f01 CP</td>
<td>-</td>
</tr>
</tbody>
</table>

FTOS#```

**Figure 21-11. show ip cam stack-unit ecmp-group member-info detail Command Example**

```text
FTOS#show ip cam stack-unit 0 po 0 ecmp-group member-info detail

<table>
<thead>
<tr>
<th>Group Index</th>
<th>Member Count</th>
<th>Mac-Addr</th>
<th>Port</th>
<th>VLan ID</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>00:01:e8:8a:d6:58</td>
<td>Te 0/3</td>
<td>0</td>
<td>1.1.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>00:01:e8:8a:d6:58</td>
<td>Te 0/8</td>
<td>0</td>
<td>2.1.1.1</td>
</tr>
</tbody>
</table>

FTOS#```
**show ip fib stack-unit**

View all forwarding information base (FIB) entries.

**Syntax**

```
show ip fib stack-unit 0-5 [ip-address [mask] [longer-prefixes] | summary]
```

**Parameters**

- **0-5**: Enter the stack unit ID, from 0 to 5.
- **ip-address mask** (OPTIONAL): Enter the IP address of the network destination to view only information on that destination. Enter the IP address in dotted decimal format (A.B.C.D). You must enter the mask in slash prefix format (/X).
- **longer-prefixes** (OPTIONAL): Enter the keyword longer-prefixes to view all routes with a common prefix.
- **summary** (OPTIONAL): Enter the keyword summary to view the total number of prefixes in the FIB.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#show ip fib stack-unit 0

Destination                Gateway              First-Hop           Mac-Addr        Port    VId   EC
------------------  --------------------------- ----------------- ------------------- -------- ----- --
10.10.10.10/32       Direct, Nu 0                0.0.0.0           00:00:00:00:00:00 BLK HOLE      0  0
FTOS>
```

**Table 21-6. show ip fib stack-unit Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Lists the destination IP address.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Displays either the word Direct and an interface for a directly connected route or the remote IP address to be used to forward the traffic.</td>
</tr>
<tr>
<td>First-Hop</td>
<td>Displays the first hop IP address.</td>
</tr>
<tr>
<td>Mac-Addr</td>
<td>Displays the MAC address.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the egress-port information.</td>
</tr>
<tr>
<td>VId</td>
<td>Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.</td>
</tr>
<tr>
<td>EC</td>
<td>Displays the number of ECMP paths.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `clear ip fib stack-unit` Clears FIB entries on a specified stack unit.
show ip interface

View IP-related information on all interfaces.

Syntax

show ip interface [interface | brief] [configuration]

Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>(OPTIONAL) Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a Loopback interface, enter the keyword Loopback followed by a number from 0 to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For the Management interface, enter the keyword ManagementEthernet followed by zero (0).</td>
</tr>
<tr>
<td></td>
<td>• For the Null interface, enter the keyword null followed by zero (0).</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 128</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to view a brief summary of the interfaces and whether an IP address is assigned.</td>
</tr>
<tr>
<td>configuration</td>
<td>(OPTIONAL) Enter the keyword configuration to display the physical interfaces with non-default configurations only.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 21-13. show ip interface Command Example

```
FTOS#show ip int te 0/0
TenGigabitEthernet 0/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Inbound access list is not set
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent

FTOS#
```

Table 21-7. show ip interface Command Example Items

<table>
<thead>
<tr>
<th>Lines</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet 0/0...</td>
<td>Displays the interface's type, slot/port and physical and line protocol status.</td>
</tr>
<tr>
<td>Internet address...</td>
<td>States whether an IP address is assigned to the interface. If one is, that address is displayed.</td>
</tr>
</tbody>
</table>
show ip interface brief

View the IP addresses assigned to the Management interface.

**Syntax**

```
show ip management-route [all | connected | summary | static]
```

**Parameters**

- `all` (OPTIONAL) Enter the keyword `all` to view all IP addresses assigned to all Management interfaces on the switch.
- `connected` (OPTIONAL) Enter the keyword `connected` to view only routes directly connected to the Management interface.
show ip protocols

View information on all routing protocols enabled and active on the switch.

**Syntax**

```
show ip protocols
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#show ip protocols
Routing Protocol is "bgp 1"
Cluster Id is set to 20.20.20.3
Router Id is set to 20.20.20.3
Fast-external-fallover enabled
Regular expression evaluation optimization enabled
Capable of ROUTE_REFRESH
For Address Family IPv4 Unicast
BGP table version is 0, main routing table version 0
Distance: external 20 internal 200 local 200
Neighbor(s):
  Address : 20.20.20.2
    Filter-list in : foo
    Route-map in : foo
  Address : 5::6
    Weight : 0
    Address : 5::6
    Weight : 0
FTOS#
```
show ip route

View information, including how they were learned, about the IP routes on the switch.

**Syntax**
show ip route [hostname | ip-address [mask] [longer-prefixes] | list prefix-list [process-id] | all | connected | static | summary]

**Parameter**
- **ip-address**  (OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
- **mask**  (OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.
- **longer-prefixes**  (OPTIONAL) Enter the keyword longer-prefixes to view all routes with a common prefix.
- **list prefix-list**  (OPTIONAL) Enter the keyword list and the name of a configured prefix list. See show ip route list.
- **process-id**  (OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
- **connected**  (OPTIONAL) Enter the keyword connected to view only the directly connected routes.
- **all**  (OPTIONAL) Enter the keyword all to view both active and non-active routes.
- **static**  (OPTIONAL) Enter the keyword static to view only routes configured by the ip route command.
- **summary**  (OPTIONAL) Enter the keyword summary. See show ip route summary.

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 21-17. show ip route all Command Example**

```
FTOS#show ip route all
Codes: C - connected, S - static, R - RIP, B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated, O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS IEL, L2 - IS-IS IEC, IA - IS-IS inter area, * - candidate default, > - non-active route, + - summary route
Gateway of last resort is not set

Destination      Gateway                  Dist/Metric Last Change
---------------  ---------                  -------------  -----------
FTOS#
```
Example

Figure 21-18. show ip route summary and show ip route static Command Examples

Table 21-9. show ip route all Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(undefined)</td>
<td>Identifies the type of route:</td>
</tr>
<tr>
<td></td>
<td>• C = connected</td>
</tr>
<tr>
<td></td>
<td>• S = static</td>
</tr>
<tr>
<td></td>
<td>• R = RIP</td>
</tr>
<tr>
<td></td>
<td>• B = BGP</td>
</tr>
<tr>
<td></td>
<td>• IN = internal BGP</td>
</tr>
<tr>
<td></td>
<td>• EX = external BGP</td>
</tr>
<tr>
<td></td>
<td>• LO = Locally Originated</td>
</tr>
<tr>
<td></td>
<td>• O = OSPF</td>
</tr>
<tr>
<td></td>
<td>• IA = OSPF inter area</td>
</tr>
<tr>
<td></td>
<td>• N1 = OSPF NSSA external type 1</td>
</tr>
<tr>
<td></td>
<td>• N2 = OSPF NSSA external type 2</td>
</tr>
<tr>
<td></td>
<td>• E1 = OSPF external type 1</td>
</tr>
<tr>
<td></td>
<td>• E2 = OSPF external type 2</td>
</tr>
<tr>
<td></td>
<td>• i = IS-IS</td>
</tr>
<tr>
<td></td>
<td>• L1 = IS-IS level-1</td>
</tr>
<tr>
<td></td>
<td>• L2 = IS-IS level-2</td>
</tr>
<tr>
<td></td>
<td>• IA = IS-IS inter-area</td>
</tr>
<tr>
<td></td>
<td>• * = candidate default</td>
</tr>
<tr>
<td></td>
<td>• &gt; = non-active route</td>
</tr>
<tr>
<td></td>
<td>• + = summary routes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
<th>Identifies the route’s destination IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>Identifies whether the route is directly connected and on which interface the route is configured.</td>
</tr>
<tr>
<td>Dist/Metric</td>
<td>Identifies if the route has a specified distance or metric.</td>
</tr>
<tr>
<td>Last Change</td>
<td>Identifies when the route was last changed or configured.</td>
</tr>
</tbody>
</table>

show ip route list
Display IP routes in an IP prefix list.

Syntax
show ip route list prefix-list
**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

ip prefix-list

Enters the CONFIGURATION-IP PREFIX-LIST mode and configure a prefix list.

show ip prefix-list summary

Displays a summary of the configured prefix lists.

**Example**

**Figure 21-19. show ip route summary Command Example**

```
FTOS#show ip route list test
Codes: C - connected, S - static, R - RIP,
       B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated,
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
       L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default,
       > - non-active route, + - summary route
Gateway of last resort is not set

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>R 2.1.0.0/24</td>
<td>via 2.1.4.1, TenGig 4/43</td>
<td>120/2 3d0h</td>
</tr>
<tr>
<td>R 2.1.1.0/24</td>
<td>via 2.1.4.1, TenGig 4/43</td>
<td>120/2 3d1h</td>
</tr>
<tr>
<td>R 2.1.2.0/24</td>
<td>via 2.1.4.1, TenGig 4/43</td>
<td>120/1 3d0h</td>
</tr>
<tr>
<td>R 2.1.3.0/24</td>
<td>via 2.1.4.1, TenGig 4/43</td>
<td>120/1 3d1h</td>
</tr>
<tr>
<td>C 2.1.4.0/24</td>
<td>Direct, TenGig 4/43</td>
<td>0/0 3d1h</td>
</tr>
</tbody>
</table>
```
Example

Figure 21-20.  show ip route summary Command Example

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Active Routes</th>
<th>Non-active Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>static</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>ospf 100</td>
<td>1368</td>
<td>2</td>
</tr>
<tr>
<td>Intra-area: 762</td>
<td>Inter-area: 1</td>
<td>External-1: 600</td>
</tr>
<tr>
<td>Total</td>
<td>1388</td>
<td>2</td>
</tr>
<tr>
<td>Total 1388 active route(s) using 222440 bytes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total 2 non-active route(s) using 128 bytes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 21-10.  show ip route summary Column Headings

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Source</td>
<td>Identifies how the route is configured in FTOS.</td>
</tr>
<tr>
<td>Active Routes</td>
<td>Identifies the best route if a route is learned from two protocol sources.</td>
</tr>
<tr>
<td>Non-active Routes</td>
<td>Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route will become the best route.</td>
</tr>
<tr>
<td>ospf 100</td>
<td>If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.</td>
</tr>
<tr>
<td>Total 1388 active...</td>
<td>Displays the number of active and non-active routes and the memory usage of those routes.</td>
</tr>
<tr>
<td></td>
<td>If there are no routes configured in the FTOS, this line does not appear.</td>
</tr>
</tbody>
</table>

Related Commands

show ip route  Displays information about the routes found in switch.

show ip traffic

View IP, ICMP, UDP, TCP, and ARP traffic statistics.

Syntax

show ip traffic

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module
Example Figure 21-21. show ip traffic Command Example (partial)

```
FTOS#show ip traffic
IP statistics:
  Rcved: 10021161 total, 3197480 local destination
         2501 format errors, 390 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         115 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
         0 fragmented, 0 couldn't fragment
  Bcast: 6281 received, 0 sent; Mcast: 500 received, 0 sent
  Sent: 6573260 generated, 0 forwarded
         3830 encapsulation failed, 0 no route

ICMP statistics:
  Rcved: 0 format errors, 0 checksum errors, 0 redirects, 3 unreachable
         0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp, 0 info request, 0 other
  Sent: 0 redirects, 1 unreachable, 0 echo, 0 echo reply
         0 mask requests, 0 mask replies, 0 quench, 0 timestamp
         0 info reply, 0 time exceeded, 0 parameter problem

UDP statistics:
  Rcved: 2938110 total, 14 checksum errors, 1 no port
         0 short packets, 0 bad length, 1883908 no port broadcasts, 0 socket full
  Sent: 329731 total, 1883908 forwarded broadcasts
```

Table 21-11. show ip traffic output definitions

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>unknown protocol...</td>
<td>No receiver for these packets. Counts those packets whose protocol type field is not recognized by FTOS.</td>
</tr>
<tr>
<td>not a gateway...</td>
<td>Packets can not be routed; host/network is unreachable.</td>
</tr>
<tr>
<td>security failures...</td>
<td>Counts the number of received unicast/multicast packets that could not be forwarded due to:</td>
</tr>
<tr>
<td></td>
<td>• route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group</td>
</tr>
<tr>
<td></td>
<td>• destination IP address belongs to reserved prefixes; host/network unreachable</td>
</tr>
<tr>
<td>bad options...</td>
<td>Unrecognized IP option on a received packet.</td>
</tr>
<tr>
<td>Frags:</td>
<td>IP fragments received.</td>
</tr>
<tr>
<td>... reassembled</td>
<td>Number of IP fragments that were reassembled.</td>
</tr>
<tr>
<td>... timeouts</td>
<td>Number of times a timer expired on a reassembled queue.</td>
</tr>
<tr>
<td>... too big</td>
<td>Number of invalid IP fragments received.</td>
</tr>
<tr>
<td>... couldn’t fragment</td>
<td>Number of packets that could not be fragmented and forwarded.</td>
</tr>
<tr>
<td>... encapsulation failed</td>
<td>Counts those packets which could not be forwarded due to ARP resolution failure. FTOS sends an arp request prior to forwarding an IP packet.</td>
</tr>
<tr>
<td></td>
<td>If a reply is not received, FTOS repeats the request three times. These packets are counted in encapsulation failed.</td>
</tr>
<tr>
<td>Rcved:</td>
<td></td>
</tr>
<tr>
<td>... short packets</td>
<td>The number of bytes in the packet are too small.</td>
</tr>
<tr>
<td>... bad length</td>
<td>The length of the packet was not correct.</td>
</tr>
<tr>
<td>... no port broadcasts</td>
<td>The incoming broadcast/multicast packet did not have any listener.</td>
</tr>
<tr>
<td>... socket full</td>
<td>The applications buffer was full and the incoming packet had to be dropped.</td>
</tr>
</tbody>
</table>
The F10 monitoring MIB provides access to the statistics described below.

### Table 21-12. F10 Monitoring MIB

<table>
<thead>
<tr>
<th>Command Display</th>
<th>Object</th>
<th>OIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP statistics:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bcast:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Received</td>
<td>f10BcastPktRecv</td>
<td>1.3.6.1.4.1.6027.3.3.5.1.1</td>
</tr>
<tr>
<td>Sent</td>
<td>f10BcastPktSent</td>
<td>1.3.6.1.4.1.6027.3.3.5.1.2</td>
</tr>
<tr>
<td>Mcast:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Received</td>
<td>f10McastPktRecv</td>
<td>1.3.6.1.4.1.6027.3.3.5.1.3</td>
</tr>
<tr>
<td>Sent</td>
<td>f10McastPktSent</td>
<td>1.3.6.1.4.1.6027.3.3.5.1.4</td>
</tr>
<tr>
<td><strong>ARP statistics:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rcvd:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request</td>
<td>f10ArpReqRecv</td>
<td>1.3.6.1.4.1.6027.3.3.5.2.1</td>
</tr>
<tr>
<td>Replies</td>
<td>f10ArpReplyRecv</td>
<td>1.3.6.1.4.1.6027.3.3.5.2.3</td>
</tr>
<tr>
<td>Sent:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request</td>
<td>f10ArpReqSent</td>
<td>1.3.6.1.4.1.6027.3.3.5.2.2</td>
</tr>
<tr>
<td>Replies</td>
<td>f10ArpReplySent</td>
<td>1.3.6.1.4.1.6027.3.3.5.2.4</td>
</tr>
<tr>
<td>Proxy</td>
<td>f10ArpProxySent</td>
<td>1.3.6.1.4.1.6027.3.3.5.2.5</td>
</tr>
</tbody>
</table>

### show tcp statistics

View information on TCP traffic through the switch.

**Syntax**

show tcp statistics

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Table 21-13. show tcp statistics cp Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvd:</td>
<td>Displays the number and types of TCP packets received by the switch.</td>
</tr>
<tr>
<td></td>
<td>• Total = total packets received</td>
</tr>
<tr>
<td></td>
<td>• no port = number of packets received with no designated port.</td>
</tr>
<tr>
<td>0 checksum error...</td>
<td>Displays the number of packets received with the following:</td>
</tr>
<tr>
<td></td>
<td>• checksum errors</td>
</tr>
<tr>
<td></td>
<td>• bad offset to data</td>
</tr>
<tr>
<td></td>
<td>• too short</td>
</tr>
<tr>
<td>329 packets...</td>
<td>Displays the number of packets and bytes received in sequence.</td>
</tr>
<tr>
<td>17 dup...</td>
<td>Displays the number of duplicate packets and bytes received.</td>
</tr>
<tr>
<td>0 partially...</td>
<td>Displays the number of partially duplicated packets and bytes received.</td>
</tr>
<tr>
<td>7 out-of-order...</td>
<td>Displays the number of packets and bytes received out of order.</td>
</tr>
<tr>
<td>0 packets with data after window</td>
<td>Displays the number of packets and bytes received that exceed the switch’s</td>
</tr>
<tr>
<td></td>
<td>window size.</td>
</tr>
<tr>
<td>0 packets after close</td>
<td>Displays the number of packet received after the TCP connection was closed.</td>
</tr>
<tr>
<td>0 window probe packets...</td>
<td>Displays the number of window probe and update packets received.</td>
</tr>
<tr>
<td>41 dup ack...</td>
<td>Displays the number of duplicate acknowledgement packets and</td>
</tr>
<tr>
<td></td>
<td>acknowledgement packets with data received.</td>
</tr>
<tr>
<td>10184 ack...</td>
<td>Displays the number of acknowledgement packets and bytes received.</td>
</tr>
<tr>
<td>Sent:</td>
<td>Displays the total number of TCP packets sent and the number of urgent</td>
</tr>
<tr>
<td></td>
<td>packets sent.</td>
</tr>
<tr>
<td>25 control packets...</td>
<td>Displays the number of control packets sent and the number retransmitted.</td>
</tr>
<tr>
<td>11603 data packets...</td>
<td>Displays the number of data packets sent.</td>
</tr>
<tr>
<td>24 data packets retransmitted</td>
<td>Displays the number of data packets resent.</td>
</tr>
</tbody>
</table>
Table 21-13. show tcp statistics cp Command Example Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>355 ack...</td>
<td>Displays the number of acknowledgement packets sent and the number of packet delayed.</td>
</tr>
<tr>
<td>0 window probe...</td>
<td>Displays the number of window probe and update packets sent.</td>
</tr>
<tr>
<td>7 Connections initiated...</td>
<td>Displays the number of TCP connections initiated, accepted, and established.</td>
</tr>
<tr>
<td>14 Connections closed...</td>
<td>Displays the number of TCP connections closed, dropped.</td>
</tr>
<tr>
<td>20 Total rxmt...</td>
<td>Displays the number of times the switch tried to re-send data and the number of connections dropped during the TCP retransmit timeout period.</td>
</tr>
<tr>
<td>0 Keepalive....</td>
<td>Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.</td>
</tr>
</tbody>
</table>
Internet Protocol Security (IPSec)

Commands

Internet protocol security (IPSec) is an end-to-end security scheme for securing IP communications by authenticating and encrypting all packets in a session. Use IPSec between hosts, gateways, or hosts and gateways.

IPSec uses a series of protocol functions to achieve information security:

- **Authentication Headers (AH)** — Connectionless integrity and origin authentication for IP packets.
- **Encapsulating Security Payloads (ESP)** — Confidentiality, authentication, and data integrity for IP packets.
- **Security Associations (SA)** — Algorithm-provided parameters required for AH and ESP protocols.

IPSec capability is available on control (protocol) and management traffic; end-node support is required.

IPSec supports two operational modes:

- **Transport mode** — Transport is the default mode for IPSec and encrypts only the payload of the packet. Routing information is unchanged.
- **Tunnel mode** — Use Tunnel mode to encrypt the entire packet, including the routing information in the IP header. Tunnel mode is typically used in creating VPNs.

Transport mode provides IP packet payload protection using ESP or AH. You can use ESP alone or in combination with AH to provide additional authentication. AH protect data from modification but do not provide confidentiality.

SA is the configuration information that specifies the type of security provided to the IPSec flow. SA is a set of algorithms and keys used to authenticate and encrypt the traffic flow. The AH and ESP use SA to provide traffic protection for the IPSec flow.

This chapter describes the IPSec-related commands. They are:

- `crypto ipsec transform-set`
- `crypto ipsec policy`
- `management crypto-policy`
- `match`
- `session-key`
- `show crypto ipsec transform-set`
- `show crypto ipsec policy`
- `transform-set`
**crypto ipsec transform-set**

Create a transform set, or combination of security algorithms and protocols, of cryptos.

**Syntax**

```
crypto ipsec transform-set name {ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}
```

To delete a transform set, use the `no crypto ipsec transform-set name {ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Enter the name for the transform set.</td>
</tr>
</tbody>
</table>
| ah-authentication| Enter the keyword `ah-authentication` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.  
  - `md5` — Use Message Digest 5 (MD5) authentication.  
  - `sha1` — Use Secure Hash Algorithm 1 (SHA-1) authentication.  
  - `null` — Causes an encryption policy configured for the area to not be inherited on the interface. |
| esp-authentication| Enter the keyword `esp-authentication` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.  
  - `md5` — Use Message Digest 5 (MD5) authentication.  
  - `sha1` — Use Secure Hash Algorithm 1 (SHA-1) authentication.  
  - `null` — Causes an encryption policy configured for the area to not be inherited on the interface. |
| esp-encryption   | Enter the keyword `esp-encryption` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.  
  - `3des` — Use 3DES encryption.  
  - `cbc` — Use CDC encryption.  
  - `des` — Use DES encryption.  
  - `null` — Causes an encryption policy configured for the area to not be inherited on the interface. |

**Defaults**

`none`

**Command Modes**

`CONFIGURATION`

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

- Both sides of the link must specify the same transform set.
- You can create up to 64 transform sets.

**Example**

```
FTOS(conf)#int ten 0/4
FTOS(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64
FTOS(conf)#int ten 0/6
FTOS(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

**crypto ipsec policy**

Create a crypto policy used by ipsec.
### crypto ipsec policy command

**Syntax**
```
crypto ipsec policy name seq-num ipsec-manual
```

To delete a crypto policy entry, use the `no crypto ipsec policy name seq-num ipsec-manual` command.

**Parameters**
- **name**
  - Enter the name for the crypto policy set.
- **seq-num**
  - Enter the sequence number assigned to the crypto policy entry. The range is from 0 to 255.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

This command creates a crypto policy entry and enters the crypto map configuration mode for configuring the flow parameters.

**Example**

```
FTOS(conf)#crypto ipsec policy West 10 ipsec-manual
FTOS(conf-crypto-policy)#
```

### management crypto-policy command

**Syntax**
```
management crypto-policy name
```

To remove the management traffic crypto policy, use the `no management crypto-policy name` command.

**Parameters**
- **name**
  - Enter the name for the crypto policy.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### match command

**Syntax**
```
match seq-num {tcp | udp} {ipv6 | ip} port-num dest-ip dest-port-num
```

To remove the a sequence number from the TCP/UDP packets, use the `no match seq-num` command.

**Parameters**
- **seq-num**
  - Enter the match command sequence number. The range is from 0 to 255.
- **tcp**
  - Enter the keyword `tcp` to configure a TCP access list filter.
### udp
Enter the keyword `udp` to configure a UDP access list filter.

### ipv6
Enter the source IPv6 address.

### ip
Enter the source IPv4 address.

### port-num
Enter the source port number. The range is from 0 to 65535.

### dest-ip
Enter the destination IP address.

### dest-port-num
Enter the destination port number. The range is from 0 to 65535.

#### Defaults
none

#### Command Modes
CONFIG-CRYPTO-POLICY

#### Command History
Introduced on the MXL 10/40GbE Switch IO Module.

#### Example
```
FTOS(conf-crypto-policy)#match 0 tcp a::1 /128 0 a::2 /128 23
FTOS(conf-crypto-policy)#match 1 tcp a::1 /128 23 a::2 /128 0
FTOS(conf-crypto-policy)#match 2 tcp a::1 /128 0 a::2 /128 21
FTOS(conf-crypto-policy)#match 3 tcp a::1 /128 21 a::2 /128 0
FTOS(conf-crypto-policy)#match 4 tcp 1.1.1.1 /32 0 1.1.1.2 /32 23
FTOS(conf-crypto-policy)#match 5 tcp 1.1.1.1 /32 23 1.1.1.2 /32 0
FTOS(conf-crypto-policy)#match 6 tcp 1.1.1.1 /32 0 1.1.1.2 /32 21
FTOS(conf-crypto-policy)#match 7 tcp 1.1.1.1 /32 21 1.1.1.2 /32 0
```

#### Usage Information
UDP is not supported. Only TCP 23 telnet and 21 ftp are supported.

## session-key
Specify the session keys used in the crypto map entry.

### Syntax
```
session-key {inbound | outbound} {ah spi hex-key-string | esp spi encrypt hex-key-string auth hex-key-string}
```

To delete the session key information from the crypto map, use the `no session-key {inbound | outbound} {ah | esp}` command.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Enter the name of the host to delete. Enter * to delete all host table entries.</td>
</tr>
<tr>
<td><code>inbound</code></td>
<td>Specify the inbound session key for IPSec.</td>
</tr>
<tr>
<td><code>outbound</code></td>
<td>Specify the outbound session key for IPSec.</td>
</tr>
<tr>
<td><code>ah</code></td>
<td>Use AH when the AH transform set is selected in the crypto map.</td>
</tr>
<tr>
<td><code>esp</code></td>
<td>Use ESP when the ESP transform set is selected in the crypto map.</td>
</tr>
<tr>
<td><code>spi</code></td>
<td>Enter the security parameter index number.</td>
</tr>
<tr>
<td><code>hex-key-string</code></td>
<td>Enter the session key in hex format (a string of 8, 16, or 20 bytes). For DES algorithms, specify at least 16 bytes per key. For SHA algorithms, specify at least 20 bytes per key.</td>
</tr>
<tr>
<td><code>encrypt</code></td>
<td>Indicates the ESP encryption transform set key string.</td>
</tr>
<tr>
<td><code>auth</code></td>
<td>Indicates the ESP authentication transform set key string.</td>
</tr>
</tbody>
</table>

### Defaults
none
show crypto ipsec transform-set
Display the transform set configuration.

Syntax
show crypto ipsec transform-set name

Parameters
name Enter the name of the transform set.

Command Mode
EXEC

Example
FTOS#show crypto ipsec transform-set
Transform-Set Name : dallas
Transform-Set refCnt : 0
AH Transform : 
ESP Auth Transform : 
ESP Encry Transform : 3des
FTOS#

show crypto ipsec policy
Display the crypto policy configuration.

Syntax
show crypto ipsec policy name

Parameters
name Enter the name for the crypto policy set.

Command Modes
EXEC

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Example:  

```
FTOS#show crypto ipsec policy

Policy name : West
Policy refcount : 1
Sequence Num : 10
SA Mode : IPSEC-MANUAL
Transform-Set Name : dallas
Peer IP Address :
Inbound AH SPI : 0
Inbound ESP Auth SPI : 0
Inbound ESP Encry SPI : 256
Inbound AH Key : 
Inbound ESP Auth Key : [0]:
Inbound ESP Encry Key : 

Outbound AH SPI : 0
Outbound ESP Auth SPI : 0
Outbound ESP Encry SPI : 257
Outbound AH Key : 
Outbound ESP Auth Key : [0]:
Outbound ESP Encry Key : 

Match sequence Num : 0
Protocol type : tcp
IP or IPv6 : IPv6
Source address : a::1
Source mask : /128
Source port : 0
Destination address : a::2
Destination mask : /128
Destination port : 23
source-interface name :
source-interface num :

Match sequence Num : 1
Protocol type : tcp
IP or IPv6 : IPv6
Source address : a::1
Source mask : /128
Source port : 0
Destination address : a::2
Destination mask : /128
Destination port : 23
source-interface name :
source-interface num :

Match sequence Num : 2
Protocol type : tcp
IP or IPv6 : IPv6
Source address : a::1
Source mask : /128
Source port : 0
Destination address : a::2
Destination mask : /128
Destination port : 21
source-interface name :
source-interface num :

Match sequence Num : 3
Protocol type : tcp
IP or IPv6 : IPv6
Source address : a::1
Source mask : /128
Source port : 21
Destination address : a::2
Destination mask : /128
Destination port : 0
source-interface name :
source-interface num :

FTOS#
```
transform-set

Specify the transform set used in the crypto map.

Syntax

transform-set transform-set-name

To delete a transform set from the crypto map, use the no transform-set transform-set-name command.

Parameters

<table>
<thead>
<tr>
<th>transform-set-name</th>
<th>Enter the name for the crypto map transform set.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defaults</td>
<td>none</td>
</tr>
<tr>
<td>Command Modes</td>
<td>CONFIG-CRYPTO-POLICY</td>
</tr>
<tr>
<td>Command History</td>
<td>Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>
IPv6 Access Control Lists (IPv6 ACLs)

Overview

IPv6 ACLs and IPv6 Route Map commands are supported on the Dell Networking MXL Switch.

Note: For IPv4 ACL commands, refer to the Access Control Lists (ACL) chapter.

Important Points to Remember

- Certain platforms require manual CAM usage space allotment. For more information, refer to the cam-acl command.
- Egress IPv6 ACL and IPv6 ACL on the Loopback interface is not supported.
- Reference to an empty ACL permits any traffic.
- ACLs are not applied to self-originated traffic (for example, Control Protocol traffic not affected by IPv6 ACL because the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set).
- You can use the same access list name for both IPv4 and IPv6 ACLs.
- You can apply both IPv4 and IPv6 ACLs on an interface at the same time.
- You can apply IPv6 ACLs on physical interfaces and a logical interfaces (Port-channel/VLAN).
- Non-contiguous masks are not supported in source or destination addresses in IPv6 ACL entries.
- Because the prefix mask is specified in /x format in IPv6 ACLs, inverse mask is not supported.
IPv6 ACL Commands

The following commands configure IPv6 ACLs:

- cam-acl
- cam-acl-egress
- ipv6 control-plane egress-filter
- ipv6 access-list
- permit
- permit icmp
- show cam-acl
- show cam-acl-egress

### cam-acl

Allocate space for IPv6 ACLs.

**Syntax**

```
cam-acl {default | l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Use the default CAM profile settings, and set the CAM as follows.</td>
</tr>
<tr>
<td></td>
<td>- L3 ACL (ipv4acl): 6</td>
</tr>
<tr>
<td></td>
<td>- L2 ACL(l2acl): 5</td>
</tr>
<tr>
<td></td>
<td>- IPv6 L3 ACL (ipv6acl): 0</td>
</tr>
<tr>
<td></td>
<td>- L3 QoS (ipv4qos): 1</td>
</tr>
<tr>
<td></td>
<td>- L2 QoS (l2qos): 1</td>
</tr>
<tr>
<td>l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10</td>
<td>Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 13. The ipv6acl range must be a factor of 2.</td>
</tr>
</tbody>
</table>

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

**Usage Information**

For the new settings to take effect, save the new CAM settings to the startup-config (write-mem or copy run start), then reload the system.

The total amount of space allowed is 16 FP blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the ipv6acl profile which is from 0 to 10. The ipv6acl allocation must be a factor of 2 (2, 4, 6, 8, 10).
cam-acl-egress

Allocate space for IPv6 egress ACLs.

Syntax

```plaintext
cam-acl-egress {default | l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4}
```

Parameters

- **default**
  - Use the default CAM profile settings, and set the CAM as follows.
  - L2 ACL (l2acl): 1
  - L3 ACL (ipv4acl): 1
  - IPv6 L3 ACL (ipv6acl): 2

- **l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4**
  - Allocate space to support IPv6 ACLs. Enter all of the profiles and a range for each. Enter the CAM profile name followed by the amount to be allotted.
  - The total space allocated must equal 13.
  - The `ipv6acl` range must be a factor of 2.

Command Modes

**CONFIGURATION**

Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (`write-mem` or `copy run start`), then reload the system.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The `ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10).

Example

**Figure 23-1. Command Example: cam-acl-egress**

```
FTOS# configure
Force10(config)# cam-acl-egress?
default Reset Egress CAM ACL entries to default setting
l2acl Set L2-ACL entries
Force10(config)# cam-acl-egress l2acl ?
<1-4> Number of FP blocks for l2acl
Force10(config)# cam-acl-egress l2acl 1 ?
ipv4acl Set IPv4-ACL entries
Force10(config)# cam-acl-egress l2acl 1 ipv4acl 1 ?
ipv6acl Set IPv6-ACL entries
Force10(config)# cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl ?
<0-4> Number of FP blocks for IPv6 (multiples of 2)
Force10(config)# cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl 2
```

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

Syntax

```plaintext
ipv6 access-list access-list-name
```

To delete an access list, use the `no ipv6 access-list access-list-name` command.
IPv6 Access Control Lists (IPv6 ACLs)

All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

Command Modes

**CONFIGURATION**

Parameters

- **access-list-name**
  - Enter the as the access list name as a string, up to 140 characters.

Defaults

The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your line card documentation.

Related Commands

- **show config**
  - View the current configuration.

ipv6 control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv6 CPU traffic.

Syntax

```
ipv6 control-plane egress-filter
```

Defaults

Not enabled

Command Modes

**EXEC Privilege**

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

permit

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

Syntax

```
permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number
- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp} command

Parameters

- **ip-protocol-number**
  - Enter an IPv6 protocol number. The range is from 0 to 255.
- **icmp**
  - Enter the keyword icmp to filter Internet Control Message Protocol version 6.
- **ipv6**
  - Enter the keyword ipv6 to filter any Internet Protocol version 6.
- **tcp**
  - Enter the keyword tcp to filter the Transmission Control protocol.
- **udp**
  - Enter the keyword udp to filter the User Datagram Protocol.

Defaults

Not configured.

Command Modes

**ACCESS-LIST**
permit icmp

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

**Syntax**

```
permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [message-type] [count [byte]] | [log] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number
- Use the `no permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

**Parameters**

- **source address**: Enter the IPv6 address of the network or host from which the packets were sent in the `x:x:x:x:x` format followed by the prefix length in the `/x` format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
- **mask**: Enter a network mask in /prefix format (/x).
- **any**: Enter the keyword any to specify that all routes are subject to the filter.
- **host ipv6-address**: Enter the keyword host followed by the IPv6 address of the host in the `x:x:x:x:x` format. The :: notation specifies successive hexadecimal fields of zero.
- **destination address**: Enter the IPv6 address of the network or host to which the packets are sent in the `x:x:x:x:x` format followed by the prefix length in the `/x` format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
- **message-type**: (OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is from 0 to 255 for ICMP type and from 0 to 255 for ICMP code.
- **count**: (OPTIONAL) Enter the keyword count to count packets processed by the filter.
- **byte**: (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.
- **log**: (OPTIONAL) Enter the keyword log to have the information kept in an ACL log file.
- **monitor**: (OPTIONAL) Enter the keyword monitor to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

**Defaults**

Not configured

**Command Modes**

ACCESS-LIST

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
show cam-acl

Show space allocated for IPv6 ACLs.

Syntax

show cam-acl

Command Modes

EXEC

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

cam-acl Configure CAM profiles to support IPv6 ACLs.

Examples

Figure 23-2. Command Example: show cam-acl (default profile)

FTOS#show cam-acl

-- Chassis Cam ACL --
  Current Settings(in block sizes)
  L2Acl    :    5
  Ipv4Acl  :    6
  Ipv6Acl  :    0
  Ipv4Qos  :    1
  L2Qos    :    1

-- Line card 4 --
  Current Settings(in block sizes)
  L2Acl    :    2
  Ipv4Acl  :    6
  Ipv6Acl  :    0
  Ipv4Qos  :    1
  L2Qos    :    1

FTOS#show cam-acl

Figure 23-3. Command Example: show cam-acl (manually set profiles)

FTOS#show cam-acl

-- Chassis Cam ACL --
  Current Settings(in block sizes)
  L2Acl    :    2
  Ipv4Acl  :    2
  Ipv6Acl  :    4
  Ipv4Qos  :    2
  L2Qos    :    3

-- Line card 4 --
  Current Settings(in block sizes)
  L2Acl    :    2
  Ipv4Acl  :    2
  Ipv6Acl  :    4
  Ipv4Qos  :    2
  L2Qos    :    3

FTOS#show cam-acl
show cam-acl-egress

Show information on FP groups allocated for egress ACLs.

Syntax
show cam-acl-egress

Command Modes
EXEC
EXEC Privilege

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands
cam-acl Configure CAM profiles to support IPv6 ACLs

Examples

Figure 23-4. Command Example: show cam-acl-egress (default profile)

FTOS#show cam-acl-egress
-- Chassis Egress Cam ACL --
  Current Settings(in block sizes)
  L2Acl : 1
  Ipv4Acl : 1
  Ipv6Acl : 2
-- Stack unit 0 --
  Current Settings(in block sizes)
  L2Acl : 1
  Ipv4Acl : 1
  Ipv6Acl : 2

FTOS#show cam-acl
IPv6 Basics

Overview

This chapter describes IPv6 basic commands for the MXL 10/40GbE Switch IO Module.

Commands

The IPv6 commands in the chapter are:

- clear ipv6 fib
- clear ipv6 route
- clear ipv6 mld_host
- ipv6 address autoconfig
- ipv6 address
- ipv6 address eui64
- ipv6 control-plane icmp error-rate-limit
- ipv6 flowlabel-zero
- ipv6 host
- ipv6 name-server
- ipv6 nd dad attempts
- ipv6 nd prefix
- ipv6 route
- ipv6 unicast-routing
- show ipv6 cam stack-unit
- show ipv6 control-plane icmp
- show ipv6 fib stack-unit
- show ipv6 flowlabel-zero
- show ipv6 interface
- show ipv6 mld_host
- show ipv6 route
- trust ipv6-diffserv
clear ipv6 fib

Clear (refresh) all forwarding information base (FIB) entries on a linecard or stack unit.

**Syntax**

```
clear ipv6 fib linecard slot | stack-unit unit-number
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>Enter the slot number to clear the FIB for a linecard.</td>
</tr>
<tr>
<td>unit-number</td>
<td>Enter the stack member number.</td>
</tr>
</tbody>
</table>

**Command Mode**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

**Syntax**

```
clear ipv6 route {* | ipv6-address prefix-length}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Enter the * to clear (refresh) all routes from the IPv6 routing table.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>Enter the IPv6 address in the x:x::::x format followed by the prefix length in the /x format.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>Range: /0 to /128</td>
</tr>
</tbody>
</table>

**Note:** The :: notation specifies successive hexadecimal fields of zeros

**Command Mode**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

clear ipv6 mld_host

Clear the IPv6 MLD host counters and reset the elapsed time.

**Syntax**

```
clear ipv6 mld_host
```

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

ipv6 address autoconfig

Configure IPv6 address auto-configuration for the management interface.

**Syntax**

```
ipv6 address autoconfig
```

To disable the address autoconfig operation on the management interface, use the `no ipv6 address autoconfig` command.
SAA can configure up to two addresses. If any preferred prefix or valid timers time out, the corresponding address are deprecated or removed. If an address is removed due to a time-out, an address from the current unused prefix is used to create a new address. If there are no remaining prefixes, the software waits to receive a new prefix from the RA.

- If auto-configuration is enabled, all IPv6 addresses on that management interface are auto-configured. Manual and auto-configurations are not supported on a single management interface.
- Removing auto-configuration removes all auto-configured IPv6 addresses and the link-local IPv6 address from that management interface.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across a platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

**ipv6 address**

Configure an IPv6 address to an interface.

```
Syntax
ipv6 address {ipv6-address prefix-length}

Parameters
ipv6-address prefix-length

Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format.
Range: /0 to /128

Note: The :: notation specifies successive hexadecimal fields of zeros
```

```
Defaults
none

Command Modes
INTERFACE

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
```

```
Example
FTOS(conf)#interface gigabitethernet 10/0
FTOS(conf-if-gi-10/0)#ipv6 address ?
X:X:X:X::X IPv6 address
FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 ?
<0-128> Prefix length in bits
FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96 ?
<cr>
```
FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96
FTOS(conf-if-gi-10/0)#show config
! interface GigabitEthernet 10/0
  no ip address
  ipv6 address 2002:1:2::3 /96
  no shutdown
FTOS(conf-if-gi-10/0)#

- If two addresses are configured, delete an existing address before configuring a new address.
- If the last manually-configured global IPv6 address is removed using the “no” form of the command, the link-local IPv6 address is removed automatically.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

ttp://www.dell.com/support.dell.com

**Usage Information**

- If two addresses are configured, delete an existing address before configuring a new address.
- If the last manually-configured global IPv6 address is removed using the “no” form of the command, the link-local IPv6 address is removed automatically.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

[ipv6 address eui64](#)

Configure IPv6 EUI64 address configuration on the interface.

**Syntax**

```
ipv6 address {ipv6-address prefix-length} eui64
```

To disable IPv6 EUI64 address autoconfiguration, use the `no ipv6 address {ipv6-address prefix-length} eui64` command.

**Parameters**

- **ipv6-address**
  - Enter the IPv6 prefix in the x:x::x::x format then the prefix length in the /x format. The range is from /0 to /128.
- **prefix-length**
  - Enter the IPv6 prefix length in the /x format.

**Notes:** The :: notation specifies successive hexadecimal fields of zeros.

**Command Modes**

- CONFIGURATION

**Default**

- none

**Command History**

- Version 9.2(0.0) Introduced on the M6100 Series.

**Example**

```
FTOS(conf)#int ten 0/4
FTOS(conf-if-te-0/4)#ipv6 address 2001::/64 eui64
FTOS(conf)#int ten 0/6
FTOS(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

**Usage Information**

This command allows you to create an EUI64 address based on the specified prefix and MAC address only. Prefixes may be configured on the interface using the `ipv6 nd prefix` command without creating an EUI64 address.
ipv6 control-plane icmp error-rate-limit

Configure the maximum number of ICMP error packets per second that can be sent per second.

**Syntax**

```
ipv6 control-plane icmp error-rate-limit \{1-200\}
```

To restore the default value, use the `no ipv6 control-plane icmp error-rate-limit` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>pps</strong></td>
<td>Enter the maximum number of error packets to be generated per second. Range: 1 to 200, where 0 disables the rate-limiting.</td>
</tr>
</tbody>
</table>

**Command Modes**

CONFIGURATION

**Default**

100 pps

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 flowlabel-zero

Configure system to set the flow label field in the packets to zero.

**Syntax**

```
ipv6 flowlabel-zero
```

To disable the 0 from being set in the field and allow the field to be filled by protocol operations, use the `no ipv6 flowlabel-zero` command.

**Default**

Disabled

**Command Modes**

CONFIGURATION

**Default**

100 pps

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If the flowlabel value is already set for BGP or SSH, the system defaults to the already configured value. All packets on the same connection are considered part of the same flow by the system. For new connections, the new flowlabel is set to zero.

ipv6 host

Assign a name and IPv6 address to be used by the host-to-IPv6 address mapping table.

**Syntax**

```
ipv6 host name \{ipv6-address\}
```

To remove an IP host, use the `no ipv6 host name \{ipv6-address\}` command.
ipv6 name-server

Enter up to six IPv6 addresses of name servers. The order you enter the addresses determines the order of their use.

Syntax: ipv6 name-server ipv6-address [ipv6-address2... ipv6-address6]

To remove a name server, use the no ipv6 name-server ipv6-address command.

Parameters:
- **ipv6-address**: Enter the IPv6 address (X:X:X:X::X) of the name server to be used. Note: The :: notation specifies successive hexadecimal fields of zeros.
- **ipv6-address2**, **ipv6-address6** (OPTIONAL): Enter up to five more IPv6 addresses, in the x:x:x:x::x format, of name servers to be used. Separate the IPv6 addresses with a space.

Defaults: none

Command Modes: CONFIGURATION

Command History:
- Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information:
You can separately configure both IPv4 and IPv6 domain name servers.

ipv6 nd dad attempts

To perform duplicate address detection (DAD) on the management interface, configure the number of neighbor solicitation messages that are sent.

Syntax: ipv6 nd dad attempts {number of attempts}

To restore the default value, use the no ipv6 nd dad attempts command.

Parameters:
- **number of attempts**: Enter the number of attempts to be made to detect a duplicate address. Range: 0 to 15. Setting the value to 0 disables DAD on the interface.

Default: 3 attempts
**ipv6 nd prefix**

Specify which IPv6 prefixes are included in Neighbor Advertisements.

**Syntax**

```
ipv6 nd prefix {ipv6-prefix | prefix-length | default} [no-advertise] | [no-autoconfig] [no-rtr-address] [off-link] [lifetime {valid | infinite} {preferred | infinite}]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-prefix</td>
<td>Enter an IPv6 prefix.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>Enter the prefix followed by the prefix length. The length range is from 0 to 128.</td>
</tr>
<tr>
<td>default</td>
<td>Enter this keyword to set default parameters for all prefixes.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Enter this keyword to prevent the specified prefix from being advertised.</td>
</tr>
<tr>
<td>no-autoconfig</td>
<td>Enter this keyword to disable Stateless Address Autoconfiguration.</td>
</tr>
<tr>
<td>no-rtr-address</td>
<td>Enter this keyword to exclude the full router address from router advertisements (the R bit is not set).</td>
</tr>
<tr>
<td>off-link</td>
<td>Enter this keyword to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.</td>
</tr>
<tr>
<td>valid-lifetime</td>
<td>Enter the amount of time that the prefix is advertised, or enter the maximum value for an unlimited amount of time. Default: 2592000. Range: 0 to 4294967295. The maximum value means that the preferred lifetime does not expire for the valid-life time parameter.</td>
</tr>
<tr>
<td>preferred-lifetime</td>
<td>Enter the amount of time that the prefix is preferred, or enter the maximum value for an unlimited amount of time. The range is from 0 to 4294967295. The default is 2592000. The maximum value indicates the preferred lifetime and does not expire.</td>
</tr>
</tbody>
</table>

**Command Mode**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; the default keyword can be used to use the default parameters for all prefixes. If a prefix has been configured with lifetime parameter values, the default values cannot be applied using the `ipv6 nd prefix default` no-autoconfig command.

**ipv6 route**

Establish a static IPv6 route.
Syntax

```
ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]
```

Parameters

- **ipv6-address prefix-length**: Enter the IPv6 address in the `x:x:x:x::x` format followed by the prefix length in the `/x` format.
  - Range: `/0` to `/128`
  - **Note**: The `::` notation specifies successive hexadecimal fields of zeros
- **interface** *(OPTIONAL)*: Enter the following keywords and slot/port or number information:
  - For a loopback interface, enter the keyword `loopback` followed by a number from zero (0) to 16383.
  - For the null interface, enter the keyword `null` followed by zero (0).
  - For a port channel interface, enter the keyword `port-channel` followed by the port channel number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a tunnel interface, enter the keyword `tunnel` followed by the tunnel interface number. The range is from 1 to 16383.
  - For a VLAN interface, enter the keyword `VLAN` followed by the VLAN number. The range is from 1 to 4094.

If you configure a static IPv6 route using an egress interface and enter the `ping` command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the `ping` command to detect the destination address.

- **ipv6-address** *(OPTIONAL)*: Enter the forwarding router IPv6 address in the `x:x:x:x::x` format.
  - **Note**: The `::` notation specifies successive hexadecimal fields of zeros
- **distance** *(OPTIONAL)*: Enter a number as the metric distance assigned to the route. The range is from 1 to 255.
- **tag value** *(OPTIONAL)*: Enter the keyword `tag` followed by a tag value number. The range is from 1 to 4294967295.
- **permanent** *(OPTIONAL)*: Enter the keyword `permanent` to specify that the route is not to be removed, even if the interface assigned to that route goes down.
  - **Note**: If you disable the interface with an IPv6 address associated with the keyword `permanent`, the route disappears from the routing table.

Defaults

- **none**

Command Modes

- **CONFIGURATION**

Command History

- **Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
FTOS(conf)#ipv6 route 44::0 /64 33::1 ?
<1-255>
distance  Distance metric for this route
permanent Permanent route
tag Set tag for this route

FTOS(conf)#ipv6 route 55::0 /64 ?
X:1:2:x::x Forwarding router's address
gigabitethernet Gigabit Ethernet interface
```
IPv6 Basics

loopback                        Loopback interface
null                            Null interface
port-channel                    Port channel interface
sonet                           Sonet interface
tenGigabitethernet              TenGigabit Ethernet interface
vlan                            VLAN interface

FTOS(conf)#ipv6 route 55::0 /64 gigabitethernet 9/0 ?
<1-255>                         Distance metric for this route
X:X:X:X::X                      Forwarding router's address
permanent                       Permanent route
tag                             Set tag for this route

FTOS(conf)#ipv6 route 55::0 /64 gigabitethernet 9/0 66::1 ?
<1-255>                         Distance metric for this route
permanent                       Permanent route
tag                             Set tag for this route

Usage Information
When the interface goes down, FTOS withdraws the route. The route is re-installed, by FTOS, when the interface comes back up. When a recursive resolution is “broken,” FTOS withdraws the route. The route is re-installed, by FTOS, when the recursive resolution is satisfied.

After an IPv6 static route interface is created, if an IP address is not assigned to a peer interface, the peer must be manually pinged to resolve the neighbor information.

Related Commands
show ipv6 route View the IPv6 configured routes.

ipv6 unicast-routing

Enable IPv6 Unicast routing.

Syntax
ipv6 unicast-routing

To disable unicast routing, use the no ipv6 unicast-routing command.

Defaults
Enabled

Command Modes
CONFIGURATION

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
Because this command is enabled by default, it does not appear in the running configuration. When unicast routing is disabled, the no ipv6 unicast-routing command is included in the running configuration. Whenever unicast routing is disabled or re-enabled, FTOS generates a syslog message indicating the action.

Disabling unicast routing on a chassis causes the following behavior:

• static and protocol learnt routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated.
• connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable.
additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed

- the IPv6 address family configuration (under router bgp) is deleted
- IPv6 Multicast traffic continues to flow unhindered

**show ipv6 cam stack-unit**

Display the IPv6 CAM entries for the specified stack-unit.

**Syntax**

```
show ipv6 cam stack-unit unit-number port-set {0-1} [summary | index | ipv6 address]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit-number</td>
<td>Enter the stack unit’s ID number. The range is from 0 to 11.</td>
</tr>
<tr>
<td>port-set</td>
<td>Enter the keyword Port Set.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword summary to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.</td>
</tr>
<tr>
<td>index</td>
<td>(OPTIONAL) Enter the index in the IPv6 CAM</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>Enter the IPv6 address in the x:x:x:x::x/n format to display networks that have more specific prefixes. Range: /0 to /128</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

First-Hop information is not shown for installed routes in the IPv6 Content Addressable Memory (CAM). However, the same is shown in the Forwarding Information Base (FIB).

**Note:** If a route has a mask greater than 64, no output will be displayed, no output will be displayed for “show ipv6 cam stack-unit unit-number port-set {0-1} ipv6-address” but an equivalent /64 entry would be listed in the “show ipv6 cam stack-unit unit-number port-set {0-1}” output. Similarly, if there is more than one ECMP object with a destination route that has a mask greater than 64, if the first 64 bits in the destination routes of the ECMP objects are the same, only one route is installed in CAM even though multiple ECMP path entries exist.

**show ipv6 control-plane icmp**

Display the status of the icmp control-plane setting for the Error Rate limit setting.

**Syntax**

```
show ipv6 control-plane icmp
```

**Default**

100
Command Mode: EXEC

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

ipv6 flowlabel-zero Configure IPv6 address auto-configuration for the management interface.

show ipv6 fib stack-unit
View all FIB entries.

Syntax

show ipv6 fib stack-unit unit-number [summary | ipv6-address]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot-number</td>
<td>Enter the number of the stack unit. The range is from 0 to 11.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword summary to view a summary of entries in IPv6 cam.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>Enter the IPv6 address in the x:x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128.</td>
</tr>
</tbody>
</table>

Note: The :: notation specifies successive hexadecimal fields of zeros.

Command Mode: EXEC

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Host tables are not stored in CAM tables. Entries for camIndex will display as zero (0) on the show ipv6 fib stack-unit output for neighbor entries, such as ARP entries.

show ipv6 flowlabel-zero
Display the flow label zero setting.

Syntax

show ipv6 flowlabel-zero

Default

Disabled

Command Mode: EXEC

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

ipv6 nd dad attempts Configure system to set the flow label field in the packets to zero.

show ipv6 interface
Display the status of interfaces configured for IPv6.
### Syntax

```
show ipv6 interface [brief] [configured] [gigabitethernet slot | slot/port] [linecard slot-number] [loopback interface-number] [managementethernet slot | slot/port] [port-channel number] [tengigabitethernet slot | slot/port] [fortyGigE slot | slot/port] [vlan vlan-id]
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>(OPTIONAL) Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a Loopback interface, enter the keyword Loopback then a number from 0 to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For the Null interface, enter the keyword null then zero (0).</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE then the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For stacking, enter the keywords stack-unit then the stack-unit ID.</td>
</tr>
<tr>
<td></td>
<td>• For a tunnel interface, enter the keyword tunnel then the tunnel ID.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN interface, enter the keyword VLAN.</td>
</tr>
<tr>
<td></td>
<td>• For a port channel interface, enter the keywords port-channel.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>(OPTIONAL) View a summary of IPv6 interfaces.</td>
</tr>
<tr>
<td><code>configured</code></td>
<td>(OPTIONAL) View information on all IPv6 configured interfaces.</td>
</tr>
<tr>
<td><code>gigabitethernet</code></td>
<td>(OPTIONAL) View information for an IPv6 gigabitethernet interface.</td>
</tr>
<tr>
<td><code>linecard slot-number</code></td>
<td>(OPTIONAL) View information for a specific IPv6 linecard or stack-unit.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 11</td>
</tr>
<tr>
<td><code>managementethernet slot/port</code></td>
<td>(OPTIONAL) View information on an IPv6 Management port. Enter the slot number (0-1) and port number zero (0).</td>
</tr>
<tr>
<td><code>loopback</code></td>
<td>(OPTIONAL) View information for IPv6 loopback interfaces.</td>
</tr>
<tr>
<td><code>port-channel</code></td>
<td>(OPTIONAL) View information for IPv6 port channels.</td>
</tr>
<tr>
<td><code>tengigabitethernet</code></td>
<td>(OPTIONAL) View information for an IPv6 tengigabitethernet interface.</td>
</tr>
<tr>
<td><code>fortyGigE</code></td>
<td>(OPTIONAL) View information for an IPv6 fortygigabitethernet interface.</td>
</tr>
<tr>
<td><code>vlan</code></td>
<td>(OPTIONAL) View information for IPv6 VLANs.</td>
</tr>
</tbody>
</table>

### Defaults

`none`

### Command Modes

`EXEC`

### Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The Management port is enabled by default (no shutdown). If necessary, use the `ipv6 address` command to assign an IPv6 address to the Management port.

### Example

```
FTOS# show ipv6 interface
TenGigabitEthernet 0/5 is up, line protocol is up
```

---

**IPv6 Basics**
IPV6 is enabled
Link Local address: fe80::201:e8ff:fe8a:e8f7
Global Unicast address(es):
  2001::1, subnet is 2001::/64
  2002::1, subnet is 2002::/120
  2003::1, subnet is 2003::/120
  2004::1, subnet is 2004::/32
Global Anycast address(es):
Joined Group address(es):
  ff02::1
  ff02::2
  ff02::1:ff00:1
  ff02::1:ff8a:e8f7
ND MTU is 0
ICMP redirects are not sent
DAD is enabled, number of DAD attempts: 3
ND reachable time is 0 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 to 600 seconds
ND router advertisements live for 1800 seconds

Example
(show ipv6 interface managementethernet)

FTOS#
FTOS#show ipv6 int man 0/0
ManagementEthernet 0/0 is up, line protocol is up
IPV6 is enabled
Link Local address: fe80::201:e8ff:fe8a:e8f7
Global Unicast address(es):
  Actual address is 600::1, subnet is 600::/64
  Virtual-IP IPv6 address is not set
Global Anycast address(es):
Joined Group address(es):
  ff02::1
  ff02::1:ff00:1
  ff02::1:ff8a:e8f7
ND MTU is 1500
ICMP redirects are not sent
DAD is enabled, number of DAD attempts: 3
ND reachable time is 31000 milliseconds
ND base reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
ND hop limit is 64
FTOS#
FTOS#show ipv6 interface brief
GigabitEthernet 0/0              [up/up]
  fe80::201:e8ff:fe3a:143e
  10::1/64
...
ManagementEthernet 0/0          [up/up]
  fe80::201:e8ff:fe5d:b74c
  fdad:bbbb:cccc:1004::50/64
...
Vlan 3                          [up/up]
  fe80::201:e8ff:fe3a:19b7
    7::1/64

Example
(show ipv6 interface brief)

show ipv6 mld_host
Display the IPv6 MLD host counters.
show ipv6 mld_host

**Syntax**

show ipv6 mld_host

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

The following table describes the information in the output example:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid MLD Packets</td>
<td>The total number of packets received and sent from the last time the elapsed time was cleared.</td>
</tr>
<tr>
<td>Reports</td>
<td>The total number of reports (queries and unsolicited reports generated from joins or leaves) that have been received or sent.</td>
</tr>
<tr>
<td>Leaves</td>
<td>The number of Multicast leaves that have been sent.</td>
</tr>
<tr>
<td>MLDv1 queries</td>
<td>The number of MLDv1 queries that have been received.</td>
</tr>
<tr>
<td>MLDv2 queries</td>
<td>The number of MLDv2 queries that have been received.</td>
</tr>
<tr>
<td>Malformed Packets</td>
<td>The number of MLDv1 and MLDv2 packets that do not match the requirement for a valid MLD packet.</td>
</tr>
</tbody>
</table>

**Example**

MLD Host Traffic Counters
Elapsed time since counters cleared: 00:28:33:52

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid MLD Packets</td>
<td>97962</td>
</tr>
<tr>
<td>Reports</td>
<td>79962</td>
</tr>
<tr>
<td>Leaves</td>
<td>----</td>
</tr>
<tr>
<td>MLDv2 Queries</td>
<td>18000</td>
</tr>
<tr>
<td>MLDv1 Queries</td>
<td>0</td>
</tr>
<tr>
<td>Errors: Malformed Packets</td>
<td>4510</td>
</tr>
</tbody>
</table>

show ipv6 route

Display the IPv6 routes.

**Syntax**

show ipv6 route [ipv6-address prefix-length] [hostname] [all] [bgp as number] [connected] [isis tag] [list prefix-list name] [ospf process-id] [rip] [static] [summary]

**Parameter**

- **ipv6-address prefix-length** (OPTIONAL) Enter the IPv6 address in the x::x::x::x format followed by the prefix length in the /x format. Range: /0 to /128.
  The :: notation specifies successive hexadecimal fields of zeros.
- **hostname** (OPTIONAL) View information for this IPv6 routes with Host Name
- **all** (OPTIONAL) View information for all IPv6 routes
- **bgp** (OPTIONAL) View information for all IPv6 BGP routes
- **connected** (OPTIONAL) View only the directly connected IPv6 routes.
- **isis** (OPTIONAL) View information for all IPv6 IS-IS routes
- **list** (OPTIONAL) View the IPv6 prefix list
- **ospf** (OPTIONAL) View information for all IPv6 OSPF routes
- **rip** (OPTIONAL) View information for all IPv6 RIP routes
IPv6 Basics

<table>
<thead>
<tr>
<th>Defaults</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

**Example (S-Series)**

```
FTOS#show ipv6 route

Codes: C - connected, L - local, S - static, R - RIP, B - BGP, IN - internal BGP, EX - external BGP, O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default, Gateway of last resort is not set

Destination    Dist/Metric,      Gateway,   Last Change
-----------------------------------------------------------
C  2001::/64 [0/0] Direct, Gi 1/1, 00:28:49
C  2002::/120 [0/0] Direct, Gi 1/1, 00:28:49
C  2003::/120 [0/0] Direct, Gi 1/1, 00:28:49
C  2004::/32 [0/0] Direct, Gi 1/1, 00:28:49
L  fe80::/10 [0/0] Direct, Nu 0, 00:29:09
```

**Example (show ipv6 route summary)**

```
FTOS#show ipv6 route summary

Route Source      Active Routes Non-active Routes
connected          5            0
static             0            0
Total              5            0
Total 5 active route(s) using 952 bytes
```
Table 24-1. show ipv6 route Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(undefined)</td>
<td>Identifies the type of route:</td>
</tr>
<tr>
<td>L = Local</td>
<td></td>
</tr>
<tr>
<td>C = connected</td>
<td></td>
</tr>
<tr>
<td>S = static</td>
<td></td>
</tr>
<tr>
<td>R = RIP</td>
<td></td>
</tr>
<tr>
<td>B = BGP</td>
<td></td>
</tr>
<tr>
<td>IN = internal BGP</td>
<td></td>
</tr>
<tr>
<td>EX = external BGP</td>
<td></td>
</tr>
<tr>
<td>LO = Locally Originated</td>
<td></td>
</tr>
<tr>
<td>O = OSPF</td>
<td></td>
</tr>
<tr>
<td>IA = OSPF inter area</td>
<td></td>
</tr>
<tr>
<td>N1 = OSPF NSSA external type 1</td>
<td></td>
</tr>
<tr>
<td>N2 = OSPF NSSA external type 2</td>
<td></td>
</tr>
<tr>
<td>E1 = OSPF external type 1</td>
<td></td>
</tr>
<tr>
<td>E2 = OSPF external type 2</td>
<td></td>
</tr>
<tr>
<td>i = IS-IS</td>
<td></td>
</tr>
<tr>
<td>L1 = IS-IS level-1</td>
<td></td>
</tr>
<tr>
<td>L2 = IS-IS level-2</td>
<td></td>
</tr>
<tr>
<td>IA = IS-IS inter-area</td>
<td></td>
</tr>
<tr>
<td>* = candidate default</td>
<td></td>
</tr>
<tr>
<td>&gt;= = non-active route</td>
<td></td>
</tr>
<tr>
<td>+ = summary routes</td>
<td></td>
</tr>
</tbody>
</table>

| Destination            | Identifies the route’s destination IPv6 address.                           |
| Gateway                | Identifies whether the route is directly connected and on which interface the route is configured. |
| Dist/Metric            | Identifies if the route has a specified distance or metric.                |
| Last Change            | Identifies when the route was last changed or configured.                  |

trust ipv6-diffserv

Allows the dynamic classification of IPv6 DSCP.

**Syntax**

```
trust ipv6-diffserv
```

To remove the definition, use the `no trust ipv6-diffserv` command.

**Defaults**

none

**Command Modes**

CONFIGURATION-POLICY-MAP-IN

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When trust IPv6 diffserv is configured, matched bytes/packets counters are *not* incremented in the `show qos statistics` command.
Trust diffserv (IPv4) can co-exist with trust ipv6-diffserv in an Input Policy Map. Dynamic classification happens based on the mapping detailed in the following table.

**Table 24-2. IPv6 -Diffserv Mapping**

<table>
<thead>
<tr>
<th>IPv6 Service Class Field</th>
<th>Queue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>111XXXXX</td>
<td>7</td>
</tr>
<tr>
<td>110XXXXX</td>
<td>6</td>
</tr>
<tr>
<td>101XXXXX</td>
<td>5</td>
</tr>
<tr>
<td>100XXXXX</td>
<td>4</td>
</tr>
<tr>
<td>011XXXXX</td>
<td>3</td>
</tr>
<tr>
<td>010XXXXX</td>
<td>2</td>
</tr>
<tr>
<td>001XXXXX</td>
<td>1</td>
</tr>
<tr>
<td>000XXXXX</td>
<td>0</td>
</tr>
</tbody>
</table>
iSCSI Optimization

Overview

Internet Small Computer System Interface (iSCSI) optimization enables quality-of-service (QoS) treatment for iSCSI storage traffic on an MXL Switch.

The following FTOS commands are used to configure and verify the iSCSI Optimization feature:

- advertise dcbx-app-tlv
- iscsi aging time
- iscsi cos
- iscsi enable
- iscsi priority-bits
- iscsi profile-compellant
- iscsi target port
- show iscsi
- show iscsi sessions
- show iscsi sessions detailed
- show run iscsi

advertise dcbx-app-tlv

Configure DCBX to send iSCSI TLV advertisements.

Syntax

advertise dcbx-app-tlv iscsi

To disable DCBX iSCSI TLV advertisements, use the no advertise dcbx-app-tlv iscsi command.

Defaults

Enabled.

Command Mode

PROTOCOL LLDP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

You can configure iSCSI TLVs to be sent either globally or on a specified interface. The interface configuration takes priority over global configuration.
iscsi aging time

Set the aging time for iSCSI sessions.

Syntax

iscsi aging time time

To remove the iSCSI session aging time, use the no iscsi aging time command.

Parameters

| Parameter: time | Description: Enter the aging time for the iSCSI session. Valid values: 5 to 43,200 minutes. |

Defaults

10 minutes.

Command Mode

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

iscsi cos

Set the QoS policy that will be applied to the iSCSI flows.

Syntax

iscsi cos {enable | disable | dot1p vlan-priority-value [remark] | dscp dscp-value [remark]}

To disable the QoS policy, use the no iscsi cos dscp command.

Parameters

| Parameter: enable | Description: Enter the keyword enable to allow the application of preferential QoS treatment to iSCSI traffic so that the iSCSI packets are scheduled in the switch with a dot1p priority 4 regardless of the VLAN priority tag in the packet. Default: iSCSI packets are handled with dot1p priority 4 without remark. |

| Parameter: disable | Description: Enter the keyword disable to disable the application of preferential QoS treatment to iSCSI frames. |

| Parameter: dot1p vlan-priority-value | Description: Enter the dot1p value of the VLAN priority tag assigned to the incoming packets in an iSCSI session. The valid range is 0 to 7. Default: The dot1p value in ingress iSCSI frames is not changed and is used in iSCSI TLV advertisements if you did not enter the iscsi priority-bits command. |

| Parameter: dscp dscp-value | Description: Enter the DSCP value assigned to the incoming packets in an iSCSI session. The valid range is 0 to 63. Default: The DSCP value in ingress packets is not changed. |

| Parameter: remark | Description: Marks the incoming iSCSI packets with the configured dot1p or DSCP value when they egress to the switch. Default: The dot1p and DSCP values in egress packets are not changed. |

Defaults

See above.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
iscsi enable

Globally enable iSCSI optimization.

**Syntax**

```plaintext
iscsi enable
```

To disable iSCSI optimization, use the `no iscsi` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enter the keyword <code>enable</code> to enable the iSCSI optimization feature.</td>
</tr>
</tbody>
</table>

**Defaults**

Enabled.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When you enable the iSCSI feature using the `iscsi enable` command, flow control settings are set to `rx on tx off` on all interfaces.

iscsi priority-bits

Configure the priority bitmap to be advertised in iSCSI application TLVs.

**Syntax**

```plaintext
iscsi priority-bits
```

To remove the configured priority bitmap, use the `no iscsi priority-bits` command.

**Defaults**

4 (0x10 in the bitmap)

**Command Modes**

PROTOCOL LLDP (only on global, not on interface)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

iscsi profile-compellant

Configure the auto-detection of Compellent arrays on a port.

**Syntax**

```plaintext
iscsi profile-compellant
```

**Defaults**

Compellent disk arrays are not detected.

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
**iscsi target port**

Configure the iSCSI target ports and optionally, the IP addresses on which iSCSI communication will be monitored.

**Syntax**

```
iscsi target port tcp-port-1[tcp-port-2...tcp-port-16][address ip-address]
```

To remove the configured iSCSI target ports or IP addresses, use the `no iscsi target port` command.

**Parameters**

- `tcp-port-2...tcp-port-16` Enter the tcp-port number of the iSCSI target ports. The `tcp-port-n` is the TCP port number or a list of TCP port numbers on which the iSCSI target listens to requests. Separate port numbers with a comma. Default: 860, 3260.
- `ip-address` (OPTIONAL) Enter the ip-address that the iSCSI will monitor. The ip-address specifies the IP address of the iSCSI target.

**Defaults**

860, 3260.

**Command Modes**

CONFIGURATION

**Command History**

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

**Usage Information**

You can configure up to 16 target TCP ports on the switch in one command or multiple commands.

When you use the `no iscsi target port` command, and the TCP port to be deleted is one bound to a specific IP address, the IP address value must be included in the command.

**show iscsi**

Display the currently configured iSCSI settings.

**Syntax**

```
show iscsi
```

**Command Mode**

EXEC

EXEC Privilege

**Command History**

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |
**Example**

**Figure 25-1. show iscsi Command Example**

```
FTOS# show iscsi

iSCSI is enabled
iSCSI COS : dot1p is 4 no-remark
Session aging time: 10
Maximum number of connections is 256
------------------------------------------------
iSCSI Targets and TCP Ports:
------------------------------------------------
TCP Port    Target IP Address
3260
860
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show iscsi</code></td>
<td>Display the currently configured iSCSI settings.</td>
</tr>
<tr>
<td><code>show iscsi sessions</code></td>
<td>Display information on active iSCSI sessions on the switch.</td>
</tr>
<tr>
<td><code>show iscsi sessions detailed</code></td>
<td>Display detailed information on active iSCSI sessions on the switch.</td>
</tr>
<tr>
<td><code>show run iscsi</code></td>
<td>show run iscsi</td>
</tr>
</tbody>
</table>

**show iscsi**

Display information on active iSCSI sessions on the switch.

**Syntax**

`show iscsi sessions`

**Command Mode**

EXEC

**EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 25-2. show iscsi sessions Command Example**

```
FTOS# show iscsi sessions
Session 0:
-----------------------------------------------------------------------------------------
Target: iqn.2001-05.com.equallogic:0-8a0906-0e70c2002-10a0018426a48c94-iom010
Initiator: iqn.1991-05.com.microsoft:win-x9l8v27yajg
ISID: 400001370000
-----------------------------------------------------------------------------------------
Session 1:
-----------------------------------------------------------------------------------------
Target: iqn.2001-05.com.equallogic:0-8a0906-0f60c2002-0360018428d48c94-iom011
Initiator: iqn.1991-05.com.microsoft:win-x918v27ysjg
ISID: 400001370000.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show iscsi</code></td>
<td>Display the currently configured iSCSI settings.</td>
</tr>
<tr>
<td><code>show iscsi sessions</code></td>
<td>Display information on active iSCSI sessions on the switch.</td>
</tr>
<tr>
<td><code>show iscsi sessions detailed</code></td>
<td>Display detailed information on active iSCSI sessions on the switch.</td>
</tr>
<tr>
<td><code>show run iscsi</code></td>
<td>show run iscsi</td>
</tr>
</tbody>
</table>
show iscsi sessions detailed

Display detailed information on active iSCSI sessions on the switch.

**Syntax**

```plaintext
show iscsi sessions detailed [session isid]
```

**Parameters**

- `isid` Enter the session’s iSCSI ID to display detailed information on specified iSCSI session.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

**Example**

Figure 25-3. show iscsi sessions detailed Command Example

```
FTOS# show iscsi sessions detailed
Session 0 :
------------------------------------------------------------------------------------------------------------------
Up Time:00:00:01:28(DD:HH:MM:SS)
Time for aging out:00:00:09:34(DD:HH:MM:SS)
ISID:806978696102
Initiator        Initiator      Target         Target     Connection
IP Address       TCP Port       IP Address     TCPPort    ID
10.10.0.44          33345      10.10.0.101     3260       0

Session 1 :
------------------------------------------------------------------------------------------------------------------
Up Time:00:00:01:22(DD:HH:MM:SS)
Time for aging out:00:00:09:31(DD:HH:MM:SS)
ISID:806978696102
Initiator        Initiator       Target        Target     Connection
IP Address       TCP Port        IP Address    TCPPort    ID
10.10.0.53           33432      10.10.0.101    3260       0
```

**Related Commands**

- `show iscsi` Display the currently configured iSCSI settings.
- `show iscsi sessions` Display information on active iSCSI sessions on the switch.
- `show run iscsi` show run iscsi
show run iscsi

Display all globally-configured non-default iSCSI settings in the current FTOS session.

Syntax
show run iscsi

Command Mode
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show iscsi</td>
<td>Display the currently configured iSCSI settings.</td>
</tr>
<tr>
<td>show iscsi sessions</td>
<td>Display information on active iSCSI sessions on the switch.</td>
</tr>
<tr>
<td>show iscsi sessions detailed</td>
<td>Display detailed information on active iSCSI sessions on the switch.</td>
</tr>
</tbody>
</table>
Intermediate System to Intermediate System (IS-IS)

Overview

Intermediate System to Intermediate System Protocol (IS-IS) for IPv4 and IPv6 is supported on the MXL 10/40GbE Switch IO Module.

IS-IS is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an intermediate system. Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

IS-IS protocol standards are listed in the Standard Compliance chapter in the FTOS Configuration Guide.

Note: The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

Commands

The following are the FTOS commands to enable IS-IS.

- adjacency-check
- advertise
- area-password
- clear config
- clear isis
- clns host
- debug isis
- debug isis adj-packets
- debug isis local-updates
- debug isis snp-packets
- debug isis spf-triggers
• debug isis update-packets
• default-information originate
• description
• distance
• distribute-list in
• distribute-list out
• distribute-list redistributed-override
• domain-password
• graceful-restart ietf
• graceful-restart interval
• graceful-restart t1
• graceful-restart t2
• graceful-restart t3
• graceful-restart restart-wait
• hello padding
• hostname dynamic
• ignore-lsp-errors
• ip router isis
• ipv6 router isis
• isis circuit-type
• isis csnp-interval
• isis hello-interval
• isis hello-multiplier
• isis hello padding
• isis ipv6 metric
• isis metric
• isis network point-to-point
• isis password
• isis priority
• is-type
• log-adjacency-changes
• lsp-gen-interval
• lsp-mtu
• lsp-refresh-interval
• max-area-addresses
• max-lsp-lifetime
• maximum-paths
• metric-style
• multi-topology
• net
• passive-interface
• redistribute
• redistribute bgp
• redistribute ospf
• router isis
• set-overload-bit
adjacency-check

Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

Syntax adjacency-check

To disable adjacency check, use the no adjacency-check command.

Defaults Enabled

Command Modes
- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Use this command to perform protocol-support consistency checks on hello packets. The adjacency-check is enabled by default.

advertise

Leak routes between levels (distribute IP prefixes between Level 1 and Level 2 and vice versa).

Syntax advertise {level1-into-level2 | level2-into-level1} prefix-list-name

To return to the default, use the no advertise {level1-into-level2 | level2-into-level1} [prefix-list-name] command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level1-into-level2</td>
<td>Enter the keyword level1-into-level2 to advertise Level 1 routes into Level 2 LSPs. This is the default.</td>
</tr>
<tr>
<td>level2-into-level1</td>
<td>Enter the keyword level2-into-level1 to advertise Level 2 inter-area routes into Level 1 LSPs. Described in RFC 2966.</td>
</tr>
<tr>
<td>prefix-list-name</td>
<td>Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.</td>
</tr>
</tbody>
</table>
area-password

Configure a Hash Message Authentication Code (HMAC) authentication password for an area.

Syntax area-password [hmac-md5 | encryption-type] password

To delete a password, enter no area-password.

Parameters

- **hmac-md5** (OPTIONAL) Enter the keyword hmac-md5 to encrypt the password.
- **encryption-type** (OPTIONAL) Enter 7 to encrypt the password using DES.
- **password** Enter a 1—16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text which only provides limited security.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Use the area-password command on routers within an area to prevent the link state database from receiving incorrect routing information from unauthorized routers.

The password configured is injected into Level 1 LSPs, CSNPs, and PSNPs.

Related Commands

- **domain-password** Allows you to set the authentication password for a routing domain.
- **isis password** Allows you to configure an authentication password for an interface.
clear config
Clear IS-IS configurations that display under the router isis heading of the show running-config command output.

Syntax clear config

Command Modes
ROUTER ISIS

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

Related Commands
copy Use this command to save the current configuration to another location.

clear isis
Restart the IS-IS process. All IS-IS data is cleared.

Syntax clear isis [tag] {* | database | traffic}

Parameters
  tag (Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
  
  * Enter the keyword * to clear all IS-IS information and restarts the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation will be done.
  
  database Clears IS-IS LSP database information.
  
  traffic Clears IS-IS counters.

Command Modes EXEC Privilege

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

clns host
Define a name-to-network service mapping point (NSAP) mapping that can then be used with commands that require NSAPs and system IDs.

Syntax clns host name nsap

Parameters
  name Enter an alphanumeric string to identify the name-to-NSAP mapping.
  
  nsap Enter a specific NSAP address that will be associated with the name parameter.

Defaults Not configured.

Command Modes ROUTER ISIS
debug isis

Enable debugging for all IS-IS operations.

Syntax
debug isis

to disable debugging of IS-IS, enter no debug isis.

Command Modes
EXEC Privilege

Command History
Version 9.2(0.0) Introduced on the Mox 10/40GbE Switch IO Module.

Usage Information
Entering debug isis enables all debugging parameters.

Use this command to display all debugging information in one output. To turn off debugging, you normally enter separate no forms of each command. Enter the no debug isis command to disable all debug messages for IS-IS at once.

debug isis adj-packets

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

Syntax
debug isis adj-packets [interface]

To turn off debugging, use the no debug isis adj-packets [interface] command.

Parameters

interface (OPTIONAL) Identifies the interface type slot/port as one of the following:
- For a Port Channel interface, enter the keyword port-channel followed by a number:
  Range: 1-128
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
- For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

Command Modes
EXEC Privilege

Command History
Version 9.2(0.0) Introduced on the Mox 10/40GbE Switch IO Module.
debug isis local-updates

Enables debugging on a specific interface and provides diagnostic information to debug IS-IS local update packets.

**Syntax**

```
debug isis local-updates [interface]
```

To turn off debugging, enter the `no debug isis local-updates [interface]` command.

**Parameters**

```
interface (OPTIONAL) Identifies the interface type slot/port as one of the following:
  • For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
```

**Command Modes**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

debug isis snp-packets

Enable debugging on a specific interface and provides diagnostic information to debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets.

**Syntax**

```
debug isis snp-packets [interface]
```

To turn off debugging, enter the `no debug isis snp-packets [interface]` command.

**Parameters**

```
interface (OPTIONAL) Identifies the interface type slot/port as one of the following:
  • For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
```

**Command Modes**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

ddebug isis spf-triggers

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

**Syntax**

```
debug isis spf-triggers
```

**Parameters**

```
interface (OPTIONAL) Identifies the interface type slot/port as one of the following:
  • For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
```

**Command Modes**

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
To turn off debugging, enter `no debug isis spf-triggers`.

### debug isis update-packets

Enable debugging on Link State PDUs (LSPs) that are detected by a router.

**Syntax**

```
dependent isis update-packets [interface]
```

To turn off debugging, enter the `no debug isis update-packets [interface]` command.

**Parameters**

- **interface** *(OPTIONAL)* Identifies the interface type slot/port as one of the following:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

### default-information originate

Generate a default route into an IS-IS routing domain and controls the distribution of default information.

**Syntax**

```
default-information originate [always] [metric metric] [route-map map-name]
```

To disable the generation of a default route into the specified IS-IS routing domain, enter the `no default-information originate [always] [metric metric] [route-map map-name]` command.

**Parameters**

- **always** *(OPTIONAL)* Enter the keyword `always` to have the default route always advertised.
- **metric metric** *(OPTIONAL)* Enter the keyword `metric` followed by a number to assign to the route.
  - Range: 0 to 16777215
- **route-map map-name** *(OPTIONAL)* A default route will be generated by the routing process if the route map is satisfied.

**Defaults**

Not configured.

**Command Modes**

`ROUTER ISIS (for IPv4)`
When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route is advertised depends on how on the configuration of the metric-style command. If the metric-style is set for narrow mode and the metric value in the default-information originate command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the metric-style is set for wide mode, their the metric value in the default-information originate command is advertised.

### description

Enter a description of the IS-IS routing protocol

**Syntax**

```plaintext
description {description}
```

To remove the description, use the `no description {description}` command.

**Parameters**

- `description` Enter a description to identify the IS-IS protocol (80 characters maximum).

**Defaults**

No default behavior or values

**Command Modes**

ROUTER ISIS

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `router isis` Enter ROUTER mode on the switch.

### distance

Define the administrative distance for learned routes.

**Syntax**

```plaintext
distance weight [ip-address mask [prefix-list]]
```

To return to the default values, enter the `no distance weight` command.
**Parameters**

| **weight** | The administrative distance value indicates the reliability of a routing information source.  
Range: 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.)  
Default: 115 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address mask</strong></td>
<td>(OPTIONAL) Enter an IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.</td>
</tr>
<tr>
<td><strong>prefix-list</strong></td>
<td>(OPTIONAL) Enter the name of a prefix list name.</td>
</tr>
</tbody>
</table>

**Defaults**

- **weight** = 115

**Command Modes**

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

---

**distribute-list in**

Filter network prefixes received in updates.

**Syntax**

```
distribute-list prefix-list-name in [interface]
```

To return to the default values, enter the `no distribute-list prefix-list-name in [interface]` command.

**Parameters**

- **prefix-list-name** (OPTIONAL) Specify the prefix list to filter prefixes in routing updates.
- **interface** (OPTIONAL) Identifies the interface type slot/port as one of the following:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:  
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

- ROUTER ISIS (for IPv6)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>distribute-list out</td>
<td>Suppress network prefixes from being advertised in outbound updates.</td>
</tr>
<tr>
<td>redistribute</td>
<td>Redistributes routes from one routing domain to another routing domain.</td>
</tr>
</tbody>
</table>

**distribute-list out**

Suppress network prefixes from being advertised in outbound updates.

**Syntax**

```
distribute-list prefix-list-name out [connected | bgp as number | ospf process-id | rip | static]
```

To return to the default values, enter the `no distribute-list prefix-list-name out [bgp as number connected | ospf process-id | rip | static]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-list-name</td>
<td>Specify the prefix list to filter prefixes in routing updates.</td>
</tr>
<tr>
<td>connected</td>
<td>(OPTIONAL) Enter the keyword <code>connected</code> for directly connected routing process.</td>
</tr>
<tr>
<td>ospf process-id</td>
<td>(OPTIONAL) Enter the keyword <code>ospf</code> followed by the OSPF process-ID number. Range: 1 to 65535</td>
</tr>
<tr>
<td>bgp as number</td>
<td>(OPTIONAL) Enter the BGP followed by the AS Number. Range: 1 to 65535</td>
</tr>
<tr>
<td>rip</td>
<td>(OPTIONAL) Enter the keyword <code>rip</code> for RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td>(OPTIONAL) Enter the keyword <code>static</code> for user-configured routing process.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Command History**

- Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

You can assign a name to a routing process so a prefix list will be applied to only the routes derived from the specified routing process.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>distribute-list in</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>redistribute</td>
<td>Redistributes routes from one routing domain to another routing domain.</td>
</tr>
</tbody>
</table>

**distribute-list redistributed-override**

Suppress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.

**Syntax**

```
distribute-list redistributed-override in
```

To return to the default, use the `no distribute-list redistributed-override in` command.
domain-password

Set the authentication password for a routing domain.

Syntax

domain-password [hmac-md5 | encryption-type] password

To disable the password, enter no domain-password.

Parameters

- **hmac-md5** (OPTIONAL) Enter the keyword hmac-md5 to encrypt the password using MD5.
- **encryption-type** (OPTIONAL) Enter 7 to encrypt the password using DES.
- **password** Enter an alphanumeric string up to 16 characters long. If you do not specify an encryption type or hmac-md5 keywords, the password is processed as plain text which provides limited security.

Defaults

No default password.

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands

- area-password Configure an IS-IS area authentication password.
- isis password Configure the authentication password for an interface.

graceful-restart ietf

Enable Graceful Restart on an IS-IS router.

Syntax

graceful-restart ietf

To return to the default, use the no graceful-restart ietf command.

Parameters

- **ietf** Enter ietf to enable Graceful Restart on the IS-IS router.
Defaults
Default is Graceful Restart disabled.

Command Modes
ROUTER ISIS

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
A Restart TLV included in every Graceful Restart enabled router’s HELLO PDUs. This enables the (re)starting as well as the existing ISIS peers to detect the GR capability of the routers on the connected network. A flag in the Restart TLV contains Restart Request (RR), Restart Acknowledge (RA) and Suppress Adjacency Advertisement (SA) bit flags.

The ISIS Graceful Restart enabled router can co-exist in mixed topologies where some routers are Graceful Restart enabled and others are not. For neighbors that are not Graceful Restart enabled, the restarting router brings up the adjacency per the usual methods.

graceful-restart interval
Set the Graceful Restart grace period, the time during which all Graceful Restart attempts are prevented.

Syntax
```
graceful-restart interval minutes
```

To return to the default, use the `no graceful-restart interval` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| minutes   | Range: 1-20 minutes  
  Default: 5 minutes |

Defaults
5 minutes

Command Modes
ROUTER ISIS

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

graceful-restart t1
Set the Graceful Restart wait time before unacknowledged restart requests are generated. This is the interval before the system sends a Restart Request (an IIH with RR bit set in Restart TLV) until the CSNP is received from the helping router.

Syntax
```
graceful-restart t1 [interval seconds | retry-times value]
```

To return to the default, use the `no graceful-restart t1` command.
Parameters

| **interval** | Enter the keyword *interval* to set the wait time.  
| Range: 5-120 seconds  
| Default: 5 seconds |

| **retry-times** | Enter the keyword *retry-times* to set the number of times the request interval is extended until a CSNP is received from the helping router.  
| Range: 1-10 attempts  
| Default: 1 |

Defaults

above

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**graceful-restart t2**

Configure the wait time for the Graceful Restart timer T2 that a restarting router uses as the wait time for each database to synchronize.

**Syntax**

```
graceful-restart t2 {level-1 | level-2} seconds
```

To return to the default, use the `no graceful-restart t2` command.

**Parameters**

| **level-1, level-2** | Enter the keyword *level-1* or *level-2* to identify the database instance type to which the wait interval applies. |
| **seconds** | Range: 5-120 seconds  
| Default: 30 seconds |

Defaults

30 seconds

Command Modes

ROUTER ISIS

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**graceful-restart t3**

Configure the overall wait time before Graceful Restart is completed.

**Syntax**

```
graceful-restart t3 {adjacency | manual} seconds
```

To return to the default, use the `no graceful-restart t3` command.
The running router sets remaining time value to the current adjacency hold time. This can be overridden by implementing this command.

Override the default restart-wait time by entering the `no graceful-restart restart-wait` command. When restart-wait is disabled, the current adjacency hold time is used.

Be sure to set the t3 timer to adjacency on the restarting router when implementing this command. The restarting router gets the remaining time value from its peer and adjusts its T3 value accordingly only when you have configured `graceful-restart t3 adjacency`.

**Related Commands**

- `graceful-restart restart-wait`: Enable the Graceful Restart maximum wait time before a restarting peer comes up.

---

### graceful-restart restart-wait

Enable the Graceful Restart maximum wait time before a restarting peer comes up.

Be sure to set the t3 timer to adjacency on the restarting router when implementing this command.

**Syntax**

```
graceful-restart restart-wait seconds
```

To return to the default, use the `no graceful-restart restart-wait` command.

**Parameters**

- `seconds`: Range: 5-300 seconds  
  Default: 30 seconds

**Defaults**

30 seconds

**Command Modes**

ROUTER ISIS

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `graceful-restart t3`: Configure the overall wait time before Graceful Restart is completed.
hello padding

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

Syntax

```
hello padding [multi-point | point-to-point]
```

To return to default, use `no hello padding [multi-point | point-to-point].`

Parameters

- `multi-point` (OPTIONAL) Enter the keyword `multi-point` to pad only LAN hello PDUs.
- `point-to-point` (OPTIONAL) Enter the keyword `point-to-point` to pad only point-to-point PDUs.

Defaults

Both LAN and point-to-point hello PDUs are padded.

Command Modes

- ROUTER ISIS

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands

- `isis hello padding` Turn ON or OFF hello padding on an interface basis.

hostname dynamic

Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

Syntax

```
hostname dynamic
```

To disable this command, enter `no hostname dynamic`.

Defaults

Enabled.

Command Modes

- ROUTER ISIS

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Use this command to build name-to-systemID mapping tables through the protocol. All `show` commands that display systems also display the hostname.

Related Commands

- `chns host` Define a name-to-NSAP mapping.
ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

Syntax

```
ignore-lsp-errors
```

To return to the default values, enter `no ignore-lsp-errors`.

Defaults

In IS-IS, the default deletes LSPs with internal checksum errors (no ignore-lsp-errors).

Command Modes

```
ROUTER ISIS
```

Usage Information

IS-IS normally purges LSPs with an incorrect data link checksum, causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This could cause disruption to your system operation.

ip router isis

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

Syntax

```
ip router isis [tag]
```

To disable IS-IS on an interface, enter the `no ip router isis [tag]` command.

Parameters

- `tag` (OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.

Defaults

No processes are configured.

Command Modes

```
INTERFACE
```

Usage Information

You must use the `net` command to assign a network entity title to enable IS-IS.

Related Commands

- `net` Configures an IS-IS network entity title (NET) for the routing process.
- `router isis` Enables the IS-IS routing protocol.

ipv6 router isis

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

Syntax

```
ipv6 router isis [tag]
```

To disable IS-IS routing, enter `no router isis [tag]`.
### isis circuit-type

Configure the adjacency type on interfaces.

**Syntax**

```plaintext
isis circuit-type \{level-1 | level-1-2 | level-2-only\}
```

To return to the default values, enter `no isis circuit-type`.

**Parameters**

- **level-1**: You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.
- **level-1-2**: You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, then a Level 2 adjacency is established. This is the default.
- **level-2-only**: You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

**Defaults**

level-1-2

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system should be configured as a Level 1-only, Level 1-2, or Level 2-only system.
Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

**isis csnp-interval**

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

**Syntax**

```plaintext
isis csnp-interval seconds [level-1 | level-2]
```

To return to the default values, enter the `no isis csnp-interval [seconds] [level-1 | level-2]` command.

**Parameters**

- `seconds` Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system.
  - Range: 0 to 65535
  - Default: 10
- `level-1` (OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
- `level-2` (OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

**Defaults**

`seconds = 10`; `level-1` (if not otherwise specified)

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

Level 1 and Level 2 CSNP intervals can be configured independently.

**isis hello-interval**

Specify the length of time between hello packets sent.

**Syntax**

```plaintext
isis hello-interval seconds [level-1 | level-2]
```

To return to the default values, enter the `no isis hello-interval [seconds] [level-1 | level-2]` command.

**Parameters**

- `seconds` Allows you to set the length of time between hello packet transmissions.
  - Range: 1 to 65535
  - Default: 10
- `level-1` (OPTIONAL) Select this value to configure the hello interval for Level 1.
  - This is the default.
- `level-2` (OPTIONAL) Select this value to configure the hello interval for Level 2.
Hello packets are held for a length of three times the value of the hello interval. Use a high hello interval seconds to conserve bandwidth and CPU usage. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).

**isis hello-multiplier**

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

**Syntax**

```plaintext
isis hello-multiplier multiplier [level-1 | level-2]
```

To return to the default values, enter `no isis hello-multiplier [multiplier] [level-1 | level-2].`

**Parameters**

- `multiplier` Specifies an integer that sets the multiplier for hello holding time.
  - Never configure a hello-multiplier lower then the default (3).
  - Range: 3 to 1000
  - Default: 3

- `level-1` (OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies.
  - This is the default.

- `level-2` (OPTIONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

**Defaults**

`multiplier =3; level-1` (if not otherwise specified)

**Command Modes**

INTERFACE

**Usage Information**

The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

**Related Commands**

- `isis hello-interval` Specify the length of time between hello packets.

**isis hello padding**

Turn ON or OFF padding of hello PDUs from the interface mode.

**Syntax**

```plaintext
isis hello padding
```

**Defaults**

`off`

**Command Modes**

INTERFACE

**Usage Information**

The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.
To return to the default, use the `no isis hello padding`.

**Defaults**

Padding of hello PDUs is enabled (ON).

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Hello PDUs are “padded” only when both the global and interface padding options are ON. Turning either one OFF will disable padding for the corresponding interface(s).

**Related Commands**

- `hello padding` Turn ON or OFF padding for LAN and point-to-point hello PDUs.

### isis ipv6 metric

Assign metric to an interface for use with IPv6 information.

**Syntax**

`isis ipv6 metric default-metric [level-1 | level-2]`

To return to the default values, enter `no ipv6 isis metric [default-metric] [level-1 | level-2]` command.

**Parameters**

- `default-metric` Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations.
  - You can configure this metric for Level 1 or Level 2 routing.
  - Range: 0 to 16777215
  - Default: 10

  - `level-1` (OPTIONAL) Enter `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing.
    - This is the default.

  - `level-2` (OPTIONAL) Enter `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

**Defaults**

`default-metric` = 10; `level-1` (if not otherwise specified)

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

### isis metric

Assign a metric to an interface.

**Syntax**

`isis metric default-metric [level-1 | level-2]`

**Parameters**

- `default-metric` Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations.
  - You can configure this metric for Level 1 or Level 2 routing.
  - Range: 0 to 16777215
  - Default: 10

  - `level-1` (OPTIONAL) Enter `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing.
    - This is the default.

  - `level-2` (OPTIONAL) Enter `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

**Defaults**

`default-metric` = 10; `level-1` (if not otherwise specified)

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.
To return to the default values, enter `no isis metric [default-metric] [level-1 | level-2].`

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-metric</td>
<td>Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. Range: 0 to 63 for narrow and transition metric styles; 0 to 16777215 for wide metric styles. Default: 10</td>
</tr>
<tr>
<td>level-1</td>
<td>(OPTIONAL) Enter <code>level-1</code> to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This is the default.</td>
</tr>
<tr>
<td>level-2</td>
<td>(OPTIONAL) Enter <code>level-2</code> to configure the SPF calculation for Level 2 (inter-area) routing.</td>
</tr>
</tbody>
</table>

**Defaults**

`default-metric = 10; level-1` (if not otherwise specified)

**Command Modes**

`INTERFACE`

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Dell Force10 recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

### isis network point-to-point

Enable the software to treat a broadcast interface as a point-to-point interface.

**Syntax**

`isis network point-to-point`

To disable the feature, enter `no isis network point-to-point.`

**Defaults**

Not enabled.

**Command Modes**

`INTERFACE`

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### isis password

Configure an authentication password for an interface.

**Syntax**

`isis password [hmac-md5] password [level-1 | level-2]`

To delete a password, enter the `no isis password [password] [level-1 | level-2]` command.

**Parameters**

- `encryption-type` (OPTIONAL) Enter 7 to encrypt the password using DES.
- `hmac-md5` (OPTIONAL) Enter the keyword `hmac-md5` to encrypt the password using MD5.
Defaults

No default password. **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

Usage Information

To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the **level-1** and **level-2** keywords.

The **no** form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords **level-1** or **level-2**.

This password provides limited security as it is processed as plain text.

### isis priority

Set priority of the designated router you select.

**Syntax**

```plaintext
isis priority value [level-1 | level-2]
```

To return to the default values, enter the **no isis priority [value] [level-1 | level-2]** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>value</strong></td>
<td>This value sets the router priority. The higher the value, the higher the priority. Range: 0 to 127 Default: 64</td>
</tr>
<tr>
<td><strong>level-1</strong></td>
<td>(OPTIONAL) Specify the priority for Level 1. This is the default.</td>
</tr>
<tr>
<td><strong>level-2</strong></td>
<td>(OPTIONAL) Specify the priority for Level 2.</td>
</tr>
</tbody>
</table>

**Defaults**

```plaintext
value = 64; level-1 (if not otherwise specified)
```

Command Modes

INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

Usage Information

You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN will be the designated router. Priorities are advertised within hellos. The router with the highest priority will become the designated intermediate system (DIS).
Routers with a priority of 0 cannot be a designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address will become DIS even though its priority is 0.

**is-type**

Configure IS-IS operating level for a router.

Syntax

```
is-type {level-1 | level-1-2 | level-2-only}
```

Parameters

- **level-1**: Allows a router to act as a Level 1 router.
- **level-1-2**: Allows a router to act as both a Level 1 and Level 2 router.
  This is the default.
- **level-2-only**: Allows a router to act as a Level 2 router.

Defaults

```
level-1-2
```

Command Modes

```
ROUTER ISIS
```

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. The IS type can be configured as Level 1.

**log-adjacency-changes**

Generate a log messages for adjacency state changes.

Syntax

```
log-adjacency-changes
```

To disable this function, enter `no log-adjacency-changes`.

Defaults

```
Adjacency changes are not logged.
```

Command Modes

```
ROUTER ISIS
```

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command enables you to monitor adjacency state changes, which is useful when you monitor large networks. Messages are logged in the system error message facility.
**lsp-gen-interval**

Set the minimum interval between successive generations of link-state packets (LSPs).

**Syntax**

```
lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the `no lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

**Parameters**

- **level-1**
  (OPTIONAL) Enter the keyword `level-1` to apply the configuration to generation of Level-1 LSPs.

- **level-2**
  (OPTIONAL) Enter the keyword `level-2` to apply the configuration to generation of Level-2 LSPs.

- **interval seconds**
  Enter the maximum number of seconds between LSP generations.
  Range: 0 to 120 seconds
  Default: 5 seconds

- **initial_wait_interval seconds**
  (OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation.
  Range: 0 to 120 seconds
  Default: 1 second

- **second_wait_interval seconds**
  (OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation.
  Range: 0 to 120 seconds
  Default: 5 seconds

**Defaults**

Defaults as above

**Command Modes**

ROUTER ISIS

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (`interval seconds`). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

**lsp-mtu**

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs generated by this router.

**Syntax**

```
lsp-mtu size
```

**Usage Information**

This command only limits the size of LSPs generated by this router.
To return to the default values, enter **no lsp-mtu**.

<table>
<thead>
<tr>
<th>Parameters</th>
<th></th>
</tr>
</thead>
</table>
| **size** | The maximum LSP size, in bytes.  
Range: 128 to 1497 for non-jumbo mode; 128 to 9195 for jumbo mode.  
Default: 1497 |

<table>
<thead>
<tr>
<th>Defaults</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1497 bytes</td>
<td></td>
</tr>
</tbody>
</table>

| Command Modes | ROUTER ISIS |

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

| Usage Information | The link MTU and the LSP MTU size must be the same.  
Since each device can generate a maximum of 255 LSPs, consider carefully whether the **lsp-mtu** command should be configured. |

## lsp-refresh-interval

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their **max-lsp-lifetime** reaches zero and then LSPs will be purged.

**Syntax**

```
set refresh-interval seconds
```

To restore the default refresh interval, enter **no lsp-refresh-interval**.

<table>
<thead>
<tr>
<th>Parameters</th>
<th></th>
</tr>
</thead>
</table>
| **seconds** | The LSP refresh interval, in seconds. This value has to be less than the seconds value specified with the **max-lsp-lifetime** command.  
Range: 1 to 65535 seconds.  
Default: 900 |

<table>
<thead>
<tr>
<th>Defaults</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>900 seconds</td>
<td></td>
</tr>
</tbody>
</table>

| Command Modes | ROUTER ISIS |

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

| Usage Information | The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.  
The refresh interval must be less than the LSP lifetime specified with the **max-lsp-lifetime** command.  
A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization caused by the flooding of refreshed packets. |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>max-lsp-lifetime</strong></td>
<td>Sets the maximum interval that LSPs persist without being refreshed</td>
</tr>
</tbody>
</table>
max-area-addresses
Configure manual area addresses.

Syntax
max-area-addresses number

To return to the default values, enter no max-area-addresses.

Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Set the maximum number of manual area addresses. Range: 3 to 6. Default: 3</td>
</tr>
</tbody>
</table>

Defaults
3 addresses

Command Modes
ROUTER ISIS

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
Use this command to configure the number of area addresses on router. This value should be consistent with routers in the same area, or else, the router will form only Level 2 adjacencies. The value should be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime
Set the maximum time that link-state packets (LSPs) exist without being refreshed.

Syntax
max-lsp-lifetime seconds

To restore the default time, enter no max-lsp-lifetime.

Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>The maximum lifetime of LSP in seconds. This value must be greater than the lsp-refresh-interval. The higher the value the longer the LSPs are kept. Range: 1 to 65535 Default: 1200</td>
</tr>
</tbody>
</table>

Defaults
1200 seconds

Command Modes
ROUTER ISIS

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval.

The seconds parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.

Related Commands
lsp-refresh-interval Use this command to set the link-state packet (LSP) refresh interval.
**maximum-paths**

Allows you to configure the maximum number of equal cost paths allowed in a routing table.

**Syntax**

```
maximum-paths number
```

To return to the default values, enter `no maximum-paths`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. Range: 1 to 16. Default: 4</td>
</tr>
</tbody>
</table>

**Defaults**

4

**Command Mode**

ROUTER ISIS *(for IPv4)*

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 *(for IPv6)*

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**metric-style**

Configure a router to generate and accept old-style, new-style, or both styles of type, length, and values (TLV).

**Syntax**

```
metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]
```

To return to the default values, enter the `no metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>narrow</code></td>
<td>Allows you to configure the system to generate and accept old-style TLVs. Metric range: 0 to 63</td>
</tr>
<tr>
<td><code>transition</code></td>
<td>Allows you to configure the system to generate both old-style and new-style TLVs. Metric range: 0 to 63</td>
</tr>
<tr>
<td><code>wide</code></td>
<td>Allows you to configure the system to generate and accept only new-style TLVs. Metric range: 0 to 16777215</td>
</tr>
<tr>
<td><code>level-1</code></td>
<td>Enables the metric style on Level 1.</td>
</tr>
<tr>
<td><code>level-2</code></td>
<td>Enables the metric style on Level 2.</td>
</tr>
</tbody>
</table>

**Defaults**

`narrow`; if no Level is specified, Level-1 and Level-2 are configured.

**Command Modes**

ROUTER ISIS

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If you enter the **metric-style wide** command, the FTOS generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs.
The new-style TLVs have wider metric fields than old-style TLVs.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis metric</td>
</tr>
</tbody>
</table>

**multi-topology**

Enables Multi-Topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

**Syntax**

```
multi-topology [transition]
```

To return to a single topology configuration, enter `no multi-topology [transition].`

**Parameters**

- `transition`  

**Defaults**

- Disabled

**Command Mode**

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**net**

Use this mandatory command to configure an IS-IS network entity title (NET) for a routing process. If a NET is not configured, the IS-IS process will not start.

**Syntax**

```
net network-entity-title
```

To remove a net, enter `no net network-entity-title`.

**Parameters**

- `network-entity-title` Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.

**Defaults**

- Not configured.

**Command Modes**

- ROUTER ISIS

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**passive-interface**

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

**Syntax**

```
passive-interface interface
```

Intermediate System to Intermediate System (IS-IS) | 535
To delete a passive interface configuration, enter the `no passive-interface interface` command.

**Parameters**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For Loopback interface, enter the keyword <code>loopback</code> followed by a number from zero (0) to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• For a SONET interface, enter the keyword <code>sonet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

`ROUTER ISIS`

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in IS-IS updates sent via other interfaces.

### redistribute

Redistribute routes from one routing domain to another routing domain.

**Syntax**

```
redistribute {static | connected | rip}; [level-1 | level-1-2 | level-2] [metric metric-value] [metric-type {external | internal}]; [route-map map-name]
```

To end redistribution or disable any of the specified keywords, enter the `no redistribute {static | connected | rip} [metric metric-value] [metric-type {external | internal}] [level-1 | level-1-2 | level-2] [route-map map-name]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>connected</code></td>
<td>Enter the keyword <code>connected</code> redistribute active routes into IS-IS.</td>
</tr>
<tr>
<td><code>rip</code></td>
<td>Enter the keyword <code>rip</code> to redistribute RIP routes into IS-IS.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Enter the keyword <code>static</code> to redistribute user-configured routes into IS-IS.</td>
</tr>
<tr>
<td><code>metric metric-value</code></td>
<td>(OPTIONAL) Assign a value to the redistributed route.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 16777215</td>
</tr>
<tr>
<td></td>
<td>Default: 0. You should use a value that is consistent with the destination protocol.</td>
</tr>
<tr>
<td>`metric-type {external</td>
<td>internal}`</td>
</tr>
<tr>
<td></td>
<td>• external</td>
</tr>
<tr>
<td></td>
<td>• internal</td>
</tr>
<tr>
<td><code>level-1</code></td>
<td>(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.</td>
</tr>
</tbody>
</table>
To redistribute a default route (0.0.0.0/0), configure the `default-information originate` command.

Changing or disabling a keyword in this command will not affect the state of the other command keywords.

When an LSP with an internal metric is received, the FTOS considers the route cost taking into consideration the advertised cost to reach the destination.

Redistributed routing information is filtered with the `distribute-list out` command to ensure that the routes are properly passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for narrow or transition mode and the metric value in the `redistribute` command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the `metric-style` command is set for wide mode, an the metric value in the `redistribute` command is advertised.

**Related Commands**

- `default-information originate` Generate a default route for the IS-IS domain.
- `distribute-list out` Suppress networks from being advertised in updates. Redistributed routing information is filtered by this command.

---

**redistribute bgp**

Redistribute routing information from a BGP process. (new command in Release 6.3.1)

**Syntax**

```
redistribute bgp AS number [level-1] [level-1-2] [level-2] [metric metric-value] [metric-type {external | internal}] [route-map map-name]
```

To return to the default values, enter the `no redistribute bgp` command with the appropriate parameters.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AS number</strong></td>
<td>Enter a number that corresponds to the Autonomous System number.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 65535</td>
</tr>
<tr>
<td><strong>level-1</strong></td>
<td>(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only</td>
</tr>
<tr>
<td><strong>level-1-2</strong></td>
<td>(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.</td>
</tr>
<tr>
<td><strong>level-2</strong></td>
<td>(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only. This is the default.</td>
</tr>
<tr>
<td><strong>metric metric-value</strong></td>
<td>(OPTIONAL) The value used for the redistributed route. You should use a metric value that is consistent with the destination protocol. Range: 0 to 16777215 Default: 0.</td>
</tr>
<tr>
<td>**metric-type {external</td>
<td>internal}**</td>
</tr>
<tr>
<td><strong>route-map map-name</strong></td>
<td><em>map-name</em> is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol. If you do not specify a <em>map-name</em>, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.</td>
</tr>
</tbody>
</table>

### Defaults

IS-IS Level 2 routes only

### Command Modes

ROUTER ISIS (for IPv4)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

### Example

#### Figure 26-1. redistribute bgp Command Example

```plaintext
FTOS(conf)#router is
FTOS(conf-router_isis)#redistribute bgp 1 level-1 metric 32 metric-type external route-map rmap-isis-to-bgp
FTOS(conf-router_bgp)#show running-config isis
   !
   router isis
   redistribute bgp 1 level-1 metric 32 metric-type external route-map rmap-isis-to-bgp
```

### Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

BGP to IS-IS redistribution supports “match” options using route maps. The metric value, level, and metric-type of redistributed routes can be set by the redistribution command. More advanced “set” options can be performed using route maps.

### redistribute ospf

Redistribute routing information from an OSPF process.
Syntax
redistribute ospf process-id [level-1 | level-1-2 | level-2] [match {internal | external}] [metric metric-value] [metric-type {external | internal}] [route-map map-name]

To return to the default values, enter the no redistribute ospf process-id [level-1 | level-1-2 | level-2] [match {internal | external}] [metric metric-value] [metric-type {external | internal}] [route-map map-name] command.

Parameters

- **process-id**: Enter a number that corresponds to the OSPF process ID to be redistributed.
  - Range: 1 to 65355

- **metric metric-value** *(OPTIONAL)*: The value used for the redistributed route. You should use a metric value that is consistent with the destination protocol.
  - Range: 0 to 16777215
  - Default: 0.

- **metric-type {external | internal}** *(OPTIONAL)*: The external link type associated with the default route advertised into a routing domain. The two options are:
  - external
  - internal

- **level-1** *(OPTIONAL)*: Routes are independently redistributed into IS-IS as Level 1 routes.
- **level-1-2** *(OPTIONAL)*: Routes are independently redistributed into IS-IS as Level-1-2 routes.
- **level-2** *(OPTIONAL)*: Routes are independently redistributed into IS-IS as Level 2 routes.
  - This is the default.

- **match {external | internal}** *(OPTIONAL)*: The command used for OSPF to route and redistribute into other routing domains. The values are
  - internal
  - external

- **route-map map-name**: *map-name* is an identifier for a configured route map.
  - The route map should filter imported routes from the source routing protocol to the current routing protocol.
  - If you do not specify a *map-name*, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.

Defaults
- As above

Command Modes
- ROUTER ISIS *(for IPv4)*
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 *(for IPv6)*

Command History
- Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
- How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the metric-style command. If the metric-style command is set for narrow mode and the metric value in the redistribute ospf command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the metric-style command is set for wide mode, an the metric value in the redistribute ospf command is advertised.
**router isis**

Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

**Syntax**

```
router isis [tag]
```

To disable IS-IS routing, enter `no router isis [tag]`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER ISIS

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

You must configure a network entity title (the `net` command) to specify the area address and the router system ID.

You must enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

Only one IS-IS routing process can be configured to perform Level 2 routing. A **level-1-2** designation performs Level 1 and Level 2 routing at the same time.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip router isis</td>
<td>Configure IS-IS routing processes for IP on interfaces and attach an area designator to the routing process.</td>
</tr>
<tr>
<td>net</td>
<td>Configure an IS-IS network entity title (NET) for a routing process.</td>
</tr>
<tr>
<td>is-type</td>
<td>Assign a type for a given area.</td>
</tr>
</tbody>
</table>

**set-overload-bit**

Configure the router to set the overload bit in its non-pseudonode LSPs. This prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

**Syntax**

```
set-overload-bit
```

To return to the default values, enter `no set-overload-bit`.

**Defaults**

Not set.

**Command Modes**

ROUTER ISIS (for IPv4)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Usage Information**

Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.
show config

Display the changes you made to the IS-IS configuration. Default values are not shown.

Syntax

show config

Command Modes

ROUTER ISIS (for IPv4)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

show isis database

Display the IS-IS link state database.

Syntax

show isis database [level-1 | level-2] [local] [detail | summary] [lspid]

Parameters

- **level-1**: (OPTIONAL) Displays the Level 1 IS-IS link-state database.
- **level-2**: (OPTIONAL) Displays the Level 2 IS-IS link-state database.
- **local**: (OPTIONAL) Displays local link-state database information.
- **detail**: (OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

*Figure 26-4. Command Example: show isis database*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show isis database</code></td>
<td>Displays the IS-IS database.</td>
</tr>
</tbody>
</table>

```
FTOS#show isis database
IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime        ATT/P/OL
ISIS.00-00     * 0x00000006   0xCF43        580                0/0/0

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime        ATT/P/OL
ISIS.00-00     * 0x00000006   0xCF43        580                0/0/0

! FTOS#show isis database detail ISIS.00-00

IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime        ATT/P/OL
ISIS.00-00     * 0x0000002B   0x853B        1075               0/0/0
Area Address: 49.0000.0001
NLPID:          0xCC 0x8E
IP Address:  10.1.1.1
IPv6 Address: 1:1
Topology:     IPv4 (0x00) IPv6 (0x8002)
Metric: 10     IS OSPF.00
Metric: 10     IS (MT-IPv6) OSPF.00
Metric: 10     IP 15.1.1.0 255.255.255.0
Metric: 10     IPv6 (MT-IPv6) 1511::/64
Metric: 10     IPv6 (MT-IPv6) 2511::/64
Metric: 10     IPv6 (MT-IPv6) 1011::/64
Metric: 10     IPv6 1511::/64
Metric: 10     IP 10.1.1.0 255.255.255.0
Hostname:     ISIS

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime        ATT/P/OL
ISIS.00-00     * 0x00000002D 0x853B        1075               0/0/0
Area Address: 49.0000.0001
NLPID:          0xCC 0x8E
IP Address:  10.1.1.1
IPv6 Address: 1:1
Topology:     IPv4 (0x00) IPv6 (0x8002)
Multi-Topology IS-IS is enabled
Metric: 10     IS OSPF.00
Metric: 10     IS (MT-IPv6) OSPF.00
Metric: 10     IP 10.1.1.0 255.255.255.0
Metric: 20     IP 10.3.3.0 255.255.255.0
Metric: 10     IPv6 (MT-IPv6) 1511::/64
Metric: 10     IPv6 (MT-IPv6) 2511::/64
Metric: 10     IPv6 (MT-IPv6) 1033::/64
Metric: 20     IPv6 2511::/64
Metric: 20     IPv6 1033::/64
Hostname:     ISIS

FTOS#
```
**show isis graceful-restart detail**

Display detailed IS-IS Graceful Restart related settings.

**Syntax**

```
show isis graceful-restart detail
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>
show isis hostname

Display IS-IS host names configured or learned on the system.

Syntax

```
show isis hostname
```

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Figure 26-6. Command Example: show isis hostname

FTOS#show isis hostname
System Id       Dynamic Name   Static Name
*F100.E120.0013 Force10        ISIS
FTOS#
```

show isis interface

Display detailed IS-IS interface status and configuration information.

Syntax

```
show isis interface [interface]
```

Example

```
``
Parameters:

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For Loopback interface, enter the keyword `loopback` followed by a number from zero (0) to 16383.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Modes:

- EXEC
- EXEC Privilege

Command History:

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Example:

**Figure 26-7. Command Example: show isis interface (Partial)**

```plaintext
FTOS>show isis int
GigabitEthernet 0/7 is up, line protocol is up
Routing Protocol: IS-IS
  Circuit Type: Level-1-2
  Interface Index 37847070, Local circuit ID 1
  Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
  Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
  LSP Interval: 33
GigabitEthernet 0/8 is up, line protocol is up
Routing Protocol: IS-IS
  Circuit Type: Level-1-2
  Interface Index 38371358, Local circuit ID 2
  Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
  Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
```

**show isis neighbors**

Display information about neighboring (adjacent) routers.

**Syntax**

`show isis neighbors [level-1 | level-2] [detail] [interface]`

**Parameters**

- **level-1** (OPTIONAL) Displays information about Level 1 IS-IS neighbors.
- **level-2** (OPTIONAL) Displays information about Level 2 IS-IS neighbors.
**show isis neighbors**

Display IS-IS routing information.

**Usage Information**

Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the `show isis neighbors` command.

**Example**

```
FTOS#show isis neighbors
System Id  Interface State     Type    Priority Uptime      Circuit Id
TEST Gi 7/1    Up                  L1L2(M)   127    09:28:01    TEST.02

FTOS#show isis neighbors detail
System Id  Interface State     Type    Priority Uptime      Circuit Id
TEST Gi 7/1    Up                  L1L2(M)    127   09:28:04    TEST.02 Area Address(es):
49.0000.0001
IP Address(es): 25.1.1.3
MAC Address: 0000.0000.0000
Hold Time: 28
Link Local Address: fe80::201:e8ff:fe00:492c
Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
Adjacency being used for MTs: IPv4 IPv6
Identified Multi-Topology ISIS enabled
```

**Table 26-2. show isis neighbors Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>The value that identifies a system in an area.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface, slot, and port in which the router was discovered.</td>
</tr>
<tr>
<td>State</td>
<td>The value providing status about the adjacency state. The range is Up and Init.</td>
</tr>
<tr>
<td>Type</td>
<td>This value displays the adjacency type (Layer 2, Layer 2 or both).</td>
</tr>
<tr>
<td>Priority</td>
<td>IS-IS priority advertised by the neighbor. The neighbor with highest priority becomes the designated router for the interface.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Displays the interfaces uptime.</td>
</tr>
<tr>
<td>Circuit Id</td>
<td>The neighbor’s interpretation of the designated router for the interface.</td>
</tr>
</tbody>
</table>
**Syntax**
```
show isis protocol
```

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
- Introduced on the MXL 10/40GbE Switch IO Module.

Figure 26-9. Command Example: show isis protocol
```
FTOS#show isis protocol
IS-IS Router: <Null Tag>
   System Id: F100.E120.0013  IS-Type: level-1-2
   Manual area address(es):
   49.0000.0001
   Routing for area address(es):
   49.0000.0001
   Interfaces supported by IS-IS:
   GigabitEthernet 1/0 - IP - IPv6
   GigabitEthernet 1/1 - IP - IPv6
   GigabitEthernet 1/10 - IP - IPv6
   Loopback 0 - IP - IPv6
   Redistributing:
   Distance: 115
   Generate narrow metrics: level-1-2
   Accept narrow metrics: level-1-2
   Generate wide metrics: none
   Accept wide metrics: none
   Multi Topology Routing is enabled in transition mode.
FTOS#
```

**show isis traffic**

This command enables you to display IS-IS traffic interface information.

**Syntax**
```
show isis traffic [interface]
```

**Parameters**
- `interface` (OPTONAL) Identifies the interface type/port as one of the following:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
- Introduced on the MXL 10/40GbE Switch IO Module.
Figure 26-10. Command Example: show isis traffic

FTOS#show isis traffic
IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
IS-IS: PTP Hellos (sent/rcvd) : 0/0
IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
IS-IS: Level-1 DR Elections : 4
IS-IS: Level-2 DR Elections : 4
IS-IS: Level-1 SPF Calculations : 0
IS-IS: Level-2 SPF Calculations : 389
IS-IS: LSP checksum errors received : 0
IS-IS: LSP authentication failures : 0
FTOS#

Table 26-3. Command Example Fields

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level-1-Level-2 Hellos (sent/rcvd)</td>
<td>Displays the number of Hello packets sent and received.</td>
</tr>
<tr>
<td>PTP Hellos (sent/rcvd)</td>
<td>Displays the number of point-to-point Hellos sent and received.</td>
</tr>
<tr>
<td>Level-1-Level-2 LSPs sourced (new/refresh)</td>
<td>Displays the number of new and refreshed LSPs.</td>
</tr>
<tr>
<td>Level-1-Level-2 LSPs flooded (sent/rcvd)</td>
<td>Displays the number of flooded LSPs sent and received.</td>
</tr>
<tr>
<td>Level-1-Level-2 LSPs CSNPs (sent/rcvd)</td>
<td>Displays the number of CSNP LSPs sent and received.</td>
</tr>
<tr>
<td>Level-1-Level-2 LSPs PSNPs (sent/rcvd)</td>
<td>Displays the number of PSNP LPSs sent and received.</td>
</tr>
<tr>
<td>Level-1-Level-2 DR Elections</td>
<td>Displays the number of times designated router elections ran.</td>
</tr>
<tr>
<td>Level-1-Level-2 SPF Calculations</td>
<td>Displays the number of shortest path first calculations.</td>
</tr>
<tr>
<td>LSP checksum errors received</td>
<td>Displays the number of checksum errors LSPs received.</td>
</tr>
<tr>
<td>LSP authentication failures</td>
<td>Displays the number of LSP authentication failures.</td>
</tr>
</tbody>
</table>

spf-interval

Specify the minimum interval between Shortest Path First (SPF) calculations.

**Syntax**

```
spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the **no spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]** command.

**Parameters**

- **level-1** (OPTIONAL) Enter the keyword **level-1** to apply the configuration to Level-1 SPF calculations.
- **level-2** (OPTIONAL) Enter the keyword **level-2** to apply the configuration to Level-2 SPF calculations.
Intermediate System to Intermediate System (IS-IS) | 549

Defaults

Defaults as above

Command Modes

ROUTER ISIS (for IPv4)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command spf-interval in CONFIG-ROUTER-ISIS-AF-IPV6 mode is used for IPv6 Multi-Topology route computation only. If using single topology mode, use the spf-interval command in CONFIG-ROUTER-ISIS mode for both IPv4 and IPv6 route computations.

SPF throttling slows down the frequency at which route calculation are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (interval seconds). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval seconds</td>
<td>Enter the maximum number of seconds between SPF calculations. Range: 0 to 120 seconds Default: 10 seconds</td>
</tr>
<tr>
<td>initial_wait_interval seconds</td>
<td>(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. Range: 0 to 120 seconds Default: 5 second</td>
</tr>
<tr>
<td>second_wait_interval seconds</td>
<td>(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. Range: 0 to 120 seconds Default: 5 seconds</td>
</tr>
</tbody>
</table>
Link Aggregation Control Protocol (LACP)

Overview

This chapter contains commands for Dell Networking’s implementation of the link aggregation control protocol (LACP) for the creation of dynamic link aggregation groups (LAGs — called port-channels in FTOS parlance). For static LAG commands, refer to the section Port Channel Commands in the Interfaces chapter, based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

Commands

Use the following commands for LACP:

- clear lacp counters
- debug lacp
- lacp long-timeout
- lacp port-priority
- lacp system-priority
- port-channel mode
- port-channel-protocol lacp
- show lacp

**clear lacp counters**

Clear Port Channel counters.

**Syntax**

```
clear lacp port-channel-number counters
```

**Parameters**

- `port-channel-number` Enter a port-channel number:
  
  Range: 1 to 128

**Defaults**

Without a Port Channel specified, the command clears all Port Channel counters.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
debug lACP

Debug LACP (configuration, events etc.)

Syntax
ddebug lACP [config | events | pdu [in | out | [interface [in | out]]]]

To disable LACP debugging, use the no debug lACP [config | events | pdu [in | out | [interface [in | out]]]] command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>(OPTIONAL) Enter the keyword config to debug the LACP configuration.</td>
</tr>
<tr>
<td>events</td>
<td>(OPTIONAL) Enter the keyword events to debug LACP event information.</td>
</tr>
<tr>
<td>pdu in</td>
<td>(OPTIONAL) Enter the keyword pdu to debug LACP Protocol Data Unit information. Optionally, enter an in or out parameter to:</td>
</tr>
<tr>
<td></td>
<td>• Receive enter in</td>
</tr>
<tr>
<td></td>
<td>• Transmit enter out</td>
</tr>
<tr>
<td>interface in</td>
<td>Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a Ten Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>Optionally, enter an in or out parameter:</td>
</tr>
<tr>
<td></td>
<td>• Receive enter in</td>
</tr>
<tr>
<td></td>
<td>• Transmit enter out</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

Syntax

lacp long-timeout

To reset the timeout period to a short timeout (1 second), use the no lacp long-timeout command.

Defaults

1 second

Command Modes

INTERFACE (conf-if-po-number)

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Usage Information

This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, the command has no effect.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lACP</td>
<td>Displays the lACP configuration</td>
</tr>
</tbody>
</table>

**lACP port-priority**

Configure the port priority to influence which ports will be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

**Syntax**

```
lACP port-priority priority-value
```

To return to the default setting, use the `no lACP port-priority priority-value` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-value</td>
<td>Enter the port-priority value. The higher the value number the lower the priority.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 65535</td>
</tr>
<tr>
<td></td>
<td>Default: 32768</td>
</tr>
</tbody>
</table>

**Defaults**

32768

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**lACP system-priority**

Configure the LACP system priority.

**Syntax**

```
lACP system-priority priority-value
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-value</td>
<td>Enter the system-priority value. The higher the value, the lower the priority.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 65535</td>
</tr>
<tr>
<td></td>
<td>Default: 32768</td>
</tr>
</tbody>
</table>

**Defaults**

32768

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**port-channel mode**

Configure the LACP port channel mode.

**Syntax**

```
port-channel number mode [active] [passive] [off]
```
port-channel-protocol lacp
Enable LACP on any LAN port.

Syntax
port-channel-protocol lacp

To disable LACP on a LAN port, use the no port-channel-protocol lacp command.

Command Modes
INTERFACE

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 27-1.  port-channel-protocol lacp Command Example

FTOS(conf)#interface TenGigabitethernet 3/15
FTOS(conf-if-tengig-3/15)#no shutdown
FTOS(conf-if-tengig-3/15)#port-channel-protocol lacp
FTOS(conf-if-tengig-3/15-lacp)#port-channel 32 mode active
... FTOS(conf)#interface TenGigabitethernet 3/16
FTOS(conf-if-tengig-3/16)#no shutdown
FTOS(conf-if-tengig-3/16)#port-channel-protocol lacp
FTOS(conf-if-tengig-3/16-lacp)#port-channel 32 mode active
show lacp

Display the LACP matrix.

**Syntax**

```
show lacp port-channel-number [sys-id | counters]
```

**Parameters**

- `port-channel-number` Enter a port-channel number:
  - Range: 1 to 128
- `sys-id` (OPTIONAL) Enter the keyword `sys-id` and the value that identifies a system.
- `counters` (OPTIONAL) Enter the keyword `counters` to display the LACP counters.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example 1**

```
Figure 27-2. show lacp port-channel-number Command Example

FTOS#show lacp 1
Port-channel 1 admin up, oper up, mode lacp
Actor System ID: Priority 32768, Address 0001.e800.a12b
Partner System ID: Priority 32768, Address 0001.e801.45a5
Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
LACP LAG 1 is an aggregatable link
A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC
I - Collection enabled, J - Collection disabled, K - Distribution enabled L - Distribution disabled,
M - Partner Defaulted, N - Partner Non-defaulted, O - Receiver is in expired state,
P - Receiver is not in expired state
Port Te 10/6 is enabled, LACP is enabled and mode is lacp
Actor Admin: State ACEHLMP Key 1 Priority 128
Oper: State ACEGIKNM Key 1 Priority 128
Partner Admin: State BDFHLMP Key 0 Priority 0
Oper: State BCEDIKMP Key 1 Priority 128
FTOS#
```

**Example 2**

```
Figure 27-3. show lacp sys-id Command Example

FTOS#show lacp 1 sys-id
Actor System ID: Priority 32768, Address 0001.e800.a12b
Partner System ID: Priority 32768, Address 0001.e801.45a5
FTOS#
```
Figure 27-4. show lacp counter Command Example

```
FTOS#show lacp 1 counters
==================================================================
| Port    | Xmit LACP PDU Xmit Marker PDU Unknown Illegal |
|---------|-----------------|-----------------|-----------------|
| TenGig 10/6 | 200           | 0               | 0               |
| FTOS#    | 200            | 0               | 0               |
```

clear lacp counters  Clears the LACP counters.
show interfaces port-channel  Displays the information on configured Port Channel groups.
Layer 2

Overview

This chapter describes commands to configure Layer 2 features. It contains the following sections:

- MAC Addressing Commands
- Virtual LAN (VLAN) Commands

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses:

- clear mac-address-table dynamic
- mac-address-table aging-time
- mac-address-table static
- mac-address-table station-move refresh-arp
- mac learning-limit
- mac learning-limit learn-limit-violation
- mac learning-limit station-move-violation
- mac learning-limit reset
- show cam mac stack-unit
- show mac-address-table
- show mac-address-table aging-time
- show mac learning-limit

**clear mac-address-table dynamic**

Clear the MAC address table of all MAC address learned dynamically.

| Syntax | clear mac-address-table dynamic {address mac-address | all | interface interface | vlan vlan-id} |
|---|---|
| Parameters |  |
| **address mac-address** | Enter the keyword **address** followed by a MAC address in nn:nn:nn:nn:nn:nn format. |
| all | Enter the keyword **all** to delete all MAC address entries in the MAC address table. |
mac-address-table aging-time

Specify an aging time for MAC addresses to be removed from the MAC Address Table.

**Syntax**

```
mac-address-table aging-time seconds
```

**Parameters**

- `seconds`: Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter 0.
- Range: 10 - 1000000
- Default: 1800 seconds

**Defaults**

1800 seconds

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- `mac learning-limit`: Sets the MAC address learning limits for a selected interface.
- `show mac-address-table aging-time`: Displays the MAC aging time.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and virtual local area networks (VLANs).

**Syntax**

```
mac-address-table static mac-address output interface vlan vlan-id
```

To remove a MAC address, use the `no mac-address-table static mac-address output interface vlan vlan-id` command.
mac-address-table station-move refresh-arp
Ensure that address resolution protocol (ARP) refreshes the egress interface when a station move occurs due to a topology change.

Syntax

[no] mac-address-table station-move refresh-arp

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

show mac-address-table Displays the MAC address table.

mac learning-limit
Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

Syntax

mac learning-limit address_limit [dynamic] [no-station-move | station-move] [sticky]

Parameters

address_limit Enter the maximum number of MAC addresses that can be learned on the interface.
Range: 1 to 1000000

dynamic (OPTIONAL) Enter the keyword dynamic to allow aging of MACs even though a learning limit is configured.
no-station-move (OPTIONAL) Enter the keywords no-station-move to disallow a station move (associate the learned MAC address with the most recently accessed port) on learned MAC addresses.

station-move (OPTIONAL) Enter the keywords station-move to allow a station move on learned MAC addresses.

sticky (OPTIONAL) Enter the keyword sticky to allow configuring the sticky mac feature along with the learning limit.

Defaults

The default behavior is dynamic.

“Static” means manually entered addresses, which do not age.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

If you do not specify the vlan option, the MAC address counters are not VLAN-based. That is, the sum of the addresses learned on all VLANs (not having any learning limit configuration) is counted against the MAC learning limit.

MAC learning limit violation logs and actions are not available on a per-VLAN basis.

With the no-station-move option, MAC addresses learned through this feature on the selected interface persist on a per-VLAN basis, even if received on another interface. Enabling or disabling this option has no effect on already learned MAC addresses.

After the MAC address learning limit is reached, the MAC addresses do not age out unless you add the dynamic option. To clear statistics on MAC address learning, use the clear counters command with the learning-limit parameter.

When you add a channel member to a port-channel and there is not enough access control list (ACL) content addressable memory (CAM) space, the MAC limit functionality on that port-channel is undefined. When this occurs, un-configure the existing configuration first and then reapply the limit with a lower value.

Related Commands

- clear counters
- clear mac-address-table dynamic
- show mac learning-limit

- clears counters used in the show interface command.
- clears the MAC address table of all MAC address learned dynamically.
- displays MAC learning-limit configuration.
mac learning-limit learn-limit-violation
Configure an action for a MAC address learning-limit violation.

Syntax
mac learning-limit learn-limit-violation {log | shutdown}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Enter the keyword log to generate a syslog message on a learning-limit violation.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Enter the keyword shutdown to shut down the port on a learning-limit violation.</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
INTERFACE (conf-if-interface-slot/port)

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands
show mac learning-limit
Displays details of the mac learning-limit.

mac learning-limit station-move-violation
Specify the actions for a station move violation.

Syntax
mac learning-limit station-move-violation {log | shutdown-both | shutdown-offending | shutdown-original}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Enter the keyword log to generate a syslog message on a station move violation.</td>
</tr>
<tr>
<td>shutdown-both</td>
<td>Enter the keyword shutdown to shut down both the original and offending interface and generate a syslog message.</td>
</tr>
<tr>
<td>shutdown-offending</td>
<td>Enter the keywords shutdown-offending to shut down the offending interface and generate a syslog message.</td>
</tr>
<tr>
<td>shutdown-original</td>
<td>Enter the keywords shutdown-original to shut down the original interface and generate a syslog message.</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
INTERFACE (conf-if-interface-slot/port)

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information
This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands
- `show mac learning-limit` — Displays details of the mac learning-limit.

**mac learning-limit reset**
Reset the MAC address learning-limit error-disabled state.

**Syntax**
```plaintext
mac learning-limit reset
```

**Defaults**
none

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**show cam mac stack-unit**
Display the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

**Syntax**
```plaintext
show cam mac stack-unit unit_number port-set port-pipe count [vlan vlan-id] [interface interface]
```

**Parameters**
- `stack-unit unit_number` (REQUIRED) Enter the keywords `stack-unit` followed by a stack member number to select the stack unit for which to gather information. Range: 0 to 5
- `port-set port-pipe` (REQUIRED) Enter the keywords `port-set` followed by a Port-Pipe number to select the Port-Pipe for which to gather information. Range: 0
- `address mac-addr` (OPTIONAL) Enter the keyword `address` followed by a MAC address in the `nn:nn:nn:nn:nn:nn` format to display information on that MAC address.
- `dynamic` (OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses learned dynamically by the switch.
- `static` (OPTIONAL) Enter the keyword `static` to display only those MAC address specifically configured on the switch.
show mac-address-table

Display the MAC address table.

Syntax

show mac-address-table [dynamic | static] [address mac-address | interface interface | vlan vlan-id] [count [vlan vlan-id] [interface interface-type [slot /port]]]

Parameters

- **interface interface** (OPTIONAL) Enter the keyword interface followed by the interface type, slot and port information:
  - For a Port Channel interface, enter the keywords port-channel followed by a number:
    Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

- **vlan vlan-id** (OPTIONAL) Enter the keyword vlan followed by the VLAN ID to display the MAC address assigned to the VLAN.
  Range: 1 to 4094.

- **dynamic** (OPTIONAL) Enter the keyword dynamic to display only those MAC addresses learned dynamically by the switch. Optionally, you can also add one of these combinations: address/mac-address, interface/interface, or vlan vlan-id.

- **static** (OPTIONAL) Enter the keyword static to display only those MAC address specifically configured on the switch. Optionally, you can also add one of these combinations: address/mac-address, interface/interface, or vlan vlan-id.

- **address mac-address** (OPTIONAL) Enter the keyword address followed by a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.

- **interface interface** (OPTIONAL) Enter the keyword interface followed by the interface type, slot and port information:
  - For a Port Channel interface, enter the keywords port-channel followed by a number:
    Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

- **interface interface-type** (OPTIONAL) Instead of entering the keyword interface followed by the interface type, slot and port information, as above, you can enter the interface type, followed by just a slot number.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
show mac-address-table

(OPTIONAL) Enter the keyword `vlan` followed by the VLAN ID to display the MAC address assigned to the VLAN.
Range: 1 to 4094.

`count`

(OPTIONAL) Enter the keyword `count`, followed optionally, by an interface or VLAN ID, to display total or interface-specific static addresses, dynamic addresses, and MAC addresses in use.

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Figure 28-1. show mac-address-table Command Example

FTOS#show mac-address-table
VlanId     Mac Address           Type   Interface  State
20     00:00:c9:ad:f6:12       Dynamic Te 0/3          Active
FTOS#
```

```
Figure 28-2. show mac-address-table count Command Example

FTOS#show mac-address-table count
MAC Entries for all vlans :          Dynamic Address Count :       5
Static Address (User-defined) Count :  0
Total MAC Addresses in Use:          5
FTOS#
```

**Table 28-1. show mac-address-table Command Information**

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>Displays the VLAN ID number.</td>
</tr>
<tr>
<td>Type</td>
<td>Lists whether the MAC address was manually configured (Static) or learned dynamically (Dynamic).</td>
</tr>
</tbody>
</table>
| Interface      | Displays the interface type and slot/port information. The following abbreviations describe the interface types:  
  - tengig — Ten Gigabit Ethernet followed by a slot/port.  
  - po — Port Channel followed by a number. Range: 1 to 128  
  - te — 10-Gigabit Ethernet followed by a slot/port. |
| State          | Lists if the MAC address is in use (Active) or not in use (Inactive). |

**Table 28-2. show mac-address-table count Command Information**

<table>
<thead>
<tr>
<th>Line Beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Entries...</td>
<td>Displays the number of MAC entries learnt per VLAN.</td>
</tr>
<tr>
<td>Dynamic Address...</td>
<td>Lists the number of dynamically learned MAC addresses.</td>
</tr>
</tbody>
</table>
show mac-address-table aging-time

Display the aging times assigned to the MAC addresses on the switch.

**Syntax**

```
show mac-address-table aging-time [vlan vlan-id]
```

**Parameters**

- `vlan vlan-id` Enter the keyword `vlan` followed by the VLAN ID to display the MAC address aging time for MAC addresses on the VLAN. Range: 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
FTOS#show mac-address-table aging-time
Mac-address-table aging time : 1800
FTOS#
```

**Related Commands**

- `show mac-address-table`: Displays the current MAC address configuration.
show mac learning-limit

Display MAC address learning limits set for various interfaces.

Syntax

```
show mac learning-limit [violate-action] [detail] [interface interface]
```

Parameters

- **violate-action** (OPTIONAL) Enter the keywords `violate-action` to display the MAC learning limit violation status.
- **detail** (OPTIONAL) Enter the keyword `detail` to display the MAC learning limit in detail.
- **interface interface** (OPTIONAL) Enter the keyword `interface` with the following keywords and slot/port or number information:
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel` followed by a number:
    Range: 1 to 128

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Example

```
Figure 28-4.  show mac learning-limit Command Example

FTOS#show mac learning-limit
Interface      Learning       Dynamic        Static         Unknown SA
Slot/port      Limit          MAC count      MAC count         Drops
FTOS#
```
Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual local area networks (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address and Layer 3 protocols on a VLAN called Inter-VLAN routing. file transfer protocol (FTP), trivial FTP (TFTP), ACLs, and simple network management protocol (SNMP) are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the VRRP state of a VLAN interface may continually switch between Master and Backup.

- description
- default vlan-id
- default-vlan disable
- name
- show config
- show vlan
- tagged
- track ip
- untagged

For more information, also refer to VLAN Stacking and VLAN-related commands, such as portmode hybrid, in Chapter 20, Interfaces.

description

Add a description about the selected VLAN.

**Syntax**

description description

To remove the description from the VLAN, use the no description command.

**Parameters**

- description

  Enter a text string description to identify the VLAN (80 characters maximum).

**Defaults**

none

**Command Modes**

INTERFACE VLAN

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

**Related Commands**

- show vlan  Displays VLAN configuration.
default vlan-id

Specify a VLAN as the Default VLAN.

Syntax

```
default vlan-id vlan-id
```n

To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the `no default vlan-id vlan-id` command.

Parameters

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>Enter the VLAN ID number of the VLAN to become the new Default VLAN. Range: 1 to 4094. Default: 1</td>
</tr>
</tbody>
</table>
```

Defaults

The Default VLAN is VLAN 1.

Command Modes

- CONFIGURATION

Command History

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- To return VLAN 1 as the Default VLAN, use the `default-vlan-id 1` command.
- The default VLAN contains only untagged interfaces.

Related Commands

```
interface vlan
```

- Configures a VLAN.

---

default-vlan disable

Disable the default VLAN so that all switchports are placed in the Null VLAN until they are explicitly configured as a member of another VLAN.

Defaults

The default VLAN is enabled.

Command Modes

- CONFIGURATION

Command History

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- The `no default vlan disable` command is not listed in the running-configuration, but when you disable the default VLAN, `default-vlan disable` is listed in the running-configuration.

name

Assign a name to the VLAN.

Syntax

```
name vlan-name
```n

To remove the name from the VLAN, use the `no name` command.

Parameters

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Enter up to 32 characters as the name of the VLAN.</td>
</tr>
</tbody>
</table>
```
Defaults
Not configured.

Command Modes
INTERFACE VLAN

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
To display information about a named VLAN, enter the show vlan command with the name parameter or the show interfaces description command.

Related Commands
description Assigns a descriptive text string to the interface.
interface vlan Configures a VLAN.
show vlan Displays the current VLAN configurations on the switch.

show config
Display the current configuration of the selected VLAN.

Syntax
show config

Command Modes
INTERFACE VLAN

Example
Figure 28-5. show config Command Example for a Selected VLAN

```
FTOS(conf-if-vl-100)#show config
!
interface Vlan 1
description a
no ip address
mtu 2500
shutdown
FTOS(conf-if-vl-100)#
```

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

show vlan
Display the current VLAN configurations on the switch.

Syntax
show vlan [brief | id vlan-id | name vlan-name]

Parameters
brief (OPTIONAL) Enter the keyword brief to display the following information:
  • VLAN ID
  • VLAN name (left blank if none is configured.)
  • Spanning Tree Group ID
  • MAC address aging time
  • IP address
### Command Modes
- EXEC
- EXEC Privilege

### Command History
- **Version 8.3.16.1**
  - Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information
The following describes the `show vlan` command shown in the following example.

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
</table>
| Column 1 - no heading | asterisk symbol (*) = Default VLAN  
G = GVRP VLAN  
P = primary VLAN  
C = community VLAN  
I = isolated VLAN  
O = OpenFlow |
| NUM | Displays existing VLAN IDs. |
| Status | Displays the word *Inactive* for inactive VLANs and the word *Active* for active VLANs. |
| Q | • Displays G for GVRP tagged  
• M for member of a VLAN-Stack VLAN  
• T for tagged interface  
• U for untagged interface  
• x (not capitalized x) for Dot1x untagged  
• X (capitalized X) for Dot1x tagged  
• o (not capitalized o) for OpenFlow untagged  
• O (capitalized O) for OpenFlow tagged  
• H for VSN tagged  
• i (not capitalized i) for Internal untagged  
• I (capitalized I) for Internal tagged  
• v (not capitalized v) for VLT untagged  
• V (capitalized V) for VLT tagged |
| Ports | Displays the type, slot, and port information.  
• Po = port channel  
• Fo = forty Gigabit Ethernet  
• Te = Ten gigabit Ethernet |
Example

Figure 28-6.  show vlan Command Example

FTOS#show vlan

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
x - Dot1x untagged, X - Dot1x tagged
G - GVRP tagged, M - Vlan-stack, H - VSN tagged
i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT tagged

NUM Status Description Q Ports
1 Inactive a
2 Inactive
* 20 Active U Te 0/3,5,13,53-56
1002 Active T Te 0/3,13,55-56

FTOS#

Figure 28-7.  show vlan id Command Example

FTOS# show vlan id 40

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
x - Dot1x untagged, X - Dot1x tagged
G - GVRP tagged, M - Vlan-stack, H - VSN tagged
i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT tagged

NUM Status Description Q Ports
1 Inactive a

FTOS#

Figure 28-8.  show vlan brief Command Example

FTOS#show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>STG</th>
<th>MAC Aging</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>unassigned</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>unassigned</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>0</td>
<td>unassigned</td>
</tr>
<tr>
<td>1002</td>
<td>0</td>
<td>0</td>
<td>unassigned</td>
</tr>
</tbody>
</table>

FTOS#

Figure 28-9.  Using a VLAN Name Example

FTOS(conf)#interface vlan 222
FTOS(conf-if-vl-222)#name test
FTOS(conf-if-vl-222)#do show vlan name test

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
x - Dot1x untagged, X - Dot1x tagged
G - GVRP tagged, M - Vlan-stack

NUM Status Description Q Ports
222 Inactive U TenGig 1/22

FTOS(conf-if-vl-222)#
FTOS#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-stack compatible</td>
<td>Enables the Stackable VLAN feature on the selected VLAN.</td>
</tr>
<tr>
<td>interface vlan</td>
<td>Configures a VLAN.</td>
</tr>
</tbody>
</table>
Add a Layer 2 interface to a VLAN as a tagged interface.

**Syntax**

```plaintext
tagged interface
```

To remove a tagged interface from a VLAN, use `no tagged interface` command.

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  - For a Port Channel interface, enter the keywords `port-channel` followed by a number:
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

**Defaults**

All interfaces in Layer 2 mode are untagged.

**Command Modes**

INTERFACE VLAN

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When you use the `no tagged` command, the interface is automatically placed in the default VLAN as an untagged interface unless the interface is a member of another VLAN. If the interface belongs to several VLANs, you must remove it from all VLANs to change it to an untagged interface.

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

In programmable-mux (PMUX) mode of input/output aggregator (IOA), when you use the `no tagged` command on an interface, the VLAN is not removed from the VLAN table, even if there are no active members for the VLAN.

**Related Commands**

- `interface vlan` Configures a VLAN.
- `untagged` Specifies which interfaces in a VLAN are untagged.

Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

**Syntax**

```plaintext
track ip interface
```

To remove the tracking feature from the VLAN, use the `no track ip interface` command.
When you configure this command, the VLAN is operationally UP if any of the interfaces specified in the `track ip` command are operationally UP. The VLAN is operationally DOWN if none of the tracking interfaces are operationally UP.

If you do not configure the `track ip` command, the VLAN's Layer 3 operational state depends on all the members of the VLAN.

The Layer 2 state of the VLAN, and hence the Layer 2 traffic, is not affected by the `track ip` command configuration.

Related Commands

- `interface vlan` Configures a VLAN.
- `tagged` Specifies which interfaces in a VLAN are tagged.

**untagged**

Add a Layer 2 interface to a VLAN as an untagged interface.

**Syntax**

```
untagged interface
```

To remove an untagged interface from a VLAN, use the `no untagged interface` command.

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  - For a Port Channel interface, enter the keywords `port-channel` followed by a number:
    Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

**Defaults**

All interfaces in Layer 2 mode are untagged.

**Command Modes**

INTERFACE VLAN

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information

Untagged interfaces can only belong to one VLAN.

In the default VLAN, you cannot use the `no untagged interface` command. To remove an untagged interface from all VLANs, including the default VLAN, enter INTERFACE mode and use the `no Port Channel Commands` command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface vlan</td>
<td>Configures a VLAN.</td>
</tr>
<tr>
<td>tagged</td>
<td>Specifies which interfaces in a VLAN are tagged.</td>
</tr>
</tbody>
</table>
Link Layer Discovery Protocol (LLDP)

Overview

The link layer discovery protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN. LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Fore10 operating software (FTOS) implementation of LLDP is based on IEEE standard 801.1ab.

Commands

This chapter contains the following commands, in addition to the commands in the related section — LLDP-MED Commands.

- advertise dot1-tlv
- advertise dot3-tlv
- advertise management-tlv
- clear lldp counters
- clear lldp neighbors
- debug lldp interface
- disable
- hello
- mode
- multiplier
- protocol lldp (Configuration)
- protocol lldp (Interface)
- show lldp neighbors
- show lldp statistics
- show running-config lldp

The starting point for using LLDP is invoking LLDP with the protocol lldp command in either CONFIGURATION or INTERFACE mode.

The information distributed by LLDP is stored by its recipients in a standard management information base (MIB). The information can be accessed by a network management system through a management protocol such as SNMP.

For details about implementing LLDP/LLDP-MED, refer to the Link Layer Discovery Protocol chapter of the FTOS Configuration Guide.
advertise dot1-tlv
Advertise dot1 TLVs (Type, Length, Value).

Syntax
advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}

To remove advertised dot1-tlv, use the no advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-protocol-vlan-id</td>
<td>Enter the keyword port-protocol-vlan-id to advertise the port protocol VLAN identification TLV.</td>
</tr>
<tr>
<td>port-vlan-id</td>
<td>Enter the keyword port-vlan-id to advertise the port VLAN identification TLV.</td>
</tr>
<tr>
<td>vlan-name</td>
<td>Enter the keyword vlan-name to advertise the vlan-name TLV.</td>
</tr>
</tbody>
</table>

Defaults
Disabled

Command Modes
CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

Related Commands

- protocol lldp (Configuration) Enables LLDP globally.
- debug lldp interface Debugs LLDP.
- show lldp neighbors Displays the LLDP neighbors.
- show running-config lldp Displays the LLDP running configuration.

advertise dot3-tlv
Advertise dot3 TLVs (Type, Length, Value).

Syntax
advertise dot3-tlv {max-frame-size}

To remove advertised dot3-tlv, use the no advertise dot3-tlv {max-frame-size} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-frame-size</td>
<td>Enter the keyword max-frame-size to advertise the dot3 maximum frame size.</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>
advertise management-tlv

Advertise management TLVs (Type, Length, Value).

**Syntax**

```plaintext
advertise management-tlv {system-capabilities | system-description | system-name}
```

To remove advertised management TLVs, use the no advertise management-tlv
{system-capabilities | system-description | system-name} command.

**Parameters**

- **system-capabilities**
  - Enter the keyword `system-capabilities` to advertise the system capabilities TLVs.

- **system-description**
  - Enter the keyword `system-description` to advertise the system description TLVs.

- **system-name**
  - Enter the keyword `system-name` to advertise the system description TLVs.

**Defaults**

none

**Command Modes**

CONFIGURATION (conf-lldp)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

All three command options — system-capabilities, system-description, and system-name — can be invoked individually or together, in any sequence.

---

clear lldp counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

**Syntax**

```plaintext
clear lldp counters interface
```

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

clear lldp neighbors

Clear LLDP neighbor information for all interfaces or a specific interfaces.

**Syntax**

```plaintext
clear lldp neighbors {interface}
```

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
Parameters

**interface**

Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword **tenGigabitEthernet** followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword **fortyGigE** followed by the slot/port information.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

d debug lldp interface

Enable LLDP debugging to display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets.

**Syntax**

d debug lldp interface \{interface | all\} \{events | packet \{brief | detail\} \{tx | rx | both\}\}

To disable debugging, use the no debug lldp interface \{interface | all\} \{events | packet \{brief | detail\} \{tx | rx | both\}\} command.

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a 10-Gigabit Ethernet interface, enter the keyword **tenGigabitEthernet** followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword **fortyGigE** followed by the slot/port information.

- **all**
  - (OPTIONAL) Enter the keyword **all** to display information on all interfaces.

- **events**
  - (OPTIONAL) Enter the keyword **events** to display major events such as timer events.

- **packet**
  - (OPTIONAL) Enter the keyword **packet** to display information regarding packets coming in or going out.

- **brief**
  - (OPTIONAL) Enter the keyword **brief** to display brief packet information.

- **detail**
  - (OPTIONAL) Enter the keyword **detail** to display detailed packet information.

- **tx**
  - (OPTIONAL) Enter the keyword **tx** to display transmit only packet information.

- **rx**
  - (OPTIONAL) Enter the keyword **rx** to display receive only packet information

- **both**
  - (OPTIONAL) Enter the keyword **both** to display both receive and transmit packet information.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---
disable

Enable or disable LLDP.

**Syntax**

disable

To enable LLDP, use the no disable

**Defaults**

Enabled, that is no disable

**Command Modes**

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- protocol lldp (Configuration) Enables LLDP globally.
- debug lldp interface Debugs LLDP
- show lldp neighbors Displays the LLDP neighbors
- show running-config lldp Displays the LLDP running configuration

hello

Configure the rate at which the LLDP control packets are sent to its peer.

**Syntax**

hello seconds

To revert to the default, use the no hello seconds command.

**Parameters**

- **seconds**
  
Enter the rate, in seconds, at which the control packets are sent to its peer.
  
  Rate: 5 to 180 seconds
  
  Default: 30 seconds

**Defaults**

30 seconds

**Command Modes**

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

mode

Set LLDP to receive or transmit.

**Syntax**

mode \{tx | rx\}

To return to the default, use the no mode \{tx | rx\} command.

**Parameters**

- **tx**
  
Enter the keyword tx to set the mode to transmit.

- **rx**
  
Enter the keyword rx to set the mode to receive.

**Defaults**

Both transmit and receive
multiplier

Set the number of consecutive misses before LLDP declares the interface dead.

**Syntax**

multiplier integer

To return to the default, use the no multiplier integer command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>integer</td>
<td>Enter the number of consecutive misses before the LLDP declares the interface dead.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 - 10</td>
</tr>
</tbody>
</table>

**Defaults**

4 x hello

**Command Modes**

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**protocol lldp (Configuration)**

Enable LLDP globally on the switch.

**Syntax**

protocol lldp

To disable LLDP globally on the chassis, use the no protocol lldp command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION (conf-lldp)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**protocol lldp (Interface)**

Enter the LLDP protocol in the INTERFACE mode.

**Syntax**

[no] protocol lldp

To return to the global LLDP configuration mode, use the no protocol lldp command from the Interface mode.

**Defaults**

LLDP is not enabled on the interface.
**show lldp neighbors**

Display LLDP neighbor information for all interfaces or a specified interface.

**Syntax**

show lldp neighbors [interface] [detail]

**Parameters**

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

- **detail** (OPTIONAL) Enter the keyword `detail` to display all the TLV information, timers, and LLDP tx and rx counters.

**Defaults**

`none`

**Command Modes**

EXEC Privilege

**Example**

```plaintext
R1(conf-if-te-1/31)#do show lldp neighbors
Loc PortID   Rem Host Name       Rem Port Id           Rem Chassis Id
-------------------------------------------------------------------------
TenGig 1/21      R2                  TenGigabitEthernet 2/11  00:01:e8:06:95:3e
TenGig 1/31      R3                  TenGigabitEthernet 3/11  00:01:e8:09:c2:4a
```

**Usage Information**

Omitting the keyword `detail` displays only the remote chassis ID, Port ID, and Dead Interval.

**show lldp statistics**

Display the LLDP statistical information.

**Syntax**

show lldp statistics

**Defaults**

`none`
show running-config lldp

Display the current global LLDP configuration.

Syntax
show running-config lldp

Defaults
none

Command Modes
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 29-3. show running-config lldp Command Example

FTOS#show running-config lldp
!
protocol lldp
 advertise dot1-tlv port-protocol-vlan-id port-vlan-id
 advertise dot3-tlv max-frame-size
 advertise management-tlv system-capabilities system-description
 hello 35
 multiplier 3
 no disable
FTOS#
LLDP-MED Commands

The LLDP-media endpoint discovery (MED) commands in this section are:

- advertise med guest-voice
- advertise med guest-voice-signaling
- advertise med location-identification
- advertise med power-via-mdi
- advertise med softphone-voice
- advertise med streaming-video
- advertise med video-conferencing
- advertise med video-signaling
- advertise med voice
- advertise med voice-signaling

FTOS LLDP-MED commands are an extension of the set of LLDP TLV advertisement commands.

As defined by ANSI/TIA-1057, LLDP-MED provides organizationally specific type length value (TLVs), so that endpoint devices and network connectivity devices can advertise their characteristics and configuration information. The Organizational Unique Identifier (OUI) for the Telecommunications Industry Association (TIA) is 00-12-BB.

- **LLDP-MED Endpoint Device** — any device that is on an IEEE 802 LAN network edge, can communicate using IP, and uses the LLDP-MED framework.
- **LLDP-MED Network Connectivity Device** — any device that provides access to an IEEE 802 LAN to an LLDP-MED endpoint device, and supports IEEE 802.1AB (LLDP) and TIA-1057 (LLDP-MED). The Dell Networking system is an LLDP-MED network connectivity device.

With regard to connected endpoint devices, LLDP-MED provides network connectivity devices with the ability to:

- manage inventory
- manage Power over Ethernet (POE)
- identify physical location
- identify network policy

advertise med guest-voice

Configure the system to advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support interactive voice services.

**Syntax**

```
advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>Enter the VLAN ID.</td>
<td>1 to 4094</td>
</tr>
<tr>
<td><code>layer2_priority</code></td>
<td>Enter the Layer 2 priority.</td>
<td>0 to 7</td>
</tr>
<tr>
<td><code>DSCP_value</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>number</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
advertise med guest-voice-signaling

Configure the system to advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data.

Syntax

advertise med guest-voice-signaling \{vlan-id layer2_priority DSCP_value\} | {priority-tagged number}

To return to the default, use the no advertise med guest-voice-signaling \{vlan-id layer2_priority DSCP_value\} | {priority-tagged number} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>Enter the VLAN ID.</td>
<td>1 to 4094</td>
</tr>
<tr>
<td>layer2_priority</td>
<td>Enter the Layer 2 priority.</td>
<td>0 to 7</td>
</tr>
<tr>
<td>DSCP_value</td>
<td>Enter the DSCP value.</td>
<td>0 to 63</td>
</tr>
<tr>
<td>priority-tagged</td>
<td>Enter the keyword priority-tagged followed the Layer 2 priority.</td>
<td>0 to 7</td>
</tr>
</tbody>
</table>

Defaults

unconfigured

Command Modes

CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug lldp interface</td>
<td>Debugs LLDP</td>
</tr>
<tr>
<td>show lldp neighbors</td>
<td>Displays the LLDP neighbors</td>
</tr>
<tr>
<td>show running-config lldp</td>
<td>Displays the LLDP running configuration</td>
</tr>
</tbody>
</table>
advertise med location-identification

Configure the system to advertise a location identifier.

Syntax

advertise med location-identification \{coordinate-based value | civic-based value | ecs-elin value\}

To return to the default, use the no advertise med location-identification \{coordinate-based value | civic-based value | ecs-elin value\} command.

Parameters

- **coordinate-based value**: Enter the keyword coordinate-based followed by the coordinated based location in hexadecimal value of 16 bytes.
- **civic-based value**: Enter the keyword civic-based followed by the civic based location in hexadecimal format. Range: 6 to 255 bytes
- **ecs-elin value**: Enter the keyword ecs-elin followed by the Emergency Call Service (ecs) Emergency Location Identification Number (elin) numeric location string. Range: 10 to 25 characters

Defaults

unconfigured

Command Modes

CONFIGURATION (conf-lldp)

Command History

- **Version 8.3.16.1**: Introduced on MXL 10/40GbE Switch IO Module

Usage Information

**ECS** — Emergency Call Service such as defined by TIA or National Emergency Numbering Association (NENA)

**ELIN** — Emergency Location Identification Number, a valid North America Numbering Plan format telephone number supplied for ECS purposes.

Related Commands

- debug lldp interface : Debugs LLDP
- show lldp neighbors : Displays the LLDP neighbors
- show running-config lldp : Displays the LLDP running configuration

advertise med power-via-mdi

Configure the system to advertise the Extended Power via MDI TLV.

Syntax

advertise med power-via-mdi

To return to the default, use the no advertise med power-via-mdi command.

Defaults

unconfigured

Command Modes

CONFIGURATION (conf-lldp)

Command History

- **Version 8.3.16.1**: Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Advertise the Extended Power via MDI on all ports that are connected to an 802.3af powered, LLDP-MED endpoint device.
advertise med softphone-voice

Configure the system to advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone.

Syntax

advertise med softphone-voice \{vlan-id\} | {priority-tagged number}

To return to the default, use the no advertise med softphone-voice \{vlan-id\} | {priority-tagged number} command.

Parameters

- **vlan-id**
  - Enter the VLAN ID.
  - Range: 1 to 4094
- **priority-tagged number**
  - Enter the keyword priority-tagged followed the Layer 2 priority.
  - Range: 0 to 7

Defaults

unconfigured

Command Modes

CONFIGURATION (conf-lldp)

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

debug lldp interface
- Debugs LLDP

show lldp neighbors
- Displays the LLDP neighbors

show running-config lldp
- Displays the LLDP running configuration

advertise med streaming-video

Configure the system to advertise streaming video services for broadcast or multicast-based video. This does not include video applications that rely on TCP buffering.

Syntax

advertise med streaming-video \{vlan-id\} | {priority-tagged number}

To return to the default, use the no advertise med streaming-video \{vlan-id\} | {priority-tagged number} command.

Parameters

- **vlan-id**
  - Enter the VLAN ID.
  - Range: 1 to 4094
- **priority-tagged number**
  - Enter the keyword priority-tagged followed the Layer 2 priority.
  - Range: 0 to 7

Defaults

unconfigured

Command Modes

CONFIGURATION (conf-lldp)
advertise med video-conferencing

Configure the system to advertise dedicated video conferencing and other similar appliances that support real-time interactive video.

Syntax

advertise med video-conferencing {vlan-id} | {priority-tagged number}

To return to the default, use the no advertise med video-conferencing {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters

- **vlan-id**: Enter the VLAN ID.
  - Range: 1 to 4094
- **priority-tagged number**: Enter the keyword priority-tagged followed the Layer 2 priority.
  - Range: 0 to 7

Defaults

unconfigured

Command Modes

CONFIGURATION (conf-lldp)

Related Commands

- debug lldp interface: Debugs LLDP
- show lldp neighbors: Displays the LLDP neighbors
- show lldp neighbors: Displays the LLDP running configuration

advertise med video-signaling

Configure the system to advertise video control packets that use a separate network policy than video data.

Syntax

advertise med video-signaling {vlan-id} | {priority-tagged number}

To return to the default, use the no advertise med video-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters

- **vlan-id**: Enter the VLAN ID.
  - Range: 1 to 4094
- **priority-tagged number**: Enter the keyword priority-tagged followed the Layer 2 priority.
  - Range: 0 to 7

Defaults

unconfigured
advertise med voice

Configure the system to advertise a dedicated IP telephony handset or other appliances supporting interactive voice services.

Syntax
advertise med voice \{vlan-id\} | \{priority-tagged number\}

To return to the default, use the no advertise med voice \{vlan-id layer2_priority DSCP_value\} | \{priority-tagged number\} command.

Parameters
- \texttt{vlan-id}
  - Enter the VLAN ID.
  - Range: 1 to 4094
- \texttt{priority-tagged number}
  - Enter the keyword \texttt{priority-tagged} followed the Layer 2 priority.
  - Range: 0 to 7

Defaults
unconfigured

Command Modes
CONFIGURATION (conf-lldp)

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands
debug lldp interface Debugs LLDP
show lldp neighbors Displays the LLDP neighbors
show running-config lldp Displays the LLDP running configuration

advertise med voice-signaling

Configure the system to advertise when voice control packets use a separate network policy than voice data.

Syntax
advertise med voice-signaling \{vlan-id\} | \{priority-tagged number\}

To return to the default, use the no advertise med voice-signaling \{vlan-id layer2_priority DSCP_value\} | \{priority-tagged number\} command.

Parameters
- \texttt{vlan-id}
  - Enter the VLAN ID.
  - Range: 1 to 4094
- \texttt{priority-tagged number}
  - Enter the keyword \texttt{priority-tagged} followed the Layer 2 priority.
  - Range: 0 to 7

Defaults
unconfigured

Command Modes
CONFIGURATION (conf-lldp)

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands
debug lldp interface Debugs LLDP
show lldp neighbors Displays the LLDP neighbors
show running-config lldp Displays the LLDP running configuration
### Defaults
unconfigured

### Command Modes
CONFIGURATION (conf-lldp)

### Command History
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

### Related Commands
- `debug lldp interface`: Debugs LLDP
- `show lldp neighbors`: Displays the LLDP neighbors
- `show lldp neighbors`: Displays the LLDP running configuration
Multicast Source Discovery Protocol (MSDP)

Overview

Multicast Source Discovery Protocol (MSDP) connects multiple PIM Sparse-Mode (PIM-SM) domains together. MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections.

The Dell Networking operating system (FTOS) supports MSDP commands on the MXL switch.

Commands

The following commands configure MSDP:

- clear ip msdp peer
- clear ip msdp sa-cache
- clear ip msdp statistic
- debug ip msdp
- ip msdp cache-rejected-sa
- ip msdp default-peer
- ip msdp log-adjacency-changes
- ip msdp mesh-group
- ip msdp originator-id
- ip msdp peer
- ip msdp redistribute
- ip msdp sa-filter
- ip msdp sa-limit
- ip msdp shutdown
- ip multicast-msdp
- show ip msdp
- show ip msdp sa-cache rejected-sa

clear ip msdp peer

Reset the TCP connection to the peer and clear all the peer statistics.

Syntax  clear ip msdp peer {peer address}
clear ip msdp sa-cache

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Syntax

`clear ip msdp sa-cache [group-address | rejected-sa | local]`

Parameters

- **group-address**: Enter the group IP address in dotted decimal format (A.B.C.D.).
- **rejected-sa**: Enter the keywords `rejected-sa` to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
- **local**: Enter the keyword `local` to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults

Without any options, this command clears the entire source-active cache.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0) - Introduced on the MXL 10/40GbE Switch IO Module.

clear ip msdp statistic

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Syntax

`clear ip msdp sa-cache [group-address | rejected-sa | local]`

Parameters

- **group-address**: Enter the group IP address in dotted decimal format (A.B.C.D.).
- **rejected-sa**: Enter the keywords `rejected-sa` to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
- **local**: Enter the keyword `local` to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults

Without any options, this command clears the entire source-active cache.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0) - Introduced on the MXL 10/40GbE Switch IO Module.
debug ip msdp

Turn on MSDP debugging.

Syntax

d debug ip msdp \{event peer address | packet peer address | pim\}

To turn debugging off, use the no debug ip msdp \{event peer address | packet peer address | pim\} command.

Parameters

- **event peer address**: Enter the keyword **event** then the peer address in a dotted decimal format (A.B.C.D.).
- **packet peer address**: Enter the keyword **packet** then the peer address in a dotted decimal format (A.B.C.D.).
- **pim**: Enter the keyword **pim** to debug advertisement from PIM.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

ip msdp cache-rejected-sa

Enable a MSDP cache for the rejected source-active entries.

Syntax

ip msdp cache-rejected-sa \{number\}

To clear the MSDP rejected source-active entries, use the no ip msdp cache-rejected-sa \{number\} command then the ip msdp cache-rejected-sa \{number\} command.

Parameters

- **number**: Enter the number of rejected SA entries to cache. The range is from 0 to 32766.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- show ip msdp sa-cache rejected-sa: Display the rejected SAs in the SA cache.

ip msdp default-peer

Define a default peer from which to accept all Source-Active (SA) messages.

Syntax

ip msdp default-peer peer address [list name]

To remove the default peer, use the no ip msdp default-peer \{peer address\} list name command.
Parameters

- **peer address**: Enter the peer address in a dotted decimal format (A.B.C.D.).
- **list name**: Enter the keywords list name and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
If a list is not specified, all SA messages received from the default peer are accepted. You can enter multiple default peer commands.

**ip msdp log-adjacency-changes**
Enable logging of MSDP adjacency changes.

Syntax
ip msdp log-adjacency-changes

To disable logging, use the no ip msdp log-adjacency-changes command.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**ip msdp mesh-group**
To be a member of a mesh group, configure a peer.

Syntax
ip msdp mesh-group {name} {peer address}

To remove the peer from a mesh group, use the no ip msdp mesh-group {name} {peer address} command.

Parameters

- **name**: Enter a string of up to 16 characters long for as the mesh group name.
- **peer address**: Enter the peer address in a dotted decimal format (A.B.C.D.).

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
A MSDP mesh group is a mechanism for reducing SA flooding, typically in an intra-domain setting. When some subset of a domain’s MSDP speakers are fully meshed, they can be configured into a mesh-group. If member $X$ of a mesh-group receives a SA message from an MSDP peer that is also a member of the mesh-group, member $X$ accepts the SA message and forwards it to all of its peers that are not part of the mesh-group. However, member $X$ cannot forward the SA message to other members of the mesh-group.

**Usage Information**

**ip msdp originator-id**

Configure the MSDP Originator ID.

**Syntax**

```
ip msdp originator-id {interface}
```

To remove the originator-id, use the `no ip msdp originator-id {interface}` command.

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a SONET interface, enter the keywords `sonet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**ip msdp peer**

Configure an MSDP peer.

**Syntax**

```
ip msdp peer peer address [connect-source] [description] [sa-limit number]
```

To remove the MSDP peer, use the `no ip msdp peer peer address [connect-source interface] [description name] [sa-limit number]` command.
Parameters

- **peer address**: Enter the peer address in a dotted decimal format (A.B.C.D.).

- **connect-source interface**: Enter the keywords `connect-source` then one of the interfaces and slot/port or number information:
  - For a Fast Ethernet interface, enter the keyword `FastEthernet` then the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

- **description name**: (OPTIONAL) Enter the keyword `description` then a description name (maximum 80 characters) to designate a description for the MSDP peer.

- **sa-limit number**: (OPTIONAL) Enter the maximum number of SA entries in SA-cache. The range is from 1 to 500000. The default is 500000.

Defaults

As described in the **Parameters** section.

Command Modes

- **CONFIGURATION**

Command History

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- The `connect-source` option is used to supply a source IP address for the TCP connection. When an interface is specified using the `connect-source` option, the primary configured address on the interface is used.

- If the total number of SA messages received from the peer is already larger than the limit when this command is applied, those SA messages will continue to be accepted. To enforce the limit in such situation, use command `clear ip msdp peer` command to reset the peer.

Related Commands

- `ip msdp sa-limit` Configure the MSDP SA Limit.
- `clear ip msdp peer` Clear the MSDP peer.
- `show ip msdp` Display the MSDP information.

**ip msdp redistribute**

Filter local PIM SA entries in the SA cache. SAs which the ACL denies time out and are not refreshed. Until they time out, they continue to reside in the MSDP SA cache.

**Syntax**

- `ip msdp redistribute [list acl-name]`

**Parameters**

- **list acl-name**: Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

**Defaults**

Not configured.

**Command Modes**

- **CONFIGURATION**
### ip msdp sa-filter

**Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.**

**Syntax**

```
ip msdp sa-filter {in | out} peer-address list [access-list name]
```

Remove this configuration using the `no ip msdp sa-filter {in | out} peer address list [access-list name]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>in</code></td>
<td>Enter the keyword <code>in</code> to enable incoming SA filtering.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Enter the keyword <code>out</code> to enable outgoing SA filtering.</td>
</tr>
<tr>
<td><code>peer-address</code></td>
<td>Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.).</td>
</tr>
<tr>
<td><code>access-list name</code></td>
<td>Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### ip msdp sa-limit

Configure the upper limit of SA (Source-Active) entries in SA-cache.

**Syntax**

```
ip msdp sa-limit number
```

To return to the default, use the `no ip msdp sa-limit number` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter the maximum number of SA entries in SA-cache. The range is from 0 to 40000.</td>
</tr>
</tbody>
</table>

**Defaults**

50000

**Command Modes**

CONFIGURATION

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
FTOS counts the SA messages originated by itself and those received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking).

If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in FTOS continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp sa-cache` command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip msdp peer</code></td>
<td>Configure the MSDP peer.</td>
</tr>
<tr>
<td><code>clear ip msdp peer</code></td>
<td>Clear the MSDP peer.</td>
</tr>
<tr>
<td><code>show ip msdp</code></td>
<td>Display the MSDP information.</td>
</tr>
</tbody>
</table>

### ip msdp shutdown

Administratively shut down a configured MSDP peer.

**Syntax**

```
ip msdp shutdown {peer address}
```

**Parameters**

`peer address` Enter the peer address in a dotted decimal format (A.B.C.D.).

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### ip multicast-msdp

Enable MSDP.

**Syntax**

```
ip multicast-msdp
```

To exit MSDP, use the `no ip multicast-msdp` command.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

### show ip msdp

Display the MSDP peer status, SA cache, or peer summary.

**Syntax**

```
show ip msdp {peer peer address | sa-cache | summary}
```

598 | Multicast Source Discovery Protocol (MSDP)
Parameters

peer peer address          Enter the keyword peer then the peer address in a dotted decimal format (A.B.C.D.).

sa-cache                 Enter the keyword sa-cache to display the Source-Active cache.

summary                  Enter the keyword summary to display a MSDP peer summary.

Defaults                  Not configured.

Command Modes

EXEC

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example 1

Figure 30-1. show ip msdp peer Command Example

FTOS#show ip msdp peer 100.1.1.1
Peer Addr: 100.1.1.1
 Local Addr: 100.1.1.2(639) Connect Source: none
 State: Established Up/Down Time: 00:00:08
 Timers: KeepAlive 60 sec, Hold time 75 sec
 SourceActive packet count (in/out): 0/0
 SAAs learned from this peer: 0
 SA Filtering:
 Input (S,G) filter: none
 Output (S,G) filter: none
 FTOS#

Example 2

Figure 30-2. show ip msdp sa-cache Command Example

FTOS#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
GroupAddr     SourceAddr    RPAddr          LearnedFrom   Expire UpTime
224.1.1.1      172.21.220.10 172.21.3.254    172.21.3.254    102 00:02:52
 FTOS#

Example 3

Figure 30-3. show ip msdp summary Command Example

FTOS#show ip msdp summary
Peer Addr Local Addr State     Source SA Up/Down Description
72.30.1.2 72.30.1.2 Established none 0 00:00:03 peer1
72.30.2.2 72.30.2.2 Established none 0 00:00:03 peer2
72.30.3.2 72.30.3.2 Established none 0 00:00:02 test-peer-3
 FTOS#

show ip msdp sa-cache rejected-sa
Display the rejected SAs in the SA cache.

Syntax

show ip msdp sa-cache rejected-sa

Defaults

none

Command Modes

EXEC
**EXEC Privilege**

| Command History |
|-----------------|-----------------|
| **Version 9.2(0.0)** | Introduced on the MXL 10/40GbE Switch IO Module. |

**Example**

**Figure 30-4. show ip msdp sa-cache rejected-sa Command Example**

```
FTOS#show ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache  200 rejected SAs received, cache-size 1000
UpTime GroupAddr SourceAddr RPAddr LearnedFrom Reason
00:00:13 225.1.2.1 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.2 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.3 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.4 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.5 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.6 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.7 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.8 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.9 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.10 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.11 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.12 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.13 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.14 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.15 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.16 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.17 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.18 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.19 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
FTOS#
```
Multiple Spanning Tree Protocol (MSTP)

Overview

The multiple spanning tree protocol (MSTP), as implemented by the Dell Networking operating software (FTOS), conforms to IEEE 802.1s.

Commands

The following commands configure and monitor MSTP:

- `debug spanning-tree mstp`
- `disable`
- `edge-port bpdufilter default`
- `hello-time`
- `max-age`
- `max-hops`
- `msti`
- `name`
- `protocol spanning-tree mstp`
- `revision`
- `show config`
- `show spanning-tree mst configuration`
- `show spanning-tree msti`
- `spanning-tree`
- `spanning-tree msti`
- `spanning-tree mstp`
- `tc-flush-standard`
debug spanning-tree mstp

Enable debugging of the multiple spanning tree protocol and view information on the protocol.

Syntax
d debug spanning-tree mstp [all | bpdu interface {in | out} | events]

To disable debugging, use the no debug spanning-tree mstp command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(OPTIONAL) Enter the keyword all to debug all spanning tree operations.</td>
</tr>
<tr>
<td>bpdu interface</td>
<td>(OPTIONAL) Enter the keyword bpdu to debug Bridge Protocol Data Units.</td>
</tr>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following:</td>
</tr>
<tr>
<td>out</td>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 128</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
<tr>
<td>events</td>
<td>Optionally, enter an in or out parameter in conjunction with the optional interface:</td>
</tr>
<tr>
<td></td>
<td>• For Receive, enter in</td>
</tr>
<tr>
<td></td>
<td>• For Transmit, enter out</td>
</tr>
<tr>
<td>events</td>
<td>(OPTIONAL) Enter the keyword events to debug MSTP events.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 31-1. debug spanning-tree mstp bpdu Command Example

```
FTOS#debug spanning-tree mstp bpdu tengigabitethernet 0/16 ?
in Receive (in)
out Transmit (out)
FTOS#
```

description

Enter a description of the multiple spanning tree protocol.

Syntax
d description {description}

To remove the description, use the no description {description} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Enter a description to identify the Multiple Spanning Tree (80 characters maximum).</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

SPANNING TREE (The prompt is “config-mstp”.)
**disable**

Globally disable the multiple spanning tree protocol on the switch.

**Syntax**  
disable

To enable Multiple Spanning Tree Protocol, use the **no disable** command.

**Defaults**  
MSTP is disabled

**Command Modes**  
MULTIPLE SPANNING TREE

**Related Commands**  
- **protocol spanning-tree mstp** — Enters MULTIPLE SPANNING TREE mode on the switch.

---

**edge-port bpdufilter default**

Enable bridge protocol data units (BPDU) filter globally to filter transmission of BPDU on port-fast enabled interfaces.

**Syntax**  
edge-port bpdufilter default

To disable global bpdu filter default, use the **no edge-port bpdufilter default** command.

**Defaults**  
Disable

**Command Modes**  
MULTIPLE SPANNING TREE

**Related Commands**  
- **protocol spanning-tree mstp** — Enters MULTIPLE SPANNING TREE mode.

---

**forward-delay**

The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

**Syntax**  
forward-delay *seconds*

To return to the default setting, use the **no forward-delay** command.
hello-time

Set the time interval between generation of Multiple Spanning Tree Bridge Protocol Data Units (BPDUs).

Syntax

```
hello-time seconds
```

To return to the default value, use the `no hello-time` command.

Parameters

- **seconds**
  - Enter a number as the time interval between transmission of BPDUs.
  - Range: 1 to 10.
  - Default: 2 seconds.

Defaults

2 seconds

Command Modes

MULTIPLE SPANNING TREE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- **max-age** Changes the wait time before MSTP refreshes protocol configuration information.
- **hello-time** Changes the time interval between BPDUs.

max-age

Set the time interval for the MSTP bridge to maintain configuration information before refreshing that information.

Syntax

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

Parameters

- **seconds**
  - Enter number of seconds the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
  - Range: 4 to 30
  - Default: 15 seconds.

Defaults

15 seconds

Command Modes

MULTIPLE SPANNING TREE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- **edge-port** The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
- **bpdufilter default**
- **max-age** Changes the wait time before MSTP refreshes protocol configuration information.
max-hops

Configure the maximum hop count.

**Syntax**

```
max-hops number
```

To return to the default values, use the **no max-hops** command.

**Parameters**

- `range`
  - Enter a number for the maximum hop count.
  - Range: 1 to 40
  - Default: 20

**Defaults**

- 20 hops

**Command Modes**

- MULTIPLE SPANNING TREE

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The `max-hops` is a configuration command that applies to both the IST and all MST instances in the MSTP region. The BPDUs sent out by the root switch set the remaining-hops parameter to the configured value of max-hops. When a switch receives the BPDU, it decrements the received value of the remaining hops and uses the resulting value as remaining-hops in the BPDUs. If the remaining-hops reaches zero, the switch discards the BPDU and ages out any information that it holds for the port.

msti

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

**Syntax**

```
msti instance {vlan range | bridge-priority priority}
```

To disable mapping or bridge priority, use the **no msti instance {vlan range | bridge-priority priority}** command.
Multiple Spanning Tree Protocol (MSTP)

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msti instance</td>
<td>Enter the MST instance number. Range: 0 to 4094.</td>
</tr>
<tr>
<td>vlan range</td>
<td>Enter the keyword vlan followed by the identifier range value. Range: 1 to 4094</td>
</tr>
<tr>
<td>bridge-priority</td>
<td>Enter the keyword bridge-priority followed by a value in increments of 4096 as the bridge priority. Range: zero (0) to 61440. Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.</td>
</tr>
</tbody>
</table>

**Defaults**

default bridge-priority is 32768

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

By default, all VLANs are mapped to MST instance zero (0) unless you use the vlan range command to map it to a non-zero instance.

Although MSTP instance IDs range from 0 to 4094, only 64 active instances are supported on the switch.

**name**

The name you assign to the multiple spanning tree region.

**Syntax**

name region-name

To remove the region name, use the no name command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>region-name</td>
<td>Enter the MST region name. Range: 32 character limit</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

MULTIPLE SPANNING TREE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

For two MSTP switches to be within the same MSTP region, the switches must share the same region name (including matching case).

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msti</td>
<td>Maps the VLAN(s) to an MST instance.</td>
</tr>
<tr>
<td>revision</td>
<td>Assigns the revision number to the MST configuration.</td>
</tr>
</tbody>
</table>
**protocol spanning-tree mstp**

Enter MULTIPLE SPANNING TREE mode to enable and configure the multiple spanning tree group.

**Syntax**

```
protocol spanning-tree mstp
```

To disable the multiple spanning tree group, use the `no protocol spanning-tree mstp` command.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

Introduced on MXL 10/40GbE Switch IO Module

**Example**

Figure 31-2.  protocol spanning-tree mstp Command Example

```
FTOS(conf)#protocol spanning-tree mstp
FTOS(conf-mstp)#no disable
```

**Usage Information**

MSTP is not enabled when you enter the MULTIPLE SPANNING TREE mode. To enable MSTP globally on the switch, enter `no disable` while in MULTIPLE SPANNING TREE mode.

For more information about the multiple spanning tree protocol, refer to the *FTOS Configuration Guide*.

**Related Commands**

- `disable` — Disables MSTP.

---

**revision**

The revision number for the multiple spanning tree configuration

**Syntax**

```
revision range
```

To return to the default values, use the `no revision` command.

**Parameters**

- `range` — Enter the revision number for the MST configuration.
  
  Range: 0 to 65535
  
  Default: 0

**Defaults**

0

**Command Modes**

MULTIPLE SPANNING TREE

**Command History**

Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

For two MSTP switches to be within the same MST region, the switches must share the same revision number.

**Related Commands**

- `msti` — Maps the VLAN(s) to an MST instance
  
  - `name` — Assigns the region name to the MST region.
show config

View the current configuration for the mode. Only non-default values are shown.

Syntax
show config

Command Modes
MULTIPLE SPANNING TREE

Example
Figure 31-3. show config Command Example

```
FTOS(conf-mstp)#show config
!
protocol spanning-tree mstp
no disable
name CustomerSvc
revision 2
MSTI 10 VLAN 101-105
max-hops 5
FTOS(conf-mstp)#
```

show spanning-tree mst configuration

View the multiple spanning tree configuration.

Syntax
show spanning-tree mst configuration

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 31-4. show spanning-tree mst configuration Command Example

```
FTOS#show spanning-tree mst configuration
MST region name: CustomerSvc
Revision: 2
MSTI VID
10  101-105
FTOS#
```

Usage Information
You must enable the multiple spanning tree protocol prior to using this command.

show spanning-tree msti

View the Multiple Spanning Tree instance.

Syntax
show spanning-tree msti [instance-number [brief]] [guard]
**show spanning-tree msti [instance-number]**

- **Parameters**
  - **instance-number** [OPTIONAL] Enter the MST instance number. Range: 0 to 4094.
  - **brief** [OPTIONAL] Enter the keyword **brief** to view a synopsis of the MST instance.
  - **guard** [OPTIONAL] Enter the keyword **guard** to display the type of guard enabled on an MSTP interface and the current port state.

- **Command Modes**
  - EXEC
  - EXEC Privilege

- **Usage Information**
  You must enable the multiple spanning tree protocol prior to using this command.

- **Command History**
  - Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

- **Example**
  **Figure 31-5.  show spanning-tree msti [instance-number] Command Example**

```
FTOS#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e800.0204
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 0001.e800.0204
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max hops 20
Bpdu filter disabled globally
CIST regional root ID Priority 32768, Address 0001.e800.0204
CIST external path cost 0

Interface        PortID   Prio Cost    Sts        Cost        Bridge ID        PortID
Name             -------- -------- ---- ------- ----------- ------- -------------------
--------
Te 0/41 128.170  128  2000    FWD 0       32768 0001.e800.0204 128.170
Te 0/42 128.171  128  2000    FWD 0       32768 0001.e800.0204 128.171
Te 0/43 128.172  128  2000    FWD 0       32768 0001.e800.0204 128.172

Interface Name          Role  PortID   Prio Cost    Sts  Cost  Link-type Edge Filter
Boundary
-------- ------ -------- -------- ---- ------ ------------
Te 0/41 Desg 128.170  128  2000    FWD 0     P2P No No
Te 0/42 Desg 128.171  128  2000    FWD 0     P2P No No
Te 0/43 Desg 128.172  128  2000    FWD 0     P2P No No
FTOS#
```
Example 2  Figure 31-6.  show spanning-tree msti Command Example with EDS and LBK

```
FTOS#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094

Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0

Interface Name PortID Prio Cost Sts Cost Bridge ID PortID
---------- -------- ---- ------- --- ------- -------------------- --------
TenGig 0/0 128.257 128 20000 EDS 0 32768 0001.e801.6aa8 128.257
```

Example 3  Figure 31-7.  show spanning-tree msti guard Command Example

```
FTOS#show spanning-tree msti 0 guard
Executing IEEE compatible Spanning Tree Protocol
Bpdu filter disabled globally

Interface Name Instance Sts Guard type Bpdu Filter
---------- -------- --------- ---------- ------------
Te 0/41 0 FWD None No
Te 0/42 0 FWD None No
Te 0/43 0 FWD None No
```

Table 31-1.  show spanning-tree msti guard Command Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>MSTP interface</td>
</tr>
<tr>
<td>Instance</td>
<td>MSTP instance</td>
</tr>
</tbody>
</table>
spanning-tree

Enable the multiple spanning tree protocol on the interface.

Syntax

```
spanning-tree
```

To disable the multiple spanning tree protocol on the interface, use the `no spanning-tree` command.

Parameters

- `spanning-tree` Enter the keyword `spanning-tree` to enable the MSTP on the interface.
  
  Default: Enable

Defaults

Enable

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

spanning-tree msti

Configure multiple spanning tree instance cost and priority for an interface.

Syntax

```
spanning-tree msti instance {cost cost | priority priority}
```

Parameters

- `instance` Enter the MST instance number.
  
  Range: 0 to 4094.

- `cost cost` (OPTIONAL) Enter the keyword `cost` followed by the port cost value.
  
  Range: 1 to 200000

  Defaults:
  - 40-Gigabit Ethernet interface = 1400
  - 10-Gigabit Ethernet interface = 2000
  - Port Channel interface with one 10-Gigabit Ethernet = 2000
  - Port Channel with two 10-Gigabit Ethernet = 1800
  - Port Channel with two 100-Mbps Ethernet = 180000

- `priority priority` Enter keyword `priority` followed by a value in increments of 16 as the priority.
  
  Range: 0 to 240.

  Default: 128

Defaults

- `cost` = depends on the interface type; `priority` = 128

Command Modes

INTERFACE

Table 31-1. show spanning-tree msti guard Command Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sts</td>
<td>Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut)</td>
</tr>
<tr>
<td>Guard Type</td>
<td>Type of STP guard configured (Root or BPDU guard)</td>
</tr>
<tr>
<td>BPDU Filter</td>
<td>BPDU filter enabled (Yes) or BPDU filter disabled (No)</td>
</tr>
</tbody>
</table>
spanning-tree mstp

Configures a Layer 2 MSTP interface as an edge port with (optionally) a BPDU guard, a BPDU filter or enables the root guard feature on the interface.

Syntax

spanning-tree mstp {edge-port [bpduguard [shutdown-on-violation | bpdufilter]] | rootguard}

Parameters

- **edge-port**
  - Enter the keyword `edge-port` to configure the interface as a Multiple Spanning Tree edge port.

- **bpduguard**
  - Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
  - (OPTIONAL) Enter the keyword `bpduguard` to enable edge port configuration to move the interface into forwarding mode immediately after the root fails.

- **bpdufilter**
  - Enter the keyword `bpdufilter` to stop sending and receiving BPDUs on the port-fast enabled ports.
  - (OPTIONAL) Enter the keyword `bpdufilter` to enable edge port configuration to move the interface into forwarding mode immediately after the root fails.

- **shutdown-on-violation**
  - (OPTIONAL) Enter the keyword `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

- **rootguard**
  - Enter the keyword `rootguard` to enable root guard on an MSTP port or port-channel interface.

Command Modes

- INTERFACE

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

On an MSTP switch, a port configured as an edge port will immediately transition to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with spanning-tree portfast enabled.

Root guard and loop guard cannot be enabled at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed:

% Error: RootGuard is configured. Cannot configure LoopGuard.

When used in an MSTP network, if root guard blocks a boundary port in the CIST, the port is also blocked in all other MST instances.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an err-disabled blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a loop-inconsistent blocking state and no traffic is forwarded on the port.
tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

**Syntax**

tc-flush-standard

To disable, use the no tc-flush-standard command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td></td>
<td>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

By default, FTOS implements an optimized flush mechanism for MSTP. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on the knob command to enable flushing MAC addresses after receiving every topology change notification.
Multicast

Overview

The multicast commands are supported by Dell Networking operating systems (FTOS) on the MXL switch. This chapter contains the following sections:

- IPv4 Multicast Commands
- IPv6 Multicast Commands

IPv4 Multicast Commands

The IPv4 Multicast commands are:

- clear ip mroute
- ip mroute
- ip multicast-limit
- ip multicast-routing
- show ip mrout
- show ip rpf
clear ip mroute

Clear learned multicast routes on the multicast forwarding table. To clear the protocol-independent multicast (PIM) tree information base, use Usage Information command.

Syntax
clear ip mroute {group-address [source-address] | * | snooping}

Parameters

- **group-address**
  - Enter multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.

- **source-address**
  - Enter * to clear all multicast routes.

- **snooping**
  - Enter the keyword snooping to delete multicast snooping route table entries.

Command Modes

EXEC Privilege

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Related Commands

- show ip pim tib Show the PIM Tree Information Base.

ip mroute

Assign a static mroute.

Syntax

ip mroute destination mask {ip-address | null 0 | {bgp | ospf} process-id | isis | rip | static} {ip-address | tag | null 0} [distance]

To delete a specific static mroute, use the command ip mroute destination mask {ip-address | null 0 | {bgp | ospf} process-id | isis | rip | static} {ip-address | tag | null 0} [distance] command.

To delete all mroutes matching a certain mroute, use the no ip mroute destination mask command.

Parameters

- **destination**
  - Enter the IP address in dotted decimal format of the destination device.

- **mask**
  - Enter the mask in slash prefix formation (/x) or in dotted decimal format.

- **null 0**
  - (OPTIONAL) Enter the keyword null then zero (0).

- **[protocol [process-id | tag] ip-address]**
  - (OPTIONAL) Enter one of the routing protocols:
    - Enter the BGP as-number then the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. The range is from 1 to 65535
    - Enter the OSPF process identification number then the IP address in dotted decimal format of the RPF neighbor. The range is from 1 to 65535
    - Enter the IS-IS alphanumeric tag string then the IP address in dotted decimal format of the RPF neighbor.
    - Enter the RIP IP address in dotted decimal format of the RPF neighbor.

- **static ip-address**
  - (OPTIONAL) Enter the Static IP address in dotted decimal format of the RPF neighbor.
ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

**Syntax**

```
ip multicast-limit limit
```

**Parameters**

- `limit` Enter the desired maximum number of multicast entries on the system.

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum possible number of entries, depending on the configured CAM profile.

To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.

ip multicast-routing

Enable IP multicast forwarding.

**Syntax**

```
ip multicast-routing
```

**Default**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
After you enable multicast, you can enable IGMP and PIM on an interface. In INTERFACE mode, enter the `ip pim sparse-mode` command to enable IGMP and PIM on the interface.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip pim sparse-mode</code></td>
<td>Enables IGMP and PIM on an interface.</td>
</tr>
</tbody>
</table>

**show ip mroute**

View the Multicast Routing Table.

**Syntax**

```
show ip mroute [static | group-address [source-address] | count | snooping [vlan vlan-id] [group-address [source-address]] | summary | vlt [group-address [source-address] | count]
```

**Parameters**

- `static` (OPTIONAL) Enter the keyword `static` to view static multicast routes.
- `group-address` (OPTIONAL) Enter the multicast group-address to view only routes associated with that group.
  - `source-address` Enter the source-address to view routes with that group-address and source-address.
- `count` (OPTIONAL) Enter the keyword `count` to view the number of multicast routes and packets.
- `snooping [vlan vlan-id] [group-address [source-address]]` Enter the keyword `snooping` to display information on the multicast routes PIM-SM snooping discovers.
  - `vlan vlan-id` Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. The VLAN ID range is from 1 to 4094.
  - `group-address` Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.
- `summary` (OPTIONAL) Enter the keyword `summary` to view a summary of all routes.
- `vlt [group-address [source-address] | count]` (OPTIONAL) Enter the keyword `vlt` to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group and optionally a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed for a specified multicast source. Enter the keyword `count` to display the total number of multicast routes with the spanned IIF.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example 1**

```
FTOS#show ip mroute static
Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change: 00:00:23
```
Example 2  

**Figure 32.2. show ip mroute snooping Command Example**

```
FTOS#show ip mroute snooping
IPv4 Multicast Snooping Table

(*, 224.0.0.0), uptime 17:46:23
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13
    GigabitEthernet 4/20
```

Example 3  

**Figure 32.3. show ip mroute Command Example**

```
FTOS#show ip mroute
IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: GigabitEthernet 3/4
  Outgoing interface list:
    GigabitEthernet 3/12
    GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/4
```

Table 32-1. show ip mroute Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S,G)</td>
<td>Displays the forwarding entry in the multicast route table.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the multicast forwarding</td>
</tr>
<tr>
<td></td>
<td>table.</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) information towards the</td>
</tr>
<tr>
<td></td>
<td>source for (S,G) entries and the RP for (*,G) entries.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Lists the interfaces that meet one of the following:</td>
</tr>
<tr>
<td></td>
<td>• a directly connected member of the Group.</td>
</tr>
<tr>
<td></td>
<td>• statically configured member of the Group.</td>
</tr>
<tr>
<td></td>
<td>• received a (*,G) or (S,G) Join message.</td>
</tr>
</tbody>
</table>
show ip rpf

View reverse path forwarding.

Syntax

show ip rpf

Command Modes

EXEC

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Network administrators use static mroutes to control the reach-ability of the multicast sources. If a PIM-registered multicast source is reachable using static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one of the PIM selects for reach-ability.

Note: The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

Example

Figure 32-5. show ip rpf Command Example

FTOS#show ip rpf
RPF information for 10.10.10.9
RPF interface: Gi 3/4
RPF neighbor: 165.87.31.4
RPF route/mask: 10.10.10.9/255.255.255.255
RPF type: unicast

IPv6 Multicast Commands

IPv6 Multicast commands are:

- debug ipv6 mld_host
- ip multicast-limit
debug ipv6 mld_host

Enable the collection of debug information for MLD host transactions.

**Syntax**

[no] debug ipv6 mld_host [int-count | interface type] [slot / port-range]

To discontinue collection of debug information for the MLD host transactions, use the `no debug ipv6 mld_host` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>int-count</code></td>
<td>Enter the keyword <code>count</code> to indicate the number of required debug messages.</td>
</tr>
<tr>
<td><code>interface type</code></td>
<td>Enter the following keywords and slot/port information:</td>
</tr>
<tr>
<td></td>
<td>• For a 10G Ethernet interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40G interface, enter the keyword <code>fortyGigE</code> then the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a management interface, enter the keyword <code>management interface</code> then the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a port-channel interface, enter the keyword <code>port-channel</code> then the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN interface, enter the keyword <code>vlan</code> then the slot/port information.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

To debug the MLD protocol for all ports or for specified ports, use the `debug ipv6 mld_host` command. Displayed information includes when a query is received, when a report is sent, when a mcast joins or leaves a group, and some reasons why an MLD query is rejected.

ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

**Syntax**

`ip multicast-limit limit`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>limit</code></td>
<td>Enter the desired maximum number of multicast entries on the system. The range is from 1 to 50000.</td>
</tr>
</tbody>
</table>

**Defaults**

15000 routes

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum number of entries, depending on the configured CAM profile.

To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.
Neighbor Discovery Protocol (NDP)

The Dell Networking operating software (FTOS) supports the network discovery protocol for IPv6 on the MXL switch. The neighbor discovery protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. NDP defines mechanisms for solving the following problems:

- Router discovery: Hosts can locate routers residing on a link
- Prefix discovery: Hosts can discover address prefixes for the link
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor unreachability detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate address detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

NDP uses the following five ICMPv6 packet types in its implementation:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

Commands

The NDP commands in this chapter are:

- clear ipv6 neighbors
- ipv6 neighbor
- show ipv6 neighbors

clear ipv6 neighbors

Delete all entries in the IPv6 neighbor discovery cache, or neighbors of a specific interface. Static entries are not removed using this command.

Syntax  
clear ipv6 neighbors [ipv6-address] [interface]
ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

Syntax

```
ipv6 neighbor {ipv6-address} {interface interface} {hardware_address}
```

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the no ipv6 neighbor {ipv6-address} {interface interface} command.

Parameters

- **ipv6-address**: Enter the IPv6 address of the neighbor in the x:x:x:x: format.
  - **NOTE**: The :: notation specifies successive hexadecimal fields of zero.

- **interface interface**: Enter the keyword interface followed by the interface type and slot/port or number information of the interface:
  - For a Fast Ethernet interface, enter the keyword fastEthernet then the slot/port information.
  - For a Port Channel interface, enter the keyword port-channel then the number:
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE then the slot/port information.
  - For a VLAN, enter the keyword vlan then the VLAN ID. The range is from 1 to 4094.

- **hardware_address**: Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn format.

Defaults

- none
show ipv6 neighbors

Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the CP (control processor).

Syntax

show ipv6 neighbors [ipv6-address] [cpu {rp1 [ipv6-address] | rp2 [ipv6-address]}] [interface interface]

Parameters

ipv6-address Enter the IPv6 address of the neighbor in the x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

cpu Enter the keyword cpu then either rp1 or rp2 (Route Processor 1 or 2), optionally then an IPv6 address to display the IPv6 neighbor entries stored on the designated RP.

interface interface • For a Fast Ethernet interface, enter the keyword fastEthernet then the slot/port information.
• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE then the slot/port information.
• For a VLAN, enter the keyword vlan then the VLAN ID. The range is from 1 to 4094.

Defaults

none

Command Modes

EXEC
EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
### Example

**Figure 33-1. show ipv6 neighbors Command Example**

```
FTOS#show ipv6 neighbors
IPv6 Address   Expires(min)   Hardware Address   State   Interface  VLAN   CPU
------------------------------------------------------------------------------
fe80::201:e8ff:fe17:5bc6       1439       00:01:e8:17:5b:c6  STALE   Gi 1/9     -   CP
fe80::201:e8ff:fe17:5bc7       1439       00:01:e8:17:5b:c7  STALE   Gi 1/10    -   CP
fe80::201:e8ff:fe17:5bc8       1439       00:01:e8:17:5b:c8  STALE   Gi 1/11    -   CP
fe80::201:e8ff:fe17:5caf       0.3        00:01:e8:17:5c:af  REACH   Po 1     -   CP
fe80::201:e8ff:fe17:5cb0       1439       00:01:e8:17:5c:b0  STALE   Po 32    -   CP
fe80::201:e8ff:fe17:5cb1       1439       00:01:e8:17:5c:b1  STALE   Po 255   -   CP
fe80::201:e8ff:fe17:5cae       1439       00:01:e8:17:5c:ae  STALE   Gi 1/3   Vl 100  CP
fe80::201:e8ff:fe17:5cae       1439       00:01:e8:17:5c:ae  STALE   Gi 1/5   Vl 1000 CP
fe80::201:e8ff:fe17:5cae       1439       00:01:e8:17:5c:ae  STALE   Gi 1/7   Vl 2000 CP
```

FTOS#
Open Shortest Path First (OSPF)

Overview

The MXL 10/40GbE Switch IO Module platform supports open shortest path first version 2 (OSPFv2) for IPv4 and version 3 (OSPFv3) for IPv6. Up to 16 OSPF instances can be run simultaneously on the MXL Switch.

OSPF is an interior gateway protocol (IGP), which means that it distributes routing information between routers in a single autonomous system (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis.

This chapter is divided into two sections. There is no overlap between the two sets of commands. You cannot use an IPv4 OSPFv2 command in the IPv6 OSPFv3 mode.

- OSPFv2 Commands
- OSPFv3 Commands

Note: Multi-process OSPF is supported on IPV4 OSPFv2 only. It is not supported on IPv6 OSPFv3.

The CLI requires that you include the Process ID when entering ROUTER-OSPF mode. Each command entered applies to the specified OSPFv2 process only.

OSPFv2 Commands

The Dell Networking implementation of OSPFv2 is based on IETF RFC 2328.

area default-cost

Set the metric for the summary default route generated by the area border router (ABR) into the stub area. Use this command on the border routers at the edge of a stub area.

Syntax

```
area area-id default-cost cost
```

To return default values, use the `no area area-id default-cost` command.
area nssa

Specify an area as a not so stubby area (NSSA).

Syntax

area area-id nssa [default-information-originate] [no-redistribution] [no-summary]

Parameters

- **area-id**: Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from 0 and 65535.
- **no-redistribution**: (OPTIONAL) Specify that the redistribute command should not distribute routes into the NSSA. You should only use this command in a NSSA Area Border Router (ABR).
- **default-information-originate**: (OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
- **no-summary**: (OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

Defaults

Not configured

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

area range

Summarize routes matching an address/mask at an area border router (ABR).

Syntax

area area-id range ip-address mask [not-advertise]

Parameters

- **area-id**: Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from 0 and 65535.
- **range**: Specify the address range as a Classless Inter-Domain Routing (CIDR) notation (A.B.C.D/prefix length).

Defaults

Not configured

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
area stub

Configure a stub area, which is an area not connected to other areas.

Syntax

```
area area-id stub [no-summary]
```

To delete a stub area, use the `no area area-id stub` command.

Parameters

- **area-id**: Specify the stub area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
- **no-summary**: (OPTIONAL) Enter the keyword `no-summary` to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.

Defaults

Disabled

Command Modes

ROUTER OSPF

Usage Information

Use this command to configure all routers and access servers within a stub.

Related Commands

- **area stub**: Creates a stub area.
- **router ospf**: Enters the ROUTER OSPF mode to configure an OSPF instance.
**auto-cost**

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

**Syntax**

```
auto-cost [reference-bandwidth ref-bw]
```

To return to the default bandwidth or to assign cost based on the interface type, use the `no auto-cost [reference-bandwidth]` command.

**Parameters**

- `ref-bw` (OPTIONAL) Specify a reference bandwidth in megabits per second.
  - Range: 1 to 4294967
  - Default: 100 megabits per second.

**Defaults**

100 megabits per second.

**Command Modes**

ROUTER OSPF

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**clear ip ospf**

Clear all OSPF routing tables.

**Syntax**

```
clear ip ospf process-id [process]
```

**Parameters**

- `process-id` Enter the OSPF process ID to clear a specific process.
  - If no process id is entered, all OSPF processes are cleared.
- `process` (OPTIONAL) Enter the keyword `process` to reset the OSPF process.

**Command Modes**

EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

Syntax

```
clear ip ospf process-id statistics [interface name {neighbor router-id}]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter the OSPF Process ID to clear statistics for a specific process. If no Process ID is entered, all OSPF processes are cleared.</td>
</tr>
</tbody>
</table>
| interface    | (OPTIONAL) Enter the keyword interface followed by one of the following interface keywords and slot/port or number information:  
|              | • For Port Channel groups, enter the keyword port-channel followed by a number: The range is from 1 to 128.  
|              | • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.  
|              | • For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.  
|              | • For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information. |
| neighbor     | (OPTIONAL) Enter the keyword neighbor followed by the neighbor’s router-id in dotted decimal format (A.B.C.D.). |

Defaults

none

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

```
show ip ospf statistics
```
Displays OSPF statistics.

deploy ip ospf

Display debug information on OSPF. Entering **deploy ip ospf** enables OSPF debugging for the first OSPF process.

Syntax

```
debug ip ospf process-id [bfd | event | packet | spf | database-timer rate-limit]
```

To cancel the debug command, enter **no deploy ip ospf**.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter the OSPF Process ID to debug a specific process. If no Process ID is entered, command applies only to the first OSPF process.</td>
</tr>
<tr>
<td>bfd</td>
<td>(OPTIONAL) Enter the keyword bfd to debug only OSPF BFD information.</td>
</tr>
<tr>
<td>event</td>
<td>(OPTIONAL) Enter the keyword event to debug only OSPF event information.</td>
</tr>
<tr>
<td>packet</td>
<td>(OPTIONAL) Enter the keyword packet to debug only OSPF packet information.</td>
</tr>
<tr>
<td>spf</td>
<td>(OPTIONAL) Enter the keyword spf to display the Shortest Path First information.</td>
</tr>
<tr>
<td>database-timer</td>
<td>(OPTIONAL) Enter the keyword database-timer rate-limit to display the LSA throttling timer information.</td>
</tr>
<tr>
<td>rate-limit</td>
<td></td>
</tr>
</tbody>
</table>
**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 34-1. debug ip ospf process-id packet Command Example**

```plaintext
FTOS#debug ip ospf 1 packet
OSPF process 1, packet debugging is on

FTOS#
08:14:24 : OSPF(100:00): Xmt. v:2 t:1(HELLO) 1:44 rid:192.1.1.1
  aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:TenGig 4/3 dst:224.0.0.5
  netmask:255.255.255.0 pri:1 N-, MC-, E+, T-, hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0
```

**Table 34-1. debug ip ospf process-id packet Output Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:14</td>
<td>Displays the time stamp.</td>
</tr>
<tr>
<td>OSPF</td>
<td>Displays the OSPF process ID: instance ID.</td>
</tr>
<tr>
<td>v:</td>
<td>Displays the OSPF version. FTOS supports version 2 only.</td>
</tr>
<tr>
<td>t:</td>
<td>Displays the type of packet sent:</td>
</tr>
<tr>
<td></td>
<td>• 1 - Hello packet</td>
</tr>
<tr>
<td></td>
<td>• 2 - database description</td>
</tr>
<tr>
<td></td>
<td>• 3 - link state request</td>
</tr>
<tr>
<td></td>
<td>• 4 - link state update</td>
</tr>
<tr>
<td></td>
<td>• 5 - link state acknowledgement</td>
</tr>
<tr>
<td>l:</td>
<td>Displays the packet length.</td>
</tr>
<tr>
<td>rid:</td>
<td>Displays the OSPF router ID.</td>
</tr>
<tr>
<td>aid:</td>
<td>Displays the Autonomous System ID.</td>
</tr>
<tr>
<td>chk:</td>
<td>Displays the OSPF checksum.</td>
</tr>
<tr>
<td>aut:</td>
<td>States if OSPF authentication is configured. One of the following is listed:</td>
</tr>
<tr>
<td></td>
<td>• 0 - no authentication configured</td>
</tr>
<tr>
<td></td>
<td>• 1 - simple authentication configured using the ip ospf authentication-key command)</td>
</tr>
<tr>
<td></td>
<td>• 2 - MD5 authentication configured using the ip ospf message-digest-key command.</td>
</tr>
<tr>
<td>auk:</td>
<td>If the ip ospf authentication-key command is configured, this field displays the key used.</td>
</tr>
<tr>
<td>keyid:</td>
<td>If the ip ospf message-digest-key command is configured, this field displays the MD5 key</td>
</tr>
<tr>
<td>to:</td>
<td>Displays the interface to which the packet is intended.</td>
</tr>
<tr>
<td>dst:</td>
<td>Displays the destination IP address.</td>
</tr>
<tr>
<td>netmask:</td>
<td>Displays the destination IP address mask.</td>
</tr>
<tr>
<td>pri:</td>
<td>Displays the OSPF priority</td>
</tr>
</tbody>
</table>
**default-information originate**

To generate a default external route into an OSPF routing domain, configure FTOS.

**Syntax**

default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]

To return to the default values, use the no default-information originate command.

**Parameters**

- **always** (OPTIONAL) Enter the keyword always to specify that default route information must always be advertised.

- **metric metric-value** (OPTIONAL) Enter the keyword metric followed by a number to configure a metric value for the route. Range: 1 to 16777214

- **metric-type type-value** (OPTIONAL) Enter the keywords metric-type followed by an OSPF link state type of 1 or 2 for default routes. The values are:
  - 1 = Type 1 external route
  - 2 = Type 2 external route.

- **route-map map-name** (OPTIONAL) Enter the keywords route-map followed by the name of an established route map.

**Defaults**

Disabled.

**Command Modes**

ROUTER OSPF

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module.

**Related Commands**

- **redistribute** Redistributes routes from other routing protocols into OSPF.
**default-metric**

Change the metrics of redistributed routes to a value useful to OSPF. Use this command with the `redistribute` command.

**Syntax**

```
default-metric number
```

To return to the default values, use the `no default-metric [number]` command.

**Parameters**

- `number`: Enter a number as the metric. The range is from 1 to 16777214.

**Defaults**

Disabled.

**Command Modes**

ROUTER OSPF

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module.

**Related Commands**

- `redistribute`: Redistributes routes from other routing protocols into OSPF.

---

**description**

Add a description about the selected OSPF configuration.

**Syntax**

```
description description
```

To remove the OSPF description, use the `no description` command.

**Parameters**

- `description`: Enter a text string description to identify the OSPF configuration (80 characters maximum).

**Defaults**

none

**Command Modes**

ROUTER OSPF

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `show ip ospf asbr`: Displays the VLAN configuration.

---

**distance**

Define an administrative distance for particular routes to a specific IP address.

**Syntax**

```
distance weight [ip-address mask access-list-name]
```

To delete the settings, use the `no distance weight [ip-address mask access-list-name]` command.
distance ospf

Configure an OSPF distance metric for different types of routes.

Syntax

distance ospf [external dist3] [inter-area dist2] [intra-area dist1]

Parameters

- **external dist3** (OPTIONAL) Enter the keyword external followed by a number to specify a distance for external type 5 and 7 routes. The range is from 1 to 255. The default is 110.
- **inter-area dist2** (OPTIONAL) Enter the keywords inter-area followed by a number to specify a distance metric for routes between areas. The range is from 1 to 255. The default is 110.
- **intra-area dist1** (OPTIONAL) Enter the keywords intra-area followed by a number to specify a distance metric for all routes within an area. The range is from 1 to 255. The default is 110.

Defaults

external dist3 = 110; inter-area dist2 = 110; intra-area dist1 = 110.

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

To specify a distance for routes learned from other routing domains, use the redistribute command.

distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

Syntax

distribute-list prefix-list-name in [interface]

Parameters

- **prefix-list-name** Name of the IP prefix list.

To delete a filter, use the no distribute-list prefix-list-name in [interface] command.
distribute-list out

Apply a filter to restrict certain routes destined for the local routing table after the SPF calculation.

**Syntax**

```plaintext
distribute-list prefix-list-name out [bgp | connected | isis | rip | static]
```

To remove a filter, use the `no distribute-list prefix-list-name out [bgp | connected | isis | rip | static]` command.

**Parameters**

- **prefix-list-name**
  - Enter the name of a configured prefix list.

- **bgp**
  - (Optional) Enter the keyword `bgp` to specify that BGP routes are distributed.

- **connected**
  - (OPTIONAL) Enter the keyword `connected` to specify that connected routes are distributed.

- **isis**
  - (Optional) Enter the keyword `isis` to specify that IS-IS routes are distributed.

- **rip**
  - (OPTIONAL) Enter the keyword `rip` to specify that RIP routes are distributed.

- **static**
  - (OPTIONAL) Enter the keyword `static` to specify that only manually configured routes are distributed.

**Defaults**

Not configured.

**Command Modes**

- ROUTER OSPF

**Command History**

- **Version 8.3.16.1**
  - Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The `distribute-list out` command applies to routes the autonomous system boundary routers (ASBRs) redistributes into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and inter-area routes.
fast-convergence

This command sets the minimum LSA origination and arrival times to zero (0), allowing more rapid route computation so that convergence takes less time.

Syntax

`fast-convergence {number}`

To cancel fast-convergence, use the `no fast convergence` command.

Parameters

- `number` Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place.
  
  The range is from 1 to 4.

Defaults

None

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The higher this parameter is set, the faster OSPF converge takes place.

Note: The faster the convergence, the more frequent the route calculations and updates. This behavior impacts CPU utilization and may impact adjacency stability in larger topologies.

Generally, convergence level 1 meets most convergence requirements. Higher convergence levels should only be selected following consultation with Dell Networking Technical Support.

flood-2328

Enable RFC 2328 flooding behavior.

Syntax

`flood-2328`

To disable, use the `no flood-2328` command.

Defaults

Disabled

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

In OSPF, flooding is the most resource-consuming task. The flooding algorithm, described in RFC 2328, requires that OSPF flood LSAs (Link State Advertisements) on all interfaces, as governed by LSA's flooding scope (see Section 13 of the RFC). When multiple direct links connect two routers, the RFC 2328 flooding algorithm generates significant redundant information across all links.
By default, FTOS implements an enhanced flooding procedure that dynamically and intelligently determines when to optimize flooding. Whenever possible, the OSPF task attempts to reduce flooding overhead by selectively flooding on a subset of the interfaces between two routers.

When **flood-2328** is enabled, this command configures FTOS to flood LSAs on all interfaces.

### graceful-restart grace-period

Specifies the time duration, in seconds, that the router’s neighbors continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

**Syntax**
```
graceful-restart grace-period seconds
```

To disable the grace period, use the **no graceful-restart grace-period** command.

**Parameters**
- **seconds**
  - Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process. The range is from 40 to 1800 seconds.

**Defaults**
Not Configured

**Command Modes**
- ROUTER OSPF

**Command History**
- Introduced on MXL 10/40GbE Switch IO Module

### graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

**Syntax**
```
graceful-restart helper-reject ip-address
```

To return to default value, enter **no graceful-restart helper-reject**.

**Parameters**
- **ip-address**
  - Enter the OSPF router-id, in IP address format, of the restart router that will not act as a helper during graceful restart.

**Defaults**
Not Configured

**Command Modes**
- ROUTER OSPF

**Command History**
- Introduced on MXL 10/40GbE Switch IO Module

### graceful-restart mode

Enable the graceful restart mode.

**Syntax**
```
graceful-restart mode [planned-only | unplanned-only]
```

**Parameters**
- **planned-only**
- **unplanned-only**
To return to default value, enter the `no graceful-restart mode` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>planned-only</td>
<td>(OPTIONAL) Enter the keywords <code>planned-only</code> to indicate graceful restart is supported in a planned restart condition only.</td>
<td>ROUTER OSPF</td>
<td>Version 9.2(0.0) Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
<tr>
<td>unplanned-only</td>
<td>(OPTIONAL) Enter the keywords <code>unplanned-only</code> to indicate graceful restart is supported in an unplanned restart condition only.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

** graceful-restart role **

Specify the role for your OSPF router during graceful restart.

** Syntax **

```
graceful-restart role [helper-only | restart-only]
```

To return to default value, enter the `no graceful-restart role` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>helper-only</td>
<td>(OPTIONAL) Enter the keywords <code>helper-only</code> to specify the OSPF router is a helper only during graceful restart.</td>
<td>ROUTER OSPF</td>
<td>Version 9.2(0.0) Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
<tr>
<td>restart-only</td>
<td>(OPTIONAL) Enter the keywords <code>restart-only</code> to specify the OSPF router is a restart only during graceful restart.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

** ip ospf auth-change-wait-time **

OSPF provides a grace period while OSPF changes its interface authentication type. During the grace period, OSPF sends out packets with new and old authentication scheme till the grace period expires.

** Syntax **

```
ip ospf auth-change-wait-time seconds
```

To return to the default, use the `no ip ospf auth-change-wait-time` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Enter the seconds. The range is from 0 to 300.</td>
<td>INTERFACE</td>
</tr>
</tbody>
</table>
ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

Syntax

```
ip ospf authentication-key [encryption-type] key
```

To delete an authentication key, use the **no ip ospf authentication-key** command.

Parameters

- **encryption-type** (OPTIONAL) Enter 7 to encrypt the key.
- **key** Enter an eight-character string. Strings longer than eight characters are truncated.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

All neighboring routers in the same network must use the same password to exchange OSPF information.

ip ospf cost

Change the cost associated with the OSPF traffic on an interface.

Syntax

```
ip ospf cost cost
```

To return to default value, use the **no ip ospf cost** command.

Parameters

- **cost** Enter a number as the cost.
  
  Range: 1 to 65535.

Defaults

The default cost is based on the reference bandwidth.

Command Modes

INTERFACE

Usage Information

If this command is not configured, cost is based on the **auto-cost** command.

When you configure OSPF over multiple vendors, use the **ip ospf cost** command to ensure that all routers use the same cost. Otherwise, OSPF routes improperly.

Related Commands

- **auto-cost** Controls how the OSPF interface cost is calculated.
ip ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

**Syntax**

```
ip ospf dead-interval seconds
```

To return to the default values, use the `no ip ospf dead-interval` command.

**Parameters**

- **seconds**
  - Enter the number of seconds for the interval.
  - Range: 1 to 65535. Default: 40 seconds.

**Defaults**

40 seconds

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

By default, the dead interval is four times the default hello-interval.

**Related Commands**

- `ip ospf hello-interval` Sets the time interval between hello packets.

---

ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

**Syntax**

```
ip ospf hello-interval seconds
```

To return to the default value, use the `no ip ospf hello-interval` command.

**Parameters**

- **seconds**
  - Enter a the number of second as the delay between hello packets.
  - Range: 1 to 65535.
  - Default: 10 seconds.

**Defaults**

10 seconds

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The time interval between hello packets must be the same for routers in a network.

**Related Commands**

- `ip ospf dead-interval` Sets the time interval before a router is declared dead.
ip ospf message-digest-key

Enable OSPF MD5 authentication and send an OSPF message digest key on the interface.

Syntax  
```
ip ospf message-digest-key keyid md5 key
```

To delete a key, use the `no ip ospf message-digest-key keyid` command.

Parameters  
```
keyid  Enter a number as the key ID.
Range: 1 to 255.
key    Enter a continuous character string as the password.
```

Defaults  
No MD5 authentication is configured.

Command Modes  
INTERFACE

Command History  
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information  
You can configure a maximum of six digest keys on an interface. Of the available six digest keys, the switches select the MD5 key that is common. The remaining MD5 keys are unused.

To change to a different key on the interface, enable the new key while the old key is still enabled. The FTOS sends two packets: the first packet authenticated with the old key and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, delete the old key. Dell Networking recommends keeping only one key per interface.

**Note:** The MD5 secret is stored as plain text in the configuration file with service password encryption. Write down or otherwise record the key. You cannot learn the key once it is configured. Use caution when changing the key.

ip ospf mtu-ignore

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

Syntax  
```
ip ospf mtu-ignore
```

To return to the default, use the `no ip ospf mtu-ignore` command.

Defaults  
Enabled

Command Modes  
INTERFACE

Command History  
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
ip ospf network

Set the network type for the interface.

Syntax

```nls
ip ospf network {broadcast | point-to-point}
```

To return to the default, use the `no ip ospf network` command.

Parameters

<table>
<thead>
<tr>
<th>broadcast</th>
<th>Enter the keyword <code>broadcast</code> to designate the interface as part of a broadcast network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>point-to-point</td>
<td>Enter the keywords <code>point-to-point</code> to designate the interface as part of a point-to-point network.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ip ospf priority

Set the priority of the interface to determine the designated router for the OSPF network.

Syntax

```nls
ip ospf priority number
```

To return to the default setting, use the `no ip ospf priority` command.

Parameters

| number | Enter a number as the priority. Range: 0 to 255. The default is 1. |

Defaults

1

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Setting a priority of 0 makes the router ineligible for election as a designated router or backup designated router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.
ip ospf retransmit-interval

Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

Syntax

    ip ospf retransmit-interval seconds

Parameters

- **seconds**: Enter the number of seconds as the interval between retransmission.
  - Range: 1 to 3600.
  - Default: 5 seconds.
  - This interval must be greater than the expected round-trip time for a packet to travel between two routers.

Defaults

5 seconds

Command Modes

INTERFACE

Command History

- **Version 8.3.16.1**: Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval must be larger for interfaces connected to virtual links.

ip ospf transmit-delay

To send a link state update packet on the interface, set the estimated time elapsed.

Syntax

    ip ospf transmit-delay seconds

Parameters

- **seconds**: Enter the number of seconds as the transmission time. This value should be greater than the transmission and propagation delays for the interface.
  - Range: 1 to 3600.
  - Default: 1 second.

Defaults

1 second

Command Modes

INTERFACE

Command History

- **Version 8.3.16.1**: Introduced on MXL 10/40GbE Switch IO Module
log-adjacency-changes

To send a Syslog message about changes in the OSPF adjacency state, set FTOS.

Syntax  
log-adjacency-changes

To disable the Syslog messages, use the no log-adjacency-changes command.

Defaults  
Disabled.

Command Mode  
ROUTER OSPF

Command History  
Version 8.3.16.1  Introduced on MXP 10/40GbE Switch IO Module

maximum-paths

To forward packets over multiple paths, enable the software.

Syntax  
maximum-paths number

To disable packet-forwarding over multiple paths, use the no maximum-paths command.

Parameters  

<table>
<thead>
<tr>
<th>number</th>
<th>Specify the number of paths.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The range for OSPFv2 is from 1 to 16. The default for OSPFv2 is 4 paths.</td>
</tr>
<tr>
<td></td>
<td>The range for OSPFv3 is from 1 to 64. The default for OSPFv3 is 8 paths.</td>
</tr>
</tbody>
</table>

Defaults  
4

Command Modes  
ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History  
Version 9.2(0.0)  Added support for OSPFv3.

Version 8.3.16.1  Introduced on MXP 10/40GbE Switch IO Module

mib-binding

Enable this OSPF process ID to manage the SNMP traps and process SNMP queries.

Syntax  
mib-binding

To mib-binding on this OSPF process, use the no mib-binding command.

Defaults  
none

Command Modes  
ROUTER OSPF

Command History  
Version 8.3.16.1  Introduced on MXP 10/40GbE Switch IO Module
Usage Information
This command is either enabled or disabled. If no OSPF process is identified as the MIB manager, the first OSPF process is used.

If an OSPF process has been selected, it must be disabled prior to assigning new process ID the MIB responsibility.

network area
Define which interfaces run OSPF and the OSPF area for those interfaces.

Syntax
```
network ip-address mask area area-id
```

To disable an OSPF area, use the `no network ip-address mask area area-id` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>Enter a network mask in /prefix format. (/x)</td>
</tr>
<tr>
<td><code>area-id</code></td>
<td>Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range: 0 to 65535. IP address format: dotted decimal format A.B.C.D. Note: If the area ID is smaller than 65535, it is converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it is converted to 1.</td>
</tr>
</tbody>
</table>

Command Modes

- ROUTER OSPF

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

To enable OSPF on an interface, the `network area` command must include, in its range of addresses, the primary IP address of an interface.

Note: An interface can be attached only to a single OSPF area.

If you delete all the `network area` commands for Area 0, the `show ip ospf` command output does not list Area 0.

passive-interface
Suppress both receiving and sending routing updates on an interface.

Syntax
```
passive-interface {default | interface}
```

To enable both the receiving and sending routing, enter the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, enter the `no passive-interface default` command.
Although the passive interface does not send or receive routing updates, the network on that interface is still included in OSPF updates sent via other interfaces.

The **default** keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the **no passive-interface interface** command. The **no** form of this command is inserted into the configuration for individual interfaces when the **no passive-interface interface** command is issued while **passive-interface default** is configured.

This command behavior has changed as follows:

**passive-interface interface**

- The previous **no passive-interface interface** is removed from the running configuration.
- The ABR status for the router is updated.
- Save **passive-interface interface** into the running configuration.

**passive-interface default**

- All present and future OSPF interface are marked as **passive**.
- Any adjacency are explicitly terminated from all OSPF interfaces.
- All previous **passive-interface interface** commands are removed from the running configuration.
- All previous **no passive-interface interface** commands are removed from the running configuration.

**no passive-interface interface**

- Remove the interface from the passive list.
- The ABR status for the router is updated.
- If **passive-interface default** is specified, then save **no passive-interface interface** into the running configuration.

**no passive-interface default**

- Clear everything and revert to the default behavior.
all previously marked passive interfaces are removed.
- May update ABR status.

redistribute

Redistribute information from another routing protocol throughout the OSPF process.

Syntax

redistribute {connected | rip | ospf | static} [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]

Parameters

- **connected**: Enter the keyword connected to specify that information from active routes on interfaces is redistributed.
- **rip**: Enter the keyword rip to specify that RIP routing information is redistributed.
- **ospf**: Enter the keyword ospf to specify that RIP routing information is redistributed.
- **static**: Enter the keyword static to specify that information from static routes is redistributed.
- **metric metric-value** (OPTIONAL): Enter the keyword metric followed by a number.
  Range: 0 (zero) to 16777214.
- **metric-type type-value** (OPTIONAL): Enter the keywords metric-type followed by one of the following:
  - 1 = OSPF External type 1
  - 2 = OSPF External type 2
- **route-map map-name** (OPTIONAL): Enter the keywords route-map followed by the name of the route map.
- **tag tag-value** (OPTIONAL): Enter the keyword tag followed by a number.
  Range: 0 to 4294967295

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

To redistribute the default route (0.0.0.0/0), configure the default-information originate command.

Related Commands

- default-information originate: Generates a default route into the OSPF routing domain.
**redistribute bgp**

Redistribute BGP routing information throughout the OSPF instance.

**Syntax**

```
redistribute bgp as number [metric metric-value | metric-type type-value] [tag tag-value]
```

To disable redistribution, use the `no redistribute bgp as number [metric metric-value | metric-type type-value] [tag tag-value]` command.

**Parameters**

- `as number` Enter the autonomous system number. The range is from 1 to 65535.
- `metric metric-value` (OPTIONAL) Enter the keyword `metric` followed by a number. The range is from 0 (zero) to 16777214.
- `metric-type type-value` (OPTIONAL) Enter the keywords `metric-type` followed by one of the following:
  - `1` = OSPF External type 1
  - `2` = OSPF External type 2
- `tag tag-value` (OPTIONAL) Enter the keyword `tag` followed by a number. The range is from 0 to 4294967295.

**Defaults**
Not configured.

**Command Modes**
ROUTER OSPF

**Command History**

- Version 9.2(0.0) Introduced on MXL 10/40GbE Switch IO Module

**redistribute isis**

Redistribute IS-IS routing information throughout the OSPF instance.

**Syntax**

```
redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]
```

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]` command.

**Parameters**

- `tag` (OPTIONAL) Enter the name of the IS-IS routing process
- `level-1` (OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.
- `level-1-2` (OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.
- `level-2` (OPTIONAL) Enter the keywords `level-2` to redistribute only IS-IS Level-2 routes.
- `metric metric-value` (OPTIONAL) Enter the keyword `metric` followed by a number. The range is from 0 (zero) to 4294967295.
- `metric-type type-value` (OPTIONAL) Enter the keywords `metric-type` followed by one of the following:
  - `1` = OSPF External type 1
  - `2` = OSPF External type 2
- `route-map map-name` (OPTIONAL) Enter the name of the IS-IS routing process
- `tag tag-value` (OPTIONAL) Enter the keyword `tag` followed by a number. The range is from 0 to 4294967295.
router-id

Use this command to configure a fixed router ID.

Syntax
  router-id ip-address

To remove the fixed router ID, use the no router-id ip-address command.

Parameters
  ip-address  Enter the router ID in the IP address format.

Defaults
  none

Command Modes
  ROUTER OSPF

Command History
  Version 9.2(0.0)    Introduced on MXL 10/40GbE Switch IO Module
  Version 8.3.16.1    Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 34-2.  router-id Command Example

FTOS(conf)#router ospf 100
FTOS(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/n]:

FTOS(conf-router_ospf)#show config
!  router ospf 100
  router-id 1.1.1.1
FTOS(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/n]:
FTOS#

Usage Information
  You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If you use this command on an OSPF router process which is already active (that is, has neighbors), a prompt displays reminding you that changing router-id brings down the existing OSPF adjacency. The new router ID is effective at the next reload.
router ospf

To configure an OSPF instance, enter the ROUTER OSPF mode.

Syntax  

```
router ospf process-id
```

To clear an OSPF instance, use the `no router ospf process-id` command.

Parameters

```
process-id  Enter a number for the OSPF instance.
Range: 1 to 65535.
```

Defaults  Not configured.

Command Modes  

**CONFIGURATION**

Command History

```
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module
```

Example

```
Figure 34-3.  router ospf Command Example

FTOS(conf)#router ospf 2
FTOS(conf-router_ospf)#
```

Usage Information

You must have an IP address assigned to an interface to enter the ROUTER OSPF mode and configure OSPF.

show config

Display the non-default values in the current OSPF configuration.

Syntax  

```
show config
```

Command Modes  

**ROUTER OSPF**

Command History

```
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module
```

Example

```
Figure 34-4.  show config Command Example

FTOS(conf-router_ospf)#show config
! router ospf 1
FTOS(conf-router_ospf-1)#
```

show ip ospf

Display information on the OSPF process configured on the switch.

Syntax  

```
show ip ospf process-id
```
**Parameters**

- **process-id**
  - Enter the OSPF process ID to show a specific process.
  - If no process ID is entered, command applies only to the first OSPF process.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1
- Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

The following describes the `show ip ospf` command shown in the following example.

<table>
<thead>
<tr>
<th>Line Beginning With</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Routing Process...”</td>
<td>Displays the OSPF process ID and the IP address associated with the process ID.</td>
</tr>
<tr>
<td>“Supports only...”</td>
<td>Displays the number of Type of Service (TOS) routes supported.</td>
</tr>
<tr>
<td>“SPF schedule...”</td>
<td>Displays the delay and hold time configured for this process ID.</td>
</tr>
<tr>
<td>“Convergence Level”</td>
<td>Displays the intervals set for LSA transmission and acceptance.</td>
</tr>
<tr>
<td>“Min LSA...”</td>
<td>Displays the number and type of areas configured for this process ID.</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS#show ip ospf 10
Routing Process ospf 10 with ID 1.1.1.1 Virtual router default-vrf
Supports only single TOS (TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
  Area BACKBONE (0)
    Number of interface in this area is 1
    SPF algorithm executed 205 times
    Area ranges are

FTOS#
```

**Related Commands**

- `show ip ospf database` - Displays information about the OSPF routes configured.
- `show ip ospf interface` - Displays the OSPF interfaces configured.
- `show ip ospf neighbor` - Displays the OSPF neighbors configured.

**show ip ospf asbr**

Display all autonomous system boundary router (ASBR) routers visible to OSPF.

**Syntax**

```
show ip ospf process-id asbr
```

**Parameters**

- **process-id**
  - Enter the OSPF process ID to show a specific process.
  - If no process ID is entered, command applies only to the first OSPF process.

**Defaults**

None
To isolate problems with external routes, use this command. In OSPF, external routes are calculated by adding the LSA cost to the cost of reaching the ASBR router. If an external route does not have the correct cost, use this command to determine if the path to the originating router is correct. The display output is not sorted in any order.

**Note:** ASBRs that are not in directly connected areas are also displayed.

You can determine if an ASBR is in a directly connected area (or not) by the flags. For ASBRs in a directly connected area, E flags are set. In the following example, router 1.1.1.1 is in a directly connected area since the Flag is E/-/-/. For remote ASBRs, the E flag is clear (-/-/-).

```
FTOS#show ip ospf 1 asbr
RouterID         Flags    Cost   Nexthop         Interface    Area
3.3.3.3          -/-/-/   2      10.0.0.2        TenGig 0/1        1
1.1.1.1          E/-/-/   0      0.0.0.0         -             0 FTOS#
```

**show ip ospf database**

Display all LSA information. If you do enable OSPF on the switch, no output is generated.

**Syntax**

```plain
show ip ospf process-id database [database-summary]
```

**Parameters**

- `process-id` Enter the OSPF process ID to show a specific process. If no process ID is entered, command applies only to the first OSPF process.
- `database-summary` (OPTIONAL) Enter the keywords `database-summary` to display the number of LSA types in each area and the total number of LSAs.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The following describes the `show ip ospf process-id database` command shown in the following example.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Identifies the router ID.</td>
</tr>
<tr>
<td>ADV Router</td>
<td>Identifies the advertising router’s ID.</td>
</tr>
<tr>
<td>Age</td>
<td>Displays the link state age.</td>
</tr>
<tr>
<td>Seq#</td>
<td>Identifies the link state sequence number. This number enables you to identify old or duplicate link state advertisements.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA’s complete contents.</td>
</tr>
<tr>
<td>Link count</td>
<td>Displays the number of interfaces for that router.</td>
</tr>
</tbody>
</table>

Example

```
FTOS>show ip ospf 1 database
OSPF Router with ID (11.1.2.1) (Process ID 1)
Router (Area 0.0.0.0)
Link ID         ADV Router        Age     Seq#          Checksum    Link count
11.1.2.1        11.1.2.1          673     0x80000005    0x707e          2
13.1.1.1        13.1.1.1          676     0x80000097    0x1035          2
192.68.135.2    192.68.135.2      1419    0x80000294    0x9cb6          1

Network (Area 0.0.0.0)
Link ID         ADV Router        Age     Seq#          Checksum    Link count
10.2.3.2        13.1.1.1          676     0x80000003    0x6592          
10.2.4.2        192.68.135.2      908     0x80000055    0x683e          

Type-5 AS External
Link ID         ADV Router        Age     Seq#          Checksum Tag
0.0.0.0         192.68.135.2      908     0x80000052    0xeb83    100
1.1.1.1         192.68.135.2      908     0x8000002a    0xbd27     0
10.1.1.0        11.1.2.1          718     0x80000002    0x9012     0
10.1.2.0        11.1.2.1          718     0x80000002    0x851c     0
10.2.2.0        11.1.2.1          718     0x80000002    0x7927     0
10.2.3.0        11.1.2.1          718     0x80000002    0xe631     0
10.2.4.0        13.1.1.1          1184    0x80000068    0x45db     0
11.1.1.0        11.1.2.1          718     0x80000002    0x831e     0
11.1.2.0        11.1.2.1          718     0x80000002    0x7828     0
12.1.2.0        192.68.135.2      1663    0x80000054    0xdbd6     0
13.1.1.0        13.1.1.1          1192    0x8000006b    0x2718     0
13.1.2.0        13.1.1.1          1184    0x8000006b    0xc222     0
172.16.1.0      13.1.1.1          148     0x8000006b    0x533b     0
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf database asbr-summary</td>
<td>Displays only ASBR summary LSA information.</td>
</tr>
</tbody>
</table>

**show ip ospf database asbr-summary**

Display information about AS Boundary LSAs.

**Syntax**

```
show ip ospf process-id database asbr-summary [link-state-id] [adv-router ip-address]
```
The following describes the `show ip ospf database asbr-summary` command shown in the following example.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA’s age.</td>
</tr>
</tbody>
</table>
| Options            | Displays the optional capabilities available on router. The following options can be found in this item:  
  • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.  
  • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.  
  • E or No E is displayed on whether the originating router can accept AS External LSAs. |
| LS Type            | Displays the LSA’s type. |
| Link State ID      | Displays the Link State ID. |
| Advertising Router | Identifies the advertising router’s ID. |
| Checksum           | Displays the Fletcher checksum of the an LSA’s complete contents. |
| Length             | Displays the length in bytes of the LSA. |
| Network Mask       | Displays the network mask implemented on the area. |
| TOS                | Displays the Type of Service (TOS) options. Option 0 is the only option. |
| Metric             | Displays the LSA metric. |
Example

Figure 34-5. show ip ospf database asbr-summary Command Example (Partial)

FTOS#show ip ospf 100 database asbr-summary
   OSPF Router with ID (1.1.1.10) (Process ID 100)
       Summary Asbr (Area 0.0.0.0)
       LS age: 1437
       Options: (No TOS-capability, No DC, E)
       Link State ID: 103.1.50.1
       Advertising Router: 1.1.1.10
       LS Seq Number: 0x8000000f
       Checksum: 0x8221
       Length: 28
       Network Mask: /0
       TOS: 0 Metric: 2

       LS age: 473
       Options: (No TOS-capability, No DC, E)
       LS type: Summary Asbr
       Link State ID: 104.1.50.1
       Advertising Router: 1.1.1.10
       LS Seq Number: 0x80000010
       Checksum: 0x4198
       Length: 28
       --More--

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf database</td>
<td>Displays OSPF database information.</td>
</tr>
</tbody>
</table>

show ip ospf database external

Display information on the AS external (Type 5) LSAs.

Syntax

show ip ospf process-id database external [link-state-id] [adv-router ip-address]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter the OSPF process ID to show a specific process. If no process ID is entered, command applies only to the first OSPF process.</td>
</tr>
<tr>
<td>link-state-id</td>
<td>(OPTIONAL) Specify the LSA ID in dotted decimal format. The LSA ID value depends on the LSA type and can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• the network’s IP address for Type 3 LSAs or Type 5 LSAs</td>
</tr>
<tr>
<td></td>
<td>• the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs</td>
</tr>
<tr>
<td></td>
<td>• the default destination (0.0.0.0) for Type 5 LSAs</td>
</tr>
<tr>
<td>adv-router ip-address</td>
<td>(OPTIONAL) Enter the keywords adv-router and the ip-address to display only the LSA information about that router.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Usage Information

The following describes the `show ip ospf process-id database` external command shown in the following example.

**Table 34-4. show ip ospf process-id database external Command Description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>• E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA's type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the router ID of the LSA's originating router.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA's complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Displays the network mask implemented on the area.</td>
</tr>
<tr>
<td>Metrics Type</td>
<td>Displays the external type.</td>
</tr>
<tr>
<td>TOS</td>
<td>Displays the TOS options. Option 0 is the only option.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Displays the LSA metric.</td>
</tr>
<tr>
<td>Forward Address</td>
<td>Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.</td>
</tr>
<tr>
<td>External Route Tag</td>
<td>Displays the 32-bit field attached to each external route. This field is not used by the OSPF protocol, but can be used for external route management.</td>
</tr>
</tbody>
</table>
Example

FTOS#show ip ospf 1 database external

OSPF Router with ID (20.20.20.5) (Process ID 1)

    Type-5 AS External
        LS age: 612
        Options: (No TOS-capability, No DC, E)
        LS type: Type-5 AS External
        Link State ID: 12.12.12.2
        Advertising Router: 20.31.3.1
        LS Seq Number: 0x80000007
        Checksum: 0x4cde
        Length: 36
        Network Mask: /32
            Metrics Type: 2
            TOS: 0
            Metrics: 25
            Forward Address: 0.0.0.0
            External Route Tag: 43

        LS age: 1868
        Options: (No TOS-capability, DC)
        LS type: Type-5 AS External
        Link State ID: 24.216.12.0
        Advertising Router: 20.20.20.8
        LS Seq Number: 0x80000005
        Checksum: 0xa00e
        Length: 36
        Network Mask: /24
            Metrics Type: 2
            TOS: 0
            Metrics: 1
            Forward Address: 0.0.0.0
            External Route Tag: 701

FTOS#

Related Commands

show ip ospf database
Displays OSPF database information.

show ip ospf database network
Display the network (Type 2) LSA information.

Syntax

show ip ospf process-id database network [link-state-id] [adv-router ip-address]

Parameters

process-id
Enter the OSPF process ID to show a specific process. If no process ID is entered, command applies only to the first OSPF process.

link-state-id
(Optional) Specify the LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
- the network’s IP address for Type 3 LSAs or Type 5 LSAs
- the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router
ip-address
(Optional) Enter the keywords adv-router and the ip-address to display only the LSA information about that router.

Command Modes

EXEC

EXEC Privilege
Figure 34-6.  show ip ospf process-id database network Command Example

FTOS#show ip ospf 1 data network

    OSPF Router with ID (20.20.20.5) (Process ID 1)
           Network (Area 0.0.0.0)
                 LS age: 1372
                 Options: (No TOS-capability, DC, E)
                 LS type: Network
                 Link State ID: 202.10.10.2
                 Advertising Router: 20.20.20.8
                 LS Seq Number: 0x80000006
                 Checksum: 0xa35
                 Length: 36
                 Network Mask: /24
                   Attached Router: 20.20.20.8
                   Attached Router: 20.20.20.9
                   Attached Router: 20.20.20.7

           Network (Area 0.0.0.1)
                 LS age: 252
                 Options: (TOS-capability, No DC, E)
                 LS type: Network
                 Link State ID: 192.10.10.2
                 Advertising Router: 192.10.10.2
                 LS Seq Number: 0x80000007
                 Checksum: 0x4309
                 Length: 36
                 Network Mask: /24
                   Attached Router: 192.10.10.2
                   Attached Router: 20.20.20.1
                   Attached Router: 20.20.20.5

FTOS#

Table 34-5.  show ip ospf process-id database network Command Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>• E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA's type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the router ID of the LSA’s originating router.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the Fletcher checksum of an LSA’s complete contents.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Attached Router</td>
<td>Identifies the IP address of routers attached to the network.</td>
</tr>
</tbody>
</table>
show ip ospf database nssa-external
Display NSSA-External (Type 7) LSA information.
Syntax: show ip ospf database nssa-external [link-state-id] [adv-router ip-address]
Parameters:
- link-state-id: (OPTIONAL) Specify the LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- adv-router ip-address: (OPTIONAL) Enter the keywords adv-router and the ip-address to display only the LSA information about that router.

Command Modes:
EXEC
EXEC Privilege

Command History:
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands:
show ip ospf database opaque-area
Display the opaque-area (Type 10) LSA information.
Syntax: show ip ospf process-id database opaque-area [link-state-id] [adv-router ip-address]
Parameters:
- process-id: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- link-state-id: (OPTIONAL) Specify the LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- adv-router ip-address: (OPTIONAL) Enter the keywords adv-router and the ip-address to display only the LSA information about that router.

Command Modes:
EXEC
EXEC Privilege

Command History:
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example

FTOS>show ip ospf 1 database opaque-area

OSPF Router with ID (3.3.3.3) (Process ID 1)
Type-10 Opaque Link Area (Area 0)

LS age: 1133
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.1
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000416
Checksum: 0x376
Length: 28
Opaque Type: 1
Opaque ID: 1
Unable to display opaque data

LS age: 833
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.2
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000002
Checksum: 0x19c2
--More--

show ip ospf database opaque-area

Table 34-6. show ip ospf process-id database opaque-area Command Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA’s age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following</td>
</tr>
<tr>
<td></td>
<td>options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>• TOS-capability or No TOS-capability is displayed depending on</td>
</tr>
<tr>
<td></td>
<td>whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>• DC or No DC is displayed depending on whether the originating router</td>
</tr>
<tr>
<td></td>
<td>can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>• E or No E is displayed on whether the originating router can accept AS</td>
</tr>
<tr>
<td></td>
<td>External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA’s type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the advertising router’s ID.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of the an LSA’s complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Opaque Type</td>
<td>Displays the Opaque type field (the first 8 bits of the Link State ID).</td>
</tr>
<tr>
<td>Opaque ID</td>
<td>Displays the Opaque type-specific ID (the remaining 24 bits of the Link</td>
</tr>
<tr>
<td></td>
<td>State ID).</td>
</tr>
</tbody>
</table>

Related Commands

show ip ospf database  Displays OSPF database information.

show ip ospf process-id database opaque-as [link-state-id] [adv-router ip-address]

Display the opaque-as (Type 11) LSA information.

Syntax
### show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

**Syntax**

```
show ip ospf process-id database opaque-link [link-state-id] [adv-router ip-address]
```

**Parameters**

- **process-id**: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- **link-state-id**: (OPTIONAL) Specify the LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- **adv-router ip-address**: (OPTIONAL) Enter the keywords `adv-router` and the IP address to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `show ip ospf database`: Displays OSPF database information.
show ip ospf database router

Display the router (Type 1) LSA information.

**Syntax**

```
show ip ospf process-id database router [link-state-id] [adv-router ip-address]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>process-id</strong></td>
<td>Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.</td>
</tr>
<tr>
<td><strong>link-state-id</strong></td>
<td>(OPTIONAL) Specify the LSA ID in dotted decimal format. The LSA ID value depends on the LSA type and can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- the network’s IP address for Type 3 LSAs or Type 5 LSAs</td>
</tr>
<tr>
<td></td>
<td>- the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs</td>
</tr>
<tr>
<td></td>
<td>- the default destination (0.0.0.0) for Type 5 LSAs</td>
</tr>
<tr>
<td><strong>adv-router</strong></td>
<td>(OPTIONAL) Enter the keywords <strong>adv-router</strong> and the <strong>ip-address</strong> to display only the LSA information about that router.</td>
</tr>
<tr>
<td><strong>ip-address</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example

Figure 34-7. show ip ospf process-id database router Command Example (Partial)

```
FTOS#show ip ospf 100 database router
    OSPF Router with ID (1.1.1.10) (Process ID 100)
          Router (Area 0)
        LS age: 967
        Options: (No TOS-capability, No DC, E)
        LS type: Router
        Link State ID: 1.1.1.10
        Advertising Router: 1.1.1.10
        LS Seq Number: 0x8000012f
        Checksum: 0x3357
        Length: 144
        AS Boundary Router
        Area Border Router
        Number of Links: 10

        Link connected to: a Transit Network
              (Link ID) Designated Router address: 192.68.129.1
              (Link Data) Router Interface address: 192.68.129.1
              Number of TOS metric: 0
              TOS 0 Metric: 1

        Link connected to: a Transit Network
              (Link ID) Designated Router address: 192.68.130.1
              (Link Data) Router Interface address: 192.68.130.1
              Number of TOS metric: 0
              TOS 0 Metric: 1

        Link connected to: a Transit Network
              (Link ID) Designated Router address: 192.68.142.2
              (Link Data) Router Interface address: 192.68.142.2
              Number of TOS metric: 0
              TOS 0 Metric: 1

        Link connected to: a Transit Network
              (Link ID) Designated Router address: 192.68.141.2
              (Link Data) Router Interface address: 192.68.141.2
              Number of TOS metric: 0
              TOS 0 Metric: 1

        Link connected to: a Transit Network
              (Link ID) Designated Router address: 192.68.140.2
              (Link Data) Router Interface address: 192.68.140.2
              Number of TOS metric: 0
              TOS 0 Metric: 1

        Link connected to: a Stub Network
              (Link ID) Network/subnet number: 11.1.5.0
```

--More--

Table 34-7. show ip ospf process-id database router Command Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>• E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the router ID of the LSA’s originating router.</td>
</tr>
</tbody>
</table>
Table 34-7.  show ip ospf process-id database router Command Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Seq Number</td>
<td>Displays the link state sequence number. This number detects duplicate or old LSAs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA’s complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Number of Links</td>
<td>Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.</td>
</tr>
<tr>
<td>Link connected to:</td>
<td>Identifies the type of network to which the router is connected.</td>
</tr>
<tr>
<td>(Link ID)</td>
<td>Identifies the link type and address.</td>
</tr>
<tr>
<td>(Link Data)</td>
<td>Identifies the router interface address.</td>
</tr>
<tr>
<td>Number of TOS Metric</td>
<td>Lists the number of TOS metrics.</td>
</tr>
<tr>
<td>TOS 0 Metric</td>
<td>Lists the number of TOS 0 metrics.</td>
</tr>
</tbody>
</table>

show ip ospf database summary
Display the network summary (Type 3) LSA routing information.

Syntax
```
show ip ospf process-id database summary [link-state-id] [adv-router ip-address]
```

Parameters
- **process-id**: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- **link-state-id**: (OPTIONAL) Specify the LSA ID in dotted decimal format. The LSA ID value depends on the LSA type and can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- **adv-router ip-address**: (OPTIONAL) Enter the keywords adv-router and the ip-address to display only the LSA information about that router.

Command Modes
- EXEC
- EXEC Privilege

Command History
- Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module
Table 34-8. show ip ospf process-id database summary Command Description

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>• E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA's type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the router ID of the LSA's originating router.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA's complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Displays the network mask implemented on the area.</td>
</tr>
</tbody>
</table>
show ip ospf interface

Display the OSPF interfaces configured. If OSPF is not enabled on the switch, no output is generated.

Syntax

```
show ip ospf process-id interface [interface]
```

Parameters

- **process-id**
  - Enter the OSPF Process ID to show a specific process.
  - If no Process ID is entered, command applies only to the first OSPF process.

- **interface**
  - (OPTIONAL) Enter the following keywords and slot/port or number information:
    - For the null interface, enter the keyword `null` then zero (0).
    - For loopback interfaces, enter the keyword `loopback` then a number from 0 to 16383.
    - For Port Channel groups, enter the keywords `port-channel` then a number:
      - The range is from 1 to 128.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
    - For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- `show ip ospf database` Displays OSPF database information.

### Table 34-8. show ip ospf process-id database summary Command Description

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOS</td>
<td>Displays the TOS options. Option 0 is the only option.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the LSA metrics.</td>
</tr>
</tbody>
</table>
show ip ospf neighbor

Display the OSPF neighbors connected to the local router.
**Syntax**

`show ip ospf process-id neighbor`

**Parameters**

- `process-id` Enter the OSPF Process ID to show a specific process.
  If no Process ID is entered, command applies only to the first OSPF process.

**Command Modes**

- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

Figure 34-10. `show ip ospf process-id neighbor` Command Example

```bash
FTOS#show ip ospf 34 neighbor
Neighbor ID Pri State       Dead Time Address      Interface Area
20.20.20.7 1 FULL/DR     00:00:32 182.10.10.3 TenGig 0/0 0.0.0.2
192.10.10.2 1 FULL/DR     00:00:37 192.10.10.2 TenGig 0/1 0.0.0.1
20.20.20.1 1 FULL/DROTHER 00:00:36 192.10.10.4 TenGig 0/1 0.0.0.1
FTOS#
```

Table 34-10. `show ip ospf process-id neighbor` Command Description

<table>
<thead>
<tr>
<th>Row Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor ID</td>
<td>Displays the neighbor router ID.</td>
</tr>
<tr>
<td>Pri</td>
<td>Displays the priority assigned neighbor.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the OSPF state of the neighbor.</td>
</tr>
<tr>
<td>Dead Time</td>
<td>Displays the expected time until FTOS declares the neighbor dead.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the IP address of the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the interface type slot/port information.</td>
</tr>
<tr>
<td>Area</td>
<td>Displays the neighbor’s area (process ID).</td>
</tr>
</tbody>
</table>

**show ip ospf routes**

Display routes OSPF calculates and stores in OSPF RIB.

**Syntax**

`show ip ospf process-id routes`

**Parameters**

- `process-id` Enter the OSPF Process ID to show a specific process.
  If no Process ID is entered, command applies only to the first OSPF process.

**Defaults**

- `none`

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
This command is useful in isolating routing problems between OSPF and the RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, then the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, Type 1 cost is not displayed.

**Example**

```
Figure 34-11.  show ip ospf process-id routes Command Example

FTOS#show ip ospf 100 route
Prefix            Cost   Nexthop         Interface    Area       Type
1.1.1.1           1       0.0.0.0            Lo 0        0       Intra-Area
3.3.3.3           2      13.0.0.3          TenGig 0/47       1       Intra-Area
13.0.0.0          1       0.0.0.0          TenGig 0/47       0       Intra-Area
150.150.150.0     2      13.0.0.3          TenGig 0/47       -       External
172.30.1.0        2      13.0.0.3          TenGig 0/47       1       Intra-Area
FTOS#
```

**show ip ospf statistics**

Display OSPF statistics.

**Syntax**

```
show ip ospf process-id statistics global | [interface name {neighbor router-id}]
```

**Parameters**

- `process-id` Enter the OSPF Process ID to show a specific process.
  - If no Process ID is entered, command applies only to the first OSPF process.
- `global` Enter the keyword `global` to display the packet counts received on all running OSPF interfaces and packet counts received and transmitted by all OSPF neighbors.
- `interface name` (OPTIONAL) Enter the keyword `interface` followed by one of the following interface keywords and slot/port or number information:
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
  - For port channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
- `neighbor router-id` (OPTIONAL) Enter the keyword `neighbor` then the neighbor’s router-id in dotted decimal format (A.B.C.D.).

**Defaults**

- `none`

**Command Modes**

- EXEC

- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example

Figure 34-12.  show ip ospf process-id statistics global Command Example

FTOS#show ip ospf 10 statistics global

<table>
<thead>
<tr>
<th>OSPF Packet Count</th>
<th>Total</th>
<th>Error</th>
<th>Hello</th>
<th>DDiscr</th>
<th>LSReq</th>
<th>LSUpd</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSAck RX</td>
<td>34</td>
<td>0</td>
<td>26</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>TX</td>
<td>34</td>
<td>0</td>
<td>25</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OSPF Global Queue Length</th>
<th>TxQ-Len</th>
<th>RxQ-Len</th>
<th>Tx-Mark</th>
<th>Rx-Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello-Q</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>LSR-Q</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Other-Q</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error packets (Receive statistics)</th>
<th>Intf-Down</th>
<th>Non-Dr</th>
<th>Self-Org</th>
<th>Nbr-State</th>
<th>Wrong-Len</th>
<th>Invl-Nbr</th>
<th>Nbr-State</th>
<th>Auth-Err</th>
<th>MD5-Err</th>
<th>Chksum</th>
<th>Conf-Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf-Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wrong-Len</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Auth-Err</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Version</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>No-Buffer</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q-Overflow</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error packets (Transmit statistics)</th>
<th>Socket Errors</th>
<th>RtidZero</th>
</tr>
</thead>
<tbody>
<tr>
<td>Socket Errors</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

FTOS#

Table 34-11.  show ip ospf statistics process-id global Command Descriptions

<table>
<thead>
<tr>
<th>Row Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Displays the total number of packets received/transmitted by the OSPF process</td>
</tr>
<tr>
<td>Error</td>
<td>Displays the error count while receiving and transmitting packets by the OSPF process</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of OSPF Hello packets</td>
</tr>
<tr>
<td>DDiscr</td>
<td>Number of database description packets</td>
</tr>
<tr>
<td>LSReq</td>
<td>Number of link state request packets</td>
</tr>
<tr>
<td>LSUpd</td>
<td>Number of link state update packets</td>
</tr>
<tr>
<td>LSAck</td>
<td>Number of link state acknowledgement packets</td>
</tr>
<tr>
<td>TxQ-Len</td>
<td>The transmission queue length</td>
</tr>
<tr>
<td>RxQ-Len</td>
<td>The reception queue length</td>
</tr>
<tr>
<td>Tx-Mark</td>
<td>The highest number mark in the transmission queue</td>
</tr>
<tr>
<td>Rx-Mark</td>
<td>The highest number mark in the reception queue</td>
</tr>
<tr>
<td>Hello-Q</td>
<td>The queue, for transmission or reception, for the hello packets</td>
</tr>
<tr>
<td>LSR-Q</td>
<td>The queue, for transmission or reception, for the link state request packets.</td>
</tr>
<tr>
<td>Other-Q</td>
<td>The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.</td>
</tr>
</tbody>
</table>
**Table 34-12. show ip ospf statistics process-id global Error Descriptions**

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf_Down</td>
<td>Received packets on an interface that is either down or OSPF is not enabled.</td>
</tr>
<tr>
<td>Non-Dr</td>
<td>Received packets with a destination address of ALL_DRS even though SELF is not a designated router</td>
</tr>
<tr>
<td>Self-Org</td>
<td>Receive the self originated packet</td>
</tr>
<tr>
<td>Wrong_Len</td>
<td>The received packet length is different to what was indicated in the OSPF header</td>
</tr>
<tr>
<td>Invld-Nbr</td>
<td>LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer</td>
</tr>
<tr>
<td>Nbr-State</td>
<td>LSA, LSR, and LSU are received from a neighbor with stats less than the loading state</td>
</tr>
<tr>
<td>Auth-Error</td>
<td>Simple authentication error</td>
</tr>
<tr>
<td>MD5-Error</td>
<td>MD5 error</td>
</tr>
<tr>
<td>Cksum-Err</td>
<td>Checksum Error</td>
</tr>
<tr>
<td>Version</td>
<td>Version mismatch</td>
</tr>
<tr>
<td>AreaMismatch</td>
<td>Area mismatch</td>
</tr>
<tr>
<td>Conf-Issue</td>
<td>The received hello packet has a different hello or dead interval than the configuration</td>
</tr>
<tr>
<td>No-Buffer</td>
<td>Buffer allocation failure</td>
</tr>
<tr>
<td>Seq-no</td>
<td>A sequence no errors occurred during the database exchange process</td>
</tr>
<tr>
<td>Socket</td>
<td>Socket Read/Write operation error</td>
</tr>
<tr>
<td>Q-overflow</td>
<td>Packet(s) dropped due to queue overflow</td>
</tr>
<tr>
<td>Unknown-Pkt</td>
<td>Received packet is not an OSPF packet</td>
</tr>
<tr>
<td>RtidZero</td>
<td>Router-id received from the peer is 0.0.0.0.</td>
</tr>
</tbody>
</table>

**Usage Information**

The `show ip ospf process-id statistics` command displays the error packet count received on each interface as:

- The hello-timer remaining value for each interface.
- The wait-timer remaining value for each interface.
- The grace-timer remaining value for each interface.
- The packet count received and transmitted for each neighbor.
- Dead timer remaining value for each neighbor.
- Transmit timer remaining value for each neighbor.
- The LSU Q length and its highest mark for each neighbor.
- The LSR Q length and its highest mark for each neighbor.
**show ip ospf timers rate-limit**

Show the LSA currently in the queue waiting for timers to expire.

**Syntax**

`show ip ospf process-id timers rate-limit`

**Parameters**

- `process-id`: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

**Defaults**

- none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#show ip ospf process-id 10 timers rate-limit
List of LSAs in rate limit Queue
LSA id: 1.1.1.0 Type: 3 Adv Rtid: 3.3.3.3 Expiry time: 00:00:09.111
LSA id: 3.3.3.3 Type: 1 Adv Rtid: 3.3.3.3 Expiry time: 00:00:23.96
FTOS#
```
**Syntax**

```
show ip ospf process-id topology
```

**Parameters**

- `process-id` Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

**Defaults**

none

**Command Modes**

EXEC

**EXEC Privilege**

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

To isolate problems with inter-area and external routes, use this command. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.

**Example**

```
Figure 34-15. show ip ospf process-id topology Command Example

FTOS#show ip ospf 1 topology
Router ID Flags Cost Nexthop Interface Area
3.3.3.3 E/B/-/ 1 20.0.0.3 TenGig 13/1 0
1.1.1.1 E/-/-/ 1 10.0.0.1 TenGig 7/1 1
FTOS#
```

---

**summary-address**

Set the OSPF ASBR to advertise one external route.

**Syntax**

```
summary-address ip-address mask [not-advertise] [tag tag-value]
```

**Parameters**

- `ip-address` Specify the IP address in dotted decimal format of the address to be summarized.
- `mask` Specify the mask in dotted decimal format of the address to be summarized.
- `not-advertise` (OPTIONAL) Enter the keywords `not-advertise` to suppress that match the network prefix/mask pair.
- `tag tag-value` (OPTIONAL) Enter the keyword `tag` followed by a value to match on routes redistributed through a route map. The range is from 0 to 4294967295.

**Defaults**

Not configured.

**Command Modes**

ROUTER OSPF

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
The command **area range** summarizes routes for the different areas.

With the **not-advertise** parameter configured, you can use this command to filter out some external routes. For example, if you want to redistribute static routes to OSPF but you don't want OSPF to advertise routes with prefix 1.1.0.0. Then you can configure **summary-address 1.1.0.0 255.255.0.0** **not-advertise** to filter out all the routes that fall in range 1.1.0.0/16.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area range</td>
<td>Summarizes routes within an area.</td>
</tr>
</tbody>
</table>

#### timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

**Syntax**

```
timers spf delay holdtime
```

To return to the default, use the **no timers spf** command.

**Parameters**

- **delay**: Enter a number as the delay. The range is from 0 to 4294967295. The default is 5 seconds.
- **holdtime**: Enter a number as the hold time. The range is from 0 to 4294967295. The default is 10 seconds.

**Defaults**

- **delay**: 5 seconds; **holdtime**: 10 seconds

**Command Modes**

ROUTER OSPF

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Setting the **delay** and **holdtime** parameters to a low number enables the switch to switch to an alternate path quickly but requires more CPU usage.

#### timers throttle lsa all

Configure LSA transmit intervals.

**Syntax**

```
timers throttle lsa all {start-interval | hold-interval | max-interval}
```

To return to the default, use the **no timers throttle lsa** command.

**Parameters**

- **start-interval**: Set the minimum interval between initial sending and resending the same LSA. The range is from 0 to 600,000 milliseconds.
- **hold-interval**: Set the next interval to send the same LSA after the start-interval has been attempted. The range is from 1 to 600,000 milliseconds.
- **max-interval**: Set the maximum amount of time the system waits before sending the LSA. The range is from 1 to 600,000 milliseconds.

**Defaults**

- **start-interval**: 0 msec
• hold-interval 5000 msec
• max-interval: 5000 msec

Command Modes

ROUTER OSPF

Command History

Usage Information

LSAs are sent after the start-interval and then after hold-interval until the maximum interval is reached. In throttling, exponential backoff is used when sending the same LSA, so that the interval is multiplied until the maximum time is reached. For example, if the start-interval 5000, hold-interval 1000 and max-interval 100,000 are set, the LSA is sent at 5000 msec, then 1000 msec, then 2000 msec, them 4000 until 100,000 msec is reached.

**timers throttle lsa arrival**

Configure the LSA acceptance intervals.

**Syntax**

`timers throttle lsa arrival arrival-time`

To return to the default, use the `no timers throttle lsa` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arrival-time</code></td>
<td>Set the interval between receiving the same LSA repeatedly, to allow sufficient time for the system to accept the LSA. The range is from 0 to 600,000 milliseconds.</td>
</tr>
</tbody>
</table>

**Defaults**

1000 msec

**Command Modes**

ROUTER OSPF

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Open shortest path first version 3 (OSPFv3) for IPv6 is supported on the MXL Switch platform.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Dell Networking implementation of OSPFv3 is based on IETF RFC 2740.

area authentication

Configure an IPsec authentication policy for OSPFv3 packets in an OSPFv3 area.

**Syntax**

`area area-id authentication ipsec spi number {MD5 | SHA1} [key-encryption-type] key`

To remove an IPsec authentication policy from an OSPFv3 area, enter the `no area area-id authentication spi number` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area area-id</td>
<td>Area for which OSPFv3 traffic is to be authenticated. For area-id, you can enter a number. The range is from 0 to 4294967295.</td>
</tr>
<tr>
<td>ipsec spi number</td>
<td>Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.</td>
</tr>
<tr>
<td>MD5</td>
<td>SHA1</td>
</tr>
<tr>
<td>key-encryption-type</td>
<td>(OPTIONAL) Specifies if the key is encrypted. The values are 0 (key is not encrypted) or 7 (key is encrypted).</td>
</tr>
<tr>
<td>key</td>
<td>Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured

**Command Modes**

ROUTER OSPFv3

**Command History**

Version 9.2(0.0) Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Before you enable IPsec authentication on an OSPFv3 area, you must first enable OSPFv3 globally on the router. Configure the same authentication policy (same SPI and key) on each interface in an OSPFv3 link.

An SPI number must be unique to one IPsec security policy (authentication or encryption) on the router.

If you have enabled IPsec encryption in an OSPFV3 area with the `area encryption` command, you cannot use the `area authentication` command in the area at the same time.
The configuration of IPsec authentication on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area authentication policy that has been configured is applied to the interface.

### area encryption

Configure an IPsec encryption policy for OSPFv3 packets in an OSPFv3 area.

**Syntax**

```
area area-id authentication ipsec spi number esp encryption-algorithm [key-encryption-type] key authentication algorithm [key-encryption-type] key | null
```

To remove an IPsec encryption policy from an interface, enter the `no area area-id encryption spi number` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>area</strong></td>
<td>Area for which OSPFv3 traffic is to be authenticated. For area-id, you can enter a number. The range is from 0 to 4294967295.</td>
</tr>
<tr>
<td><strong>area-id</strong></td>
<td>Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.</td>
</tr>
<tr>
<td><strong>ipsec spi number</strong></td>
<td>Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.</td>
</tr>
<tr>
<td><strong>esp encryption-algorithm</strong></td>
<td>(OPTIONAL) Specifies if the key is encrypted. The values are 0 (key is not encrypted) or 7 (key is encrypted).</td>
</tr>
<tr>
<td><strong>key-encryption-type</strong></td>
<td>Text string used in authentication. For 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.</td>
</tr>
<tr>
<td><strong>key</strong></td>
<td>Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.</td>
</tr>
<tr>
<td><strong>authentica</strong></td>
<td>(OPTIONAL) Specifies if the key is encrypted. The values are 0 (key is not encrypted) or 7 (key is encrypted).</td>
</tr>
<tr>
<td><strong>tion algorithm</strong></td>
<td>Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).</td>
</tr>
<tr>
<td><strong>null</strong></td>
<td>Causes an encryption policy configured for the area to not be inherited on the interface.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured

**Command Modes**

ROUTER OSPFv3

**Command History**

Version 9.2(0.0) Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Before you enable IPsec authentication on an OSPFv3 area, first enable OSPFv3 globally on the router. Configure the same authentication policy (same SPI and key) on each interface in an OSPFv3 link.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router.
When you configure encryption for an OSPFv3 area with the `area encryption` command, you enable both IPsec encryption and authentication. However, when you enable authentication on an area with the `area authentication` command, you do not enable encryption at the same time.

If you have enabled IPsec authentication in an OSPFv3 area with the `area authentication` command, you cannot use the `area encryption` command in the area at the same time.

The configuration of IPsec encryption on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area encryption policy that has been configured is applied to the interface.

clear ipv6 ospf process
Reset an OSPFv3 router process without removing or re-configuring the process.

Syntax
```
clear ipv6 ospf process
```

Command Modes
- EXEC
- EXEC Privilege

Command History
```
Version 9.2(0.0) Introduced on MXL 10/40GbE Switch IO Module
```

debug ipv6 ospf bfd
Display debug information and interface types for BFD on OSPF IPv6 packets.

Syntax
```
debug ipv6 ospf bfd [interface]
```

Parameters
- `interface` (OPTIONAL) Enter one of the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a tunnel interface, enter the keyword `tunnel` then a number. The range is from 1 to 16383.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes
- EXEC Privilege

Command History
```
Version 9.2(0.0) Introduced on MXL 10/40GbE Switch IO Module
```

Usage Information
The following section describes the command fields.
debug ipv6 ospf

Display debug information and interface types on OSPF IPv6 packets or events.

Syntax

```
debug ipv6 ospf [packet | events] [interface]
```

To cancel the debug command, enter `no debug ipv6 ospf`.

Parameters

```
interface
```

(OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a tunnel interface, enter the keyword `tunnel` then a number. The range is from 1 to 16383.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

EXEC Privilege
default-information originate

Configure the FTOS to generate a default external route into an OSPFv3 routing domain.

Syntax

default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]

To return to the default values, use the no default-information originate command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>(OPTIONAL) Enter the keyword always to specify that default route information must always be advertised.</td>
</tr>
<tr>
<td>metric</td>
<td>(OPTIONAL) Enter the keyword metric then a number to configure a metric value for the route. The range is from 1 to 16777214.</td>
</tr>
<tr>
<td>metric-value</td>
<td>(OPTIONAL) Enter the keywords metric-type then an OSPFv3 link state type of 1 or 2 for default routes. The values are:</td>
</tr>
<tr>
<td>type-value</td>
<td>• 1 = Type 1 external route</td>
</tr>
<tr>
<td>route-map</td>
<td>(OPTIONAL) Enter the keywords route-map then the name of an established route map.</td>
</tr>
<tr>
<td>map-name</td>
<td></td>
</tr>
</tbody>
</table>

Defaults Disabled

Command Modes ROUTER OSPFv3

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

graceful-restart grace-period

Enable OSPFv3 graceful restart globally by setting the grace period (in seconds) that an OSPFv3 router’s neighbors continues to advertise the router as adjacent during a graceful restart.

Syntax

graceful-restart grace-period seconds

To return to the default values, use the no graceful-restart grace-period command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>The time duration, in seconds, that specifies the duration of the restart process before OSPFv3 terminates the process. The range is from 40 to 1800 seconds.</td>
</tr>
</tbody>
</table>

Defaults OSPFv3 graceful restart is disabled and functions in a helper-only role.

Command Modes ROUTER OSPFv3

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>
By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

To enable OSPFv3 graceful restart, enter the ipv6 router ospf command to enter OSPFv3 configuration mode and then configure a grace period using the graceful-restart grace-period command. The grace period is the length of time that OSPFv3 neighbors continue to advertise the restarting router as though it is fully adjacent. When graceful restart is enabled (restarting role), an OSPFv3 restarting expects its OSPFv3 neighbors to help when it restarts by not advertising the broken link.

When you enable the helper-reject role on an interface with the ipv6 ospf graceful-restart helper-reject command, you reconfigure OSPFv3 graceful restart to function in a “restarting-only” role. In a “restarting-only” role, OSPFv3 does not participate in the graceful restart of a neighbor.

**graceful-restart mode**

Specify the type of events that trigger an OSPFv3 graceful restart.

**Syntax**

```
graceful-restart mode [planned-only | unplanned-only]
```

To return to the default values, use the `no graceful-restart noded` command.

**Parameters**

- `planned-only` (OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only.
- `unplanned-only` (OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in a planned restart condition only.

**Defaults**

OSPFv3 graceful restart supports both planned and unplanned failures.

**Command Modes**

- ROUTER OSPFv3

**Command History**

- Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

OSPFv3 graceful restart supports planned-only and/or unplanned-only restarts. The default is support for both planned and unplanned restarts.

- A planned restart occurs when you enter the `redundancy force-failover rpm` command to force the primary RPM to switch to the backup RPM. During a planned restart, OSPF sends out a Type-11 Grace LSA before the system switches over to the backup RPM.
- An unplanned restart occurs when an unplanned event causes the active RPM to switch to the backup RPM, such as when an active process crashes, the active RPM is removed, or a power failure happens. During an unplanned restart, OSPF sends out a Grace LSA when the backup RPM comes online.

By default, both planned and unplanned restarts trigger an OSPFv3 graceful restart. Selecting one or the other mode restricts OSPFv3 to the single selected mode.
**ipv6 ospf area**

Enable IPv6 OSPF on an interface.

**Syntax**

```
ipv6 ospf process id area area id
```

To disable OSPFv6 routing for an interface, use the `no ipv6 ospf process id area area id` command.

**Parameters**

- `process id` Enter the process identification number.
- `area area id` Specify the OSPF area. The range is from 0 to 65535.

**Defaults**

none

**Command Modes**

INTERFACE

**Command History**

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

---

**ipv6 ospf authentication**

Enable IPv6 OSPF on an interface.

**Syntax**

```
ipv6 ospf authentication {null | ipsec spi number \{MD5 | SHA1\} \[key-encryption-type\] key;}
```

To remove an IPsec authentication policy from an interface, enter the `no ipv6 ospf authentication spi number` command.

To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf authentication null` command.

**Parameters**

- `null` Causes an authentication policy configured for the area to not be inherited on the interface.
- `ipsec spi number` Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
- `MD5 | SHA1` Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
- `key-encryption-type` (OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
- `key` Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

**Defaults**

Not configured

**Command Modes**

INTERFACE

**Command History**

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module
Before you enable IPsec authentication on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFV3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same authentication policy (same SPI and key) on each OSPFv3 interface in a link.

### ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

**Syntax**

```plaintext
ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]
```

To disable all BFD sessions on an OSPFv3 interface implicitly, use the **no ipv6 ospf bfd all-neighbors disable** command.

**Parameters**

- **disable** (OPTIONAL) Enter the keyword **disable** to disable BFD on this interface.
- **interval** milliseconds (OPTIONAL) Enter the keyword **interval** to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **100**.
- **min_rx** milliseconds Enter the keyword **min_rx** to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 100. The default is **100**.
- **multiplier** value Enter the keyword **multiplier** to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
- **role** [**active** | **passive**] Enter the role that the local system assumes:
  - **active** — The active system initiates the BFD session. Both systems can be active for the same session.
  - **passive** — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.
  The default is **Active**.

**Defaults**

See Parameters

**Command Modes**

INTERFACE

**Command History**

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

This command provides the flexibility to fine-tune the timer values based on individual interface needs when the **ipv6 ospf bfd** command is configured in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the **bfd all-neighbors** command. Using the no form of this command does not disable BFD if BFD is configured in CONFIGURATION mode.

To disable BFD on a specific interface while BFD is configured in CONFIGURATION mode, use the keyword **disable**.
ipv6 ospf cost

Explicitly specify the cost of sending a packet on an interface.

Syntax

```
ipv6 ospf interface-cost
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-cost</td>
<td>Enter a unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.</td>
</tr>
</tbody>
</table>

Defaults

Default cost based on the bandwidth.

Command Modes

INTERFACE

Command History

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

Usage Information

In general, the path cost is calculated as:

\[10^8 / \text{bandwidth}\]

Using this formula, the default path cost is calculated as:

- GigabitEthernet—Default cost is 1
- TenGigabitEthernet—Default cost is 1
- FortygigEthernet — Default cost is 1
- Ethernet—Default cost is 10

ipv6 ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the time interval elapses, the neighboring routers declare the router down.

Syntax

```
ipv6 ospf dead-interval seconds
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Enter the time interval in seconds. The range is from 1 to 65535 seconds.</td>
</tr>
</tbody>
</table>

Defaults

40 seconds (Ethernet)

Command Modes

INTERFACE

Command History

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

Usage Information

By default, the dead interval is four times longer than the default `ipv6 ospf hello-interval`. 
Configure an IPsec encryption policy for OSPFv3 packets on an IPv6 interface.

**Syntax**

```
ipv6 ospf encryption {null | ipsec spi number esp encryption-algorithm [key-encryption-type] key authentication-algorithm [key-encryption-type] key}
```

To remove an IPsec encryption policy from an interface, enter the `no ipv6 ospf encryption spi number` command.

To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf encryption null` command.

**Parameters**

- **null**
  - Causes an encryption policy configured for the area to not be inherited on the interface.

- **ipsec spi number**
  - Security Policy index (SPI) value that identifies an IPsec security policy.
  - The range is from 256 to 4294967295.

- **esp encryption-algorithm**
  - Encryption algorithm used with ESP.
  - Valid values are: 3DES, DES, AES-CBC, and NULL.
  - For AES-CBC, only the AES-128 and AES-192 ciphers are supported.

- **key-encryption-type**
  - (OPTIONAL) Specifies if the key is encrypted.
  - The values are 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  - Text string used in authentication.
  - For 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.

- **authentication-algorithm**
  - Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.

- **key-encryption-type**
  - (OPTIONAL) Specifies if the key is encrypted.
  - The values are 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  - Text string used in authentication.
  - For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).
  - For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

- **Version 9.2.(0.0)**
  - Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Before you enable IPsec encryption on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same encryption policy (same SPI and key) on each OSPFv3 interface in a link.
ipv6 ospf graceful-restart helper-reject

Configure an OSPFv3 interface to not act upon the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

Syntax

ipv6 ospf graceful-restart helper-reject

To disable the helper-reject role, enter the no ipv6 ospf graceful-restart helper-reject command.

Defaults

The helper-reject role is not configured

Command Modes

INTERFACE

Command History

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

Usage Information

By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

The graceful-restart role command is not supported in OSPFv3. When you enable the helper-reject role on an interface, you reconfigure an OSPFv3 router to function in a “restarting-only” role.

ipv6 ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

Syntax

ipv6 ospf hello-interval seconds

Parameters

seconds

Enter the time interval in seconds as the time between hello packets. The range is 1 50 65525 seconds.

Defaults

10 seconds (Ethernet)

Command Modes

INTERFACE

Command History

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The time interval between hello packets must be the same for routers in a network.

isv6 ospf priority

To determine the designated router for the OSPFv3 network, set the priority of the interface.

Syntax

ipv6 ospf priority number
To return to the default time interval, use the `no ipv6 ospf priority` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Defaults</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
<td>1</td>
<td>INTERFACE</td>
<td>Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

Setting a priority of 0 makes the router ineligible for election as a designated router or backup designated router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

### ipv6 router ospf

Enable OSPF for IPv6 router configuration.

**Syntax**

`ipv6 router ospf process-id`

To exit OSPF for IPv6, use the `no ipv6 router ospf process-id` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Defaults</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>process-id</strong></td>
<td>none</td>
<td>CONFIGURATION</td>
<td>Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

### maximum-paths

To forward packets over multiple paths, enable the software.

**Syntax**

`maximum-paths number`

To disable packet-forwarding over multiple paths, use the `no maximum-paths` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Defaults</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
<td>4</td>
<td>ROUTER OSPFv3 for OSPFv3</td>
<td>Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>
### passive-interface

Suppress both receiving and sending routing updates on an interface.

#### Syntax

```
passive-interface {default | interface}
```

To enable both the receiving and sending routing, enter the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, enter the `no passive-interface default` command.

#### Parameters

- **default**
  - Enter the keyword `default` to make all OSPF interfaces (current and future) passive.

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
    - For Port Channel groups, enter the keywords `port-channel` followed by a number: Range: 1-128
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
    - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094..

#### Command Modes

- **ROUTER OSPF for OSPFv2**

- **ROUTER OSPFv3 for OSPFv3**

#### Command History

- **Version 9.2(0.0)** Added support for OSPFv3.
- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

#### Usage Information

By default, no interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix continues to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is not sent or received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.
**redistribute**

Redistribute information from another routing protocol into OSPFv3 throughout the OSPF process.

**Syntax**
```bash
redistribute {bgp as number} {connected | static} [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]
```

To disable redistribution, use the `no redistribute {connected | static}` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp as number</td>
<td>Enter the keyword <code>bgp</code> then the autonomous system number. The range is from 1 to 65535.</td>
</tr>
<tr>
<td>connected</td>
<td>Enter the keyword <code>connected</code> to specify that information from active routes on interfaces is redistributed.</td>
</tr>
<tr>
<td>static</td>
<td>Enter the keyword <code>static</code> to specify that information from static routes is redistributed.</td>
</tr>
<tr>
<td>metric metric-value</td>
<td>(OPTIONAL) Enter the keyword <code>metric</code> followed by a number. Range: 0 (zero) to 16777214.</td>
</tr>
</tbody>
</table>
| metric-type type-value | (OPTIONAL) Enter the keywords `metric-type` followed by one of the following:  
  - 1 = OSPF External type 1  
  - 2 = OSPF External type 2  
  The default is 2. |
| route-map map-name  | (OPTIONAL) Enter the keywords `route-map` followed by the name of the route map. |
| tag tag-value       | (OPTIONAL) Enter the keyword `tag` followed by a number. The range is from 0 to 4294967295. The default is 0. |

**Defaults**
Not configured.

**Command Modes**
ROUTER OSPFv3 for OSPFv3

**Command History**
- Version 9.2(0.0) Added support for OSPFv3.
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**
To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

**Related Commands**
- `default-information originate` Generates a default route into the OSPF routing domain.

**router-id**

Use this command to configure a fixed router ID.

**Syntax**
```bash
router-id ip-address
```

To remove the fixed router ID, use the `no router-id ip-address` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the router ID in the dotted decimal IP address format.</td>
</tr>
</tbody>
</table>
The router ID is selected automatically from the set of IPv6 addresses configured on a router.

**Command Modes**

ROUTER OSPFv3 for OSPFv3

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for OSPFv3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Example**

*Figure 34-17. router-id Command Example*

```
FTOS(conf)#router ospf 100
FTOS(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/n]:

FTOS(conf-router_ospf)#show config
router ospf 100
router-id 1.1.1.1
FTOS(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/n]:

FTOS#`
```

**Usage Information**

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If you use this command on an OSPF router process which is already active (that is, has neighbors), a prompt displays reminding you that changing router-id brings down the existing OSPF adjacency. The new router ID is effective at the next reload.

**show crypto ipsec policy**

Display the configuration of IPsec authentication and encryption policies.

**Syntax**

```
show crypto ipsec policy [name name]
```

**Parameters**

- `name name` (OPTIONAL) Displays configuration details about a specified policy.

**Defaults**

No default behavior or values.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for OSPFv3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

The `show crypto ipsec policy` command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

**show crypto ipsec sa ipv6**

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.
**Syntax**

show crypto ipsec sa ipv6 [interface interface]

**Parameters**

- **interface interface** (OPTIONAL) Displays information about the SAs used on a specified OSPFv3 interface, where interface is one of the following values:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port number.
  - For a Port Channel interface, enter the keywords port-channel then the port channel number.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port number.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE then the slot/port number.
  - For a VLAN interface, enter the keyword vlan then the vlan-id. The valid VLAN IDs range is from 1 to 4094.

**Defaults**

No default behavior or values.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The `show crypto ipsec sa ipv6` command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.

---

**show ipv6 ospf database**

Display information in the OSPFv3 database, including link-state advertisements (LSAs).

**Syntax**

show ipv6 ospf database [database-summary | grace-lsa]

**Parameters**

- **database-summary** (OPTIONAL) Enter the keywords `database-summary` to view a summary of database LSA information.
- **grace-lsa** (OPTIONAL): Enter the keywords `grace-lsa` to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 9.2.(0.0) Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The `show ipv6 ospf database` command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.
show ipv6 ospf interface

View OSPFv3 interface information.

**Syntax**

```sql
show ipv6 ospf [interface]
```

**Parameters**

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` and the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` and the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` and the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel` and a number. The range is from 1 to 128.
  - For a Tunnel interface, enter the keywords `tunnel` and a number. The range is from 1 to 16383.
  - For a VLAN, enter the keyword `vlan` and a number from 1 to 4094.

**Defaults**

None

**Command Modes**

EXEC

<table>
<thead>
<tr>
<th>Command History</th>
<th>Usage Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 9.2.(0.0)</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

If BFD is enabled at the global level, the `show ipv6 ospf interface` command shows the BFD provisioning.

If BFD is enabled at the interface level, the `show ipv6 ospf interface` command shows the BFD interval timers.

**Example**

```plaintext
show ipv6 ospf interface Command

FTOS#show ipv6 ospf interface gigabitethernet 1/0
GigabitEthernet 1/0 is up, line protocol is up
Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
NetworkType BROADCAST, Cost: 1, Passive: No
Transmit Delay is 100 sec, State DR, Priority 1
Designated router on this network is 11.1.1.1 (local)
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 1,
Retransmit 5
FTOS#
```

show ipv6 ospf neighbor

Display the OSPF neighbor information on a per-interface basis.

**Syntax**

```sql
show ipv6 ospf neighbor [interface]
```
Parameters

interface (OPTIONAL) Enter the following keywords and slot/port or number information:
- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet and the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet and the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE and the slot/port information.
- For a Port Channel interface, enter the keywords port-channel and a number. The range is from 1 to 128.
- For a Tunnel interface, enter the keywords tunnel and a number. The range is from 1 to 16383.
- For a VLAN, enter the keyword vlan and a number from 1 to 4094.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

| Version 9.2.(0.0) | Introduced on MXL 10/40GbE Switch IO Module |
Port Monitoring

Overview

The port monitoring feature allows you to monitor network traffic by forwarding a copy of each incoming or outgoing packet from one port to another port.

Commands

- description
- monitor session
- show config
- show monitor session
- show running-config monitor session
- source (port monitoring)

Important Points to Remember

- Port monitoring is supported on physical ports only. Logical interfaces, such as Port Channels and virtual local area networks (VLANs), are not supported.
- The Dell Networking operating software (FTOS) supports as many monitor sessions on a system as the number of port-pipes.
- The monitoring (destination, “MG”) and monitored (source, “MD”) ports must be on the same switch.
- A monitoring port can monitor any physical port in the chassis.
- Only one MG and one MD may be in a single port-pipe.
- A monitoring port can monitor more than one port.
- More than one monitored port can have the same destination monitoring port.
- FTOS supports multiple source ports to be monitored by a single destination port in one monitor session.
- One monitor session can have only one MG port.

Note: The monitoring port should not be a part of any other configuration.
description

Enter a description of this monitoring session.

Syntax
description \{description\}

To remove the description, use the no description \{description\} command.

Parameters
- \textit{description}
  - Enter a description regarding this session (80 characters maximum).

Defaults
none

Command Modes
MONITOR SESSION (conf-mon-sess-\textit{session-ID})

Command History
- Version 8.3.16.1 Introduced on M I/O Aggregator

Related Commands
- monitor session Enables a monitoring session.

monitor session

Create a session for monitoring traffic with port monitoring.

Syntax
monitor session \textit{session-ID}

To delete a session, use the no monitor session \textit{session-ID} command.
To delete all monitor sessions, use the no monitor session all command.

Parameters
- \textit{session-ID}
  - Enter a session identification number.
  - Range: 0 to 65535

Defaults
none

Command Modes
CONFIGURATION

Command History
- Version 8.3.16.1 Introduced on M I/O Aggregator

Example

\begin{verbatim}
FTOS(conf)# monitor session 60
FTOS(conf-mon-sess-60)
\end{verbatim}

Usage Information
The monitor command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Related Commands
- show monitor session Displays the monitor session
- show running-config monitor session Displays the running configuration of a monitor session
show config

Display the current monitor session configuration.

Syntax

show config

Defaults

none

Command Modes

MONITOR SESSION (conf-mon-sess-session-ID)

Command History

Version 8.3.16.1 Introduced on M I/O Aggregator

Example

Figure 35-2. show config Command Example

```
FTOS(conf-mon-sess-11)#show config
!
monitor session 11
  source TenGigabitEthernet 10/0 destination TenGigabitEthernet 10/47 direction rx
```

show monitor session

Display the monitor information of a particular session or all sessions.

Syntax

show monitor session {session-ID}

To display monitoring information for all sessions, use the show monitor session command.

Parameters

- **session-ID** (OPTIONAL) Enter a session identification number.
  Range: 0 to 65535

Defaults

none

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on M I/O Aggregator

Example

Figure 35-3. show monitor session Command Example

```
FTOS#show monitor session 11
SessionID Source Destination Direction Mode
---------- ------ -------------- --------- -------
   11    TenGig 10/0 TenGig 10/47      rx       interface
```

Related Commands

- **monitor session** Creates a session for monitoring.
show running-config monitor session
Display the running configuration of all monitor sessions or a specific session.

Syntax
show running-config monitor session {session-ID}
To display the running configuration for all monitor sessions, use just the show running-config
monitor session command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-ID</td>
<td>(OPTIONAL) Enter a session identification number.</td>
<td>0 to 65535</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on M I/O Aggregator

Example
Figure 35-4. show running-config monitor session Command Example

FTOS#show running-config monitor session
monitor session 8
  source TenGigabitEthernet 10/46 destination TenGigabitEthernet 10/1 direction rx
monitor session 11
  source TenGigabitEthernet 10/0 destination TenGigabitEthernet 10/47 direction rx

FTOS#show running-config monitor session 11
monitor session 11
  source TenGigabitEthernet 10/0 destination TenGigabitEthernet 10/47 direction rx

Usage Information
The monitoring command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session</td>
<td>Creates a session for monitoring.</td>
</tr>
<tr>
<td>show monitor session</td>
<td>Displays a monitor session.</td>
</tr>
</tbody>
</table>
source (port monitoring)

Configure a port monitor source.

**Syntax**

```
source interface destination interface direction {rx | tx | both}
```

To disable a monitor source, use the `no source interface destination interface direction {rx | tx | both}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| interface | Enter the one of the following keywords and slot/port information:  
• For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.  
• For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. |
| destination | Enter the keyword `destination` to indicate the interface destination. |
| direction {rx | tx | both} | Enter the keyword `direction` followed by one of the packet directional indicators.  
rx: to monitor receiving packets only  
tx: to monitor transmitting packets only  
both: to monitor both transmitting and receiving packets |

**Defaults**

none

**Command Modes**

MONITOR SESSION (conf-mon-sess-session-ID)

**Command History**

Version 8.3.16.1 Introduced on M I/O Aggregator

**Example**

```
Figure 35-5. Configuring a Port Monitor Source Command Example

FTOS(conf-mon-sess-11)#source tengig 10/0 destination tengig 10/47 direction rx
FTOS(conf-mon-sess-11)#
```
PIM-Sparse Mode (PIM-SM)

Overview

The protocol-independent multicast (PIM) commands are supported by the Dell Networking operating software (FTOS) on the MXL Switch platform.

This chapter contains the following sections:

- IPv4 PIM-Sparse Mode Commands
- IPv6 PIM-Sparse Mode Commands

IPv4 PIM-Sparse Mode Commands

The following describes the IPv4 PIM-sparse mode (PIM-SM) commands.

- clear ip pim rp-mapping
- Usage Information
- debug ip pim
- ip pim bsr-border
- ip pim bsr-candidate
- ip pim dr-priority
- ip pim join-filter
- ip pim ingress-interface-map
- ip pim neighbor-filter
- ip pim query-interval
- ip pim register-filter
- ip pim rp-address
- ip pim rp-candidate
- ip pim sparse-mode
- ip pim sparse-mode sg-expiry-timer
- ip pim spt-threshold
- no ip pim snooping dr-flood
- show ip pim bsr-router
- show ip pim interface
- show ip pim neighbor
- show ip pim rp
- show ip pim snooping interface
- show ip pim snooping neighbor
clear ip pim rp-mapping

The bootstrap router (BSR) feature uses this command to remove all or particular rendezvous point (RP) advertisement.

Syntax

```
clear ip pim rp-mapping rp-address
```

Parameters

- `rp-address` (OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D)

Command Modes

- EXEC Privilege

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

clear ip pim tib

Clear PIM tree information from the PIM database.

Syntax

```
clear ip pim tib [group]
```

Parameters

- `group` (OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D)

Command Modes

- EXEC Privilege

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you use this command on a local VLT node, all multicast routes from the local PIM TIB, the entire multicast route table, and all the entries in the data plane are deleted. The local VLT node sends a request to the peer VLT node to download multicast routes learned by the peer. Both local and synced routes are removed from the local VLT node multicast route table. The peer VLT node clears synced routes from the node.

If you use this command on a peer VLT node, only the synced routes are deleted from the multicast route table.

dbueip ip pim

View IP PIM debugging messages.

Syntax

```
dbueip ip pim [bsr | events | packet [in | out] | register | state | timer [assert | hello | joinprune | register]]
```

To disable PIM debugging, use the `no debug ip pim` command, or use the `undebug all` to disable all debugging command.
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bsr</td>
<td>(OPTIONAL) Enter the keyword bsr to view PIM Candidate RP/BSR activities.</td>
</tr>
<tr>
<td>events</td>
<td>(OPTIONAL) Enter the keyword events to view PIM events for a specific group.</td>
</tr>
<tr>
<td>group</td>
<td>(OPTIONAL) Enter the keyword group to view PIM messages for a specific group.</td>
</tr>
<tr>
<td>packet [in</td>
<td>out]</td>
</tr>
<tr>
<td>register</td>
<td>(OPTIONAL) Enter the keyword register to view PIM register address in dotted decimal format (A.B.C.D).</td>
</tr>
<tr>
<td>state</td>
<td>(OPTIONAL) Enter the keyword state to view PIM state changes.</td>
</tr>
<tr>
<td>timer [assert</td>
<td>hello</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

Command Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

**ip pim bsr-border**

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

**Syntax**

ip pim bsr-border

To return to the default value, use the no ip pim bsr-border command.

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time out. To clean the candidate RP advertisements, use the clear ip pim rp-mapping command.
ip pim bsr-candidate

To join the Bootstrap election process, configure the PIM router.

Syntax

`ip pim bsr-candidate interface [hash-mask-length] [priority]`

To return to the default value, use the `no ip pim bsr-candidate` command.

Parameters

- **interface**: Enter the following keywords and slot/port or number information:
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
- **hash-mask-length** (OPTIONAL): Enter the hash mask length. The range is from zero (0) to 32. The default is 30.
- **priority** (OPTIONAL): Enter the priority used in Bootstrap election process. The range is from zero (0) to 255. The default is zero (0).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

ip pim dr-priority

Change the designated router (DR) priority for the interface.

Syntax

`ip pim dr-priority priority-value`

To remove the DR priority value assigned, use the `no ip pim dr-priority` command.

Parameters

- **priority-value**: Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1.

Defaults

1

Command Modes

INTERFACE

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same DR priority value, the interface with the largest interface IP address becomes the designated router.
**ip pim join-filter**

Permit or deny PIM Join/Prune messages on an interface using an extended IP access list. This command prevents the PIM SM router from creating state based on multicast source and/or group.

**Syntax**

```
ip pim join-filter ext-access-list {in | out}
```

To remove the access list, use the `no ip pim join-filter ext-access-list {in | out}` command.

**Parameters**

- `ext-access-list` Enter the name of an extended access list.
- `in` Enter this keyword to apply the access list to inbound traffic.
- `out` Enter this keyword to apply the access list to outbound traffic.

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Force10(conf)# ip access-list extended iptv-channels  
Force10(config-ext-nacl)# permit ip 10.1.2.3/24 225.1.1.0/24  
Force10(config-ext-nacl)# permit ip any 232.1.1.0/24  
Force10(config-ext-nacl)# permit ip 100.1.1.0/16 any  
Force10(config-if-gi-1/1)# ip pim join-filter iptv-channels in  
Force10(config-if-gi-1/1)# ip pim join-filter iptv-channels out
```

**Related Commands**

- `ip access-list extended` Configure an access list based on IP addresses or protocols.

**ip pim ingress-interface-map**

When the Dell Networking system is the RP, statically map potential incoming interfaces to (*,G) entries to create a lossless multicast forwarding environment.

**Syntax**

```
ip pim ingress-interface-map std-access-list
```

**Parameters**

- `std-access-list` Enter the name of a standard access list.

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Force10(conf)# ip access-list standard map1  
Force10(config-std-nacl)# permit 224.0.0.1/24  
Force10(config-std-nacl)# exit  
Force10(config)# int gig 1/1  
Force10(config-if-gi-1/1)# ip pim ingress-interface-map map1
```
ip pim neighbor-filter

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

Syntax

```
ip pim neighbor-filter {access-list}
```

To remove the restriction, use the `no ip pim neighbor-filter {access-list}` command.

Parameters

- `access-list` Enter the name of a standard access list. Maximum 16 characters.

Defaults

none

Command Modes

CONFIGURATION

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Do not enter this command before creating the access-list.

ip pim query-interval

Change the frequency of PIM Router-Query messages.

Syntax

```
ip pim query-interval seconds
```

To return to the default value, use the `no ip pim query-interval seconds` command.

Parameters

- `seconds` Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is 30 seconds.

Defaults

30 seconds

Command Modes

INTERFACE

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

ip pim register-filter

To prevent a PIM source DR from sending register packets to an RP for the specified multicast source and group, use this feature.

Syntax

```
ip pim register-filter access-list
```

To return to the default, use the `no ip pim register-filter access-list` command.

Parameters

- `access-list` Enter the name of an extended access list. Maximum 16 characters.

Defaults

Not configured

Command Modes

CONFIGURATION
The access name is an extended IP access list that denies PIM register packets to RP at the source DR based on the multicast and group addresses. Do not enter this command before creating the access-list.

**ip pim rp-address**

Configure a static PIM Rendezvous Point (RP) address for a group or access-list.

**Syntax**

```
ip pim rp-address address {group-address group-address mask} override
```

To remove an RP address, use the `no ip pim rp-address address {group-address group-address mask} override` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address</strong></td>
<td>Enter the RP address in dotted decimal format (A.B.C.D).</td>
</tr>
<tr>
<td><strong>group-address</strong></td>
<td>Enter the keyword <code>group-address</code> then a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.</td>
</tr>
<tr>
<td><strong>override</strong></td>
<td>Enter the keyword <code>override</code> to override the BSR updates with static RP. The override takes effect immediately during enable/disable.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured

**Command Modes**

CONFIGURATION

**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

First-hop routers use this address by to send register packets on behalf of source multicast hosts. The RP addresses are stored in the order in which they are entered. RP addresses learned using BSR take priority over static RP addresses. Without the override option, RPs advertised by the BSR updates take precedence over the statically configured RPs.

**ip pim rp-candidate**

To send out a Candidate-RP-Advertisement message to the bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR, configure a PIM router.

**Syntax**

```
ip pim rp-candidate {interface [priority]}
```

To return to the default value, use the `no ip pim rp-candidate {interface [priority]}` command.
Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| interface  | Enter the following keywords and slot/port or number information:  
  - For a Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port information.  
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.  
  - For a Port Channel interface, enter the keywords port-channel then a number: The range is from 1 to 128.  
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.  
  - For a VLAN, enter the keyword vlan then a number from 1 to 4094.  
| priority   | (OPTIONAL) Enter the priority used in Bootstrap election process. The range is from zero (0) to 255. The default is 192. |

Defaults

Not configured.

Command Modes

- CONFIGURATION
- INTERFACE

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

iip pim sparse-mode

Enable PIM sparse mode and IGMP on the interface.

Syntax

ip pim sparse-mode

To disable PIM sparse mode and IGMP, enter no ip pim sparse-mode command.

Defaults

Disabled.

Command Modes

- INTERFACE

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The interface must be enabled (no shutdown command) and not have the switchport command configured. Multicast must also be enabled globally (using the ip multicast-lag-hashing command). PIM is supported on the port-channel interface.

Related Commands

ip multicast-lag-hashing Enables multicast globally.
ip pim sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources, or for a specific set of (S,G) pairs defined by an access list.

**Syntax**

```
ip pim sparse-mode sg-expiry-timer seconds [access-list name]
```

To disable configured timers and return to default mode, enter `no ip pim sparse-mode sg-expiry-timer`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Enter the number of seconds the S, G entries will be retained. The range is from 211 to 86400.</td>
</tr>
<tr>
<td><code>access-list name</code></td>
<td>(OPTIONAL) Enter the name of a previously configured Extended ACL to enable the expiry time to specified S,G entries</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled. The default expiry timer (with no times configured) is 210 sec.

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

This command configures an expiration timer for all S,G entries, unless they are assigned to an Extended ACL.

ip pim spt-threshold

To switch to the shortest path tree when the traffic reaches the specified threshold value, configure the PIM router.

**Syntax**

```
ip pim spt-threshold value | infinity
```

To return to the default value, use the `no ip pim spt-threshold`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>(OPTIONAL) Enter the traffic value in kilobits per second. The default is 10 packets per second. A value of zero (0) will cause a switchover on the first packet.</td>
</tr>
<tr>
<td><code>infinity</code></td>
<td>(OPTIONAL) Enter the keyword <code>infinity</code> to never switch to the source-tree.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

This is applicable to last hop routers on the shared tree towards the Rendezvous Point (RP).
no ip pim snooping dr-flood

Disable the flooding of multicast packets to the PIM designated router.

Syntax: no ip pim snooping dr-flood

To re-enable the flooding of multicast packets to the PIM designated router, use the `ip pim snooping dr-flood` command.

Defaults: Enabled.

Command Modes: CONFIGURATION

Command History: Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information: By default, when you enable PIM-SM snooping, a switch floods all multicast traffic to the PIM designated router (DR), including unnecessary multicast packets. To minimize the traffic sent over the network to the designated router, you can disable designated-router flooding.

When designated-router flooding is disabled, PIM-SM snooping only forwards the multicast traffic, which belongs to a multicast group for which the switch receives a join request, on the port connected towards the designated router.

If the PIM DR flood is not disabled (default setting):

- Multicast traffic is transmitted on the egress port towards the PIM DR if the port is not the incoming interface.
- Multicast traffic for an unknown group is sent on the port towards the PIM DR. When DR flooding is disabled, multicast traffic for an unknown group is dropped.

Related Commands:

- `ip pim sparse-mode` Enable PIM-SM snooping.

show ip pim bsr-router

View information on the Bootstrap router.

Syntax: show ip pim bsr-router

Command Modes: EXEC

EXEC Privilege

Command History: Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
show ip pim interface

View information on the interfaces with IP PIM enabled.

**Syntax**

```
show ip pim interface
```

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

Figure 36-3. show ip pim interface Command Example

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>Ver/Mode</th>
<th>Nbr Count</th>
<th>Query Intvl</th>
<th>DR Prio</th>
<th>DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.21.200.254</td>
<td>Gi 7/9</td>
<td>v2/S</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>172.21.200.254</td>
</tr>
<tr>
<td>172.60.1.2</td>
<td>Gi 7/11</td>
<td>v2/S</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>172.60.1.2</td>
</tr>
<tr>
<td>192.3.1.1</td>
<td>Gi 7/16</td>
<td>v2/S</td>
<td>1</td>
<td>30</td>
<td>1</td>
<td>192.3.1.1</td>
</tr>
<tr>
<td>192.4.1.1</td>
<td>Gi 13/5</td>
<td>v2/S</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>192.4.1.1</td>
</tr>
<tr>
<td>172.21.110.1</td>
<td>Gi 13/6</td>
<td>v2/S</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>172.21.110.1</td>
</tr>
<tr>
<td>172.21.203.1</td>
<td>Gi 13/7</td>
<td>v2/S</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>172.21.203.1</td>
</tr>
</tbody>
</table>

**Table 36-1. show ip pim interface Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Lists the IP addresses of the interfaces participating in PIM.</td>
</tr>
<tr>
<td>Interface</td>
<td>List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.</td>
</tr>
<tr>
<td>Ver/Mode</td>
<td>Displays the PIM version number and mode for each interface participating in PIM.</td>
</tr>
<tr>
<td>• v2 = PIM version 2</td>
<td></td>
</tr>
<tr>
<td>• S = PIM Sparse mode</td>
<td></td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Displays the number of PIM neighbors discovered over this interface.</td>
</tr>
<tr>
<td>Query Intvl</td>
<td>Displays the query interval for Router Query messages on that interface (configured with <code>ip pim query-interval</code> command).</td>
</tr>
<tr>
<td>DR Prio</td>
<td>Displays the Designated Router priority value configured on the interface (ip pim dr-priority command).</td>
</tr>
<tr>
<td>DR</td>
<td>Displays the IP address of the Designated Router for that interface.</td>
</tr>
</tbody>
</table>
show ip pim neighbor

View PIM neighbors.

Syntax

show ip pim neighbor

Command Modes

EXEC

EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 36-4. show ip pim neighbor Command Example

Table 36-2. show ip pim neighbor Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor address</td>
<td>Displays the IP address of the PIM neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.</td>
</tr>
<tr>
<td>Uptime/expires</td>
<td>Displays the amount of time the neighbor has been up followed by the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).</td>
</tr>
<tr>
<td>Ver</td>
<td>Displays the PIM version number.</td>
</tr>
<tr>
<td>DR</td>
<td>Displays the Designated Router priority and the mode.</td>
</tr>
<tr>
<td>DR prio/Mode</td>
<td></td>
</tr>
</tbody>
</table>

show ip pim rp

View all multicast groups-to-RP mappings.

Syntax

show ip pim rp [mapping | group-address]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mapping</td>
<td>(OPTIONAL) Enter the keyword mapping to display the multicast groups-to-RP mapping and information on how RP is learnt.</td>
</tr>
<tr>
<td>group-address</td>
<td>(OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.</td>
</tr>
</tbody>
</table>
show ip pim snooping interface

Display information on VLAN interfaces with PIM-SM snooping enabled.

**Syntax**

```bash
show ip pim snooping interface [vlan vlan-id]
```

**Parameters**

- **vlan vlan-id**: (OPTIONAL) Enter a VLAN ID to display information about a specified VLAN configured for PIM-SM snooping. The valid VLAN ID range is from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- **Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.
Example

Figure 36-8.  show ip pim snooping interface Command Example

Table 36-3.  show ip pim snooping interface Command Example Fields

show ip pim snooping neighbor

Display information on PIM neighbors learned through PIM-SM snooping.

Syntax

show ip pim snooping neighbor [vlan vlan-id]

Parameters

vlan vlan-id  (OPTIONAL) Enter a VLAN ID to display information about PIM neighbors that by PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.

Command Modes

EXEC

EXEC Privilege

Command History

Version 9.2(0.0)  Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 36-9.  show ip pim snooping neighbor Command Example
show ip pim snooping tib

Display information from the tree information base (TIB) discovered by PIM-SM snooping about multicast group members and states.

**Syntax**

show ip pim snooping tib [vlan vlan-id] [group-address [source-address]]

**Parameters**

- **vlan vlan-id** (OPTIONAL) Enter a VLAN ID to display TIB information discovered by PIM-SM snooping on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.
- **group-address** (OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D) to display TIB information discovered by PIM-SM snooping for a specified multicast group.
- **source-address** (OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D) to display TIB information discovered by PIM-SM snooping for a specified multicast source.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Figure 36-10.  show ip pim snooping tib Command Example

Table 36-5.  show ip pim snooping tib Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the entry in the PIM multicast snooping database.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the PIM multicast route table.</td>
</tr>
<tr>
<td>expires</td>
<td>Displays the amount of time until the entry expires and is removed from the database.</td>
</tr>
<tr>
<td>RP</td>
<td>Displays the IP address of the RP/source for this entry.</td>
</tr>
<tr>
<td>flags</td>
<td>List the flags to define the entries:</td>
</tr>
<tr>
<td></td>
<td>• S = PIM Sparse Mode</td>
</tr>
<tr>
<td></td>
<td>• C = directly connected</td>
</tr>
<tr>
<td></td>
<td>• L = local to the multicast group</td>
</tr>
<tr>
<td></td>
<td>• P = route was pruned</td>
</tr>
<tr>
<td></td>
<td>• R = the forwarding entry is pointing toward the RP</td>
</tr>
<tr>
<td></td>
<td>• F = FTOS is registering this entry for a multicast source</td>
</tr>
<tr>
<td></td>
<td>• T = packets were received via Shortest Tree Path</td>
</tr>
<tr>
<td></td>
<td>• J = first packet from the last hop router is received and the entry is ready to switch to SPT</td>
</tr>
<tr>
<td></td>
<td>• K = acknowledge pending state</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) interface towards the RP/source.</td>
</tr>
</tbody>
</table>
show ip pim summary

View information about PIM-SM operation.

Syntax
show ip pim summary

Command Modes
EXEC
EXEC Privilege

Command History
| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |

Table 36-5.  show ip pim snooping tib Command Example Fields  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPF neighbor</td>
<td>Displays the next hop from this interface towards the RP/source.</td>
</tr>
</tbody>
</table>
| Outgoing interface list: | Lists the interfaces that meet one of the following criteria:  
  • a directly connect member of the Group.  
  • statically configured member of the Group.  
  • received a (*,G) Join message. |
show ip pim tib

View the PIM tree information base (TIB).

Syntax

show ip pim tib [group-address [source-address]]

Parameters

- **group-address**: (OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).
- **source-address**: (OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 9.2(0.0)**: Introduced on the MXL 10/40GbE Switch IO Module.
**Example**

Figure 36-12. show ip pim tib Command Example

```
FTOS# show ip pim tib
PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT, M - MSDP created entry, A - Candidate for MSDP Advertisement, K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 226.1.1.1), uptime 01:29:19, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0

(*, 226.1.1.2), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0

(*, 226.1.1.3), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0

(*, 226.1.1.4), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0
```

Table 36-6. show ip pim tib Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the entry in the multicast PIM database.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the PIM route table.</td>
</tr>
<tr>
<td>expires</td>
<td>Displays the amount of time until the entry expires and is removed from the database.</td>
</tr>
<tr>
<td>RP</td>
<td>Displays the IP address of the RP/source for this entry.</td>
</tr>
<tr>
<td>flags</td>
<td>List the flags to define the entries:</td>
</tr>
<tr>
<td></td>
<td>• D = PIM Dense Mode</td>
</tr>
<tr>
<td></td>
<td>• S = PIM Sparse Mode</td>
</tr>
<tr>
<td></td>
<td>• C = directly connected</td>
</tr>
<tr>
<td></td>
<td>• L = local to the multicast group</td>
</tr>
<tr>
<td></td>
<td>• P = route was pruned</td>
</tr>
<tr>
<td></td>
<td>• R = the forwarding entry is pointing toward the RP</td>
</tr>
<tr>
<td></td>
<td>• F = FTOS is registering this entry for a multicast source</td>
</tr>
<tr>
<td></td>
<td>• T = packets were received via Shortest Tree Path</td>
</tr>
<tr>
<td></td>
<td>• J = first packet from the last hop router is received and the entry is ready to switch to SPT</td>
</tr>
<tr>
<td></td>
<td>• K = acknowledge pending state</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) interface towards the RP/source.</td>
</tr>
<tr>
<td>RPF neighbor</td>
<td>Displays the next hop from this interface towards the RP/source.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Lists the interfaces that meet one of the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• a directly connect member of the Group.</td>
</tr>
<tr>
<td></td>
<td>• statically configured member of the Group.</td>
</tr>
<tr>
<td></td>
<td>• received a (*.G) Join message.</td>
</tr>
</tbody>
</table>
show running-config pim

Display the current configuration of PIM-SM snooping.

Syntax
show running-config pim

Command Modes
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

Related Commands

- `ip pim sparse-mode`: Enable PIM-SM snooping.

Example

Command Example: show running-config pim

```
FTOS# show running-config pim
!
ip pim snoop enable
```
IPv6 PIM-Sparse Mode Commands

The IPv6 PIM-SM commands are:
- ipv6 pim bsr-border
- ipv6 pim bsr-candidate
- ipv6 pim dr-priority
- ipv6 pim join-filter
- ipv6 pim query-interval
- ipv6 pim neighbor-filter
- ipv6 pim register-filter
- ipv6 pim rp-address
- ipv6 pim rp-candidate
- ipv6 pim sparse-mode
- ipv6 pim spt-threshold
- show ipv6 pim bsr-router
- show ipv6 pim interface
- show ipv6 pim neighbor
- show ipv6 pim rp
- show ipv6 pim tib

ipv6 pim bsr-border
Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Syntax
ipv6 pim bsr-border

Defaults
Disabled

Command Modes
INTERFACE

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
This command is applied to the subsequent PIM-BSR messages. Existing BSR advertisements are cleaned up by time-out.

ipv6 pim bsr-candidate
Configure the router as a bootstrap (BSR) candidate.

Syntax
ipv6 pim bsr-candidate interface [hash-mask-length] [priority]

To disable the bootstrap candidate, use the no ipv6 pim bsr-candidate command.
ipv6 pim dr-priority

Change the designated router (DR) priority for the IPv6 interface.

**Syntax**

```
ipv6 pim dr-priority priority-value
```

To remove the DR priority value assigned, use the `no ipv6 pim dr-priority` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-value</td>
<td>Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1.</td>
</tr>
</tbody>
</table>

**Defaults**

1

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same DR priority value, the interface with the largest interface IP address becomes the Designated Router.

ipv6 pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

**Syntax**

```
ipv6 pim join-filter access-list
```
ipv6 pim query-interval

Change the frequency of IPv6 PIM router-query messages.

**Syntax**

ipv6 pim query-interval seconds

To return to the default value, use the `no ipv6 pim query-interval seconds` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is 30 seconds.</td>
</tr>
</tbody>
</table>

**Defaults**

30 seconds

**Command Modes**

INTERFACE

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

ipv6 pim neighbor-filter

Prevent the system from forming a PIM adjacency with a neighboring system.

**Syntax**

ipv6 pim neighbor-filter {access-list}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>Enter the name of a standard access list. Maximum 16 characters.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
ipv6 pim register-filter

Configure the source DR so that it does not send register packets to the RP for the specified sources and groups.

**Syntax**

```
ipv6 pim register-filter access-list
```

**Parameters**

- `access-list` Enter the name of the extended ACL that contains the sources and groups to filter.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

| Version 9.2(0.0) | Introduced on the MXL 10/40GbE Switch IO Module. |

**Example**

```
Force10(conf)#ipv6 pim register-filter REG-FIL_ACL
Force10(conf)#ipv6 access-list REG-FIL_ACL
Force10(conf-ipv6-acl)#deny ipv6 165:87:34::10/128 ff0e::225:1:2:0/112
Force10(conf-ipv6-acl)#permit ipv6 any any
Force10(conf-ipv6-acl)#exit
```

ipv6 pim rp-address

Configure a static PIM rendezvous point (RP) address for a group. First-hop routers use this address to send register packets on behalf of the source multicast host.

**Syntax**

```
ipv6 pim rp-address address group-address group-address mask override
```

To remove an RP address, use the `no ipv6 pim re-address address group-address mask override`.

**Parameters**

- `address` Enter the IPv6 RP address in the `x:x:x:x::x` format.
  
  **NOTE:** The `::` notation specifies successive hexadecimal fields of zero.

- `group-address` `group-address mask` Enter the keyword `group-address` then the group address in the `x:x:x::x` format and then the mask in `/nn` format to assign that group address to the RP.
  
  **NOTE:** The `::` notation specifies successive hexadecimal fields of zero.

- `override` Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/disable.
  
  **NOTE:** This option is applicable to multicast group range.

**Defaults**

No default values or behavior

**Command Modes**

CONFIGURATION
The RP addresses are stored in the order in which they are entered. RP addresses learned via BSR take priority over static RP addresses.

Without the override option, BSR-advertised RPs updates take precedence over the statically configured RPs.

**ipv6 pim rp-candidate**

Specify an interface as an RP candidate.

**Syntax**

```
ipv6 pim rp-candidate interface [priority-value]
```

**Parameters**

- **interface**
  
  Enter the following keywords and slot/port or number information:
  
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  
  - For a Port Channel interface, enter the keyword `port-channel` then a number:
  
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

- **priority-value** (OPTIONAL) Enter a number as the priority of this RP Candidate, which is included in the Candidate-RP-Advertisements. The range is from 0 (highest) to 255 (lowest).

**Defaults**

None

**Command Modes**

CONFIGURATION

**Usage Information**

The interface must be enabled (use the no shutdown command) and not have the switchport command configured. Also enable Multicast globally. PIM is supported on the port-channel interface.

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

Enable IPv6 PIM sparse mode on the interface.

**Syntax**

```
ipv6 pim sparse-mode
```

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Usage Information**

The interface must be enabled (use the no shutdown command) and not have the switchport command configured. Also enable Multicast globally. PIM is supported on the port-channel interface.

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.
ipv6 pim spt-threshold

Specifies when a PIM leaf router should join the shortest path tree.

Syntax
ipv6 pim spt-threshold \{kbps | infinity\}

To return to the default value, use the no ipv6 pim spt-threshold command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kbps</td>
<td>Enter a traffic rate in kilobytes per second. The range is from 0 to 4294967 kbps. The default is 10 kbps.</td>
</tr>
<tr>
<td>infinity</td>
<td>Enter the keyword infinity to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).</td>
</tr>
</tbody>
</table>

Defaults
10 kbps

Command Modes
CONFIGURATION

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.

show ipv6 pim bsr-router

View information on the bootstrap router (v2).

Syntax
show ipv6 pim bsr-router

Command Modes
EXEC
EXEC Privilege

Example

Figure 36-13. show ipv6 pim bsr-router Command Example

FTOS#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
BSR address: 14::2
Uptime: 00:02:54, BSR Priority: 0, Hash mask length: 126
Next bootstrap message in 00:00:06

This system is a candidate BSR
Candidate BSR address: 14::2, priority: 0, hash mask length: 126
FTOS
show ipv6 pim interface

Display IPv6 PIM enabled interfaces.

Syntax

show ipv6 pim interface

Command Modes

EXEC
EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 36-14.  show ipv6 pim interface Command Example

```
FTOS#show ipv6 pim interface
Interface Ver/   Nbr    Query  DR  Mode  Count  Intvl  Prio
      Mode   Count  Intvl  Prio
Gi 10/3   v2/S   1      30     1
      Address : fe80::201:e8ff:fe02:140f
      DR      : this router
Gi 10/11  v2/S   0      30     1
      Address : fe80::201:e8ff:fe02:1417
      DR      : this router
```

show ipv6 pim neighbor

Displays IPv6 PIM neighbor information.

Syntax

show ipv6 pim neighbor [detail]

Parameters

detail  (OPTIONAL) Enter the keyword detail to displayed PIM neighbor detailed information.

Command Modes

EXEC
EXEC Privilege

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 36-15.  show ipv6 pim neighbor detail Command Example

```
FTOS#show ipv6 pim neighbor detail
Neighbor                  Interface      Uptime/Expires     Ver  DR  Prio/Mode
Address                                                          Prio/Mode
fe80::201:e8ff:fe00:6265  Gi 10/3        00:07:39/00:01:42  v2  1  / S
165:87:50::6
```


show ipv6 pim rp

View all IPv6 multicast groups-to-rendezvous point (RP) mappings.

Syntax
show ipv6 pim rp [mapping | group-address]

Parameters
- mapping: (OPTIONAL) Enter the keyword mapping to display the multicast groups-to-RP mapping and information on how RP is learnt.
- group-address: (OPTIONAL) Enter the multicast group address in the x:x:x:x format to view RP mappings for a specific group.

Command Modes
- EXEC
- EXEC Privilege

Command History
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example 1
Figure 36-16. show ipv6 pim rp Command Example

```
FTOS#show ipv6 pim rp
Group   RP
ff0e::225:1:2:1  14::1
ff0e::225:1:2:2  14::1
ff0e::226:1:2:1  14::1
ff0e::226:1:2:2  14::1
FTOS
``` 

Example 2
Figure 36-17. show ipv6 pim rp mapping Command Example

```
FTOS#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
   RP: 14::1, v2
     Info source: 14::1, via bootstrap, priority 192
     Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
   RP: 14::2, v2
FTOS
``` 

show ipv6 pim tib

View the IPv6 PIM multicast-routing database (tree information base—tib).

Syntax
show ipv6 pim tib [group-address [source-address]]

Parameters
- group-address: (OPTIONAL) Enter the multicast group address in the x:x:x:x format to view RP mappings for a specific group.
  - NOTE: The :: notation specifies successive hexadecimal fields of zero.
- source-address: (OPTIONAL) Enter the source address in the x:x:x:x format.
  - NOTE: The :: notation specifies successive hexadecimal fields of zero.
Figure 36-18. show ipv6 pim tib Command Example

FTOS

show ipv6 pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
    R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
    M - MSDP created entry, A - Candidate for MSDP Advertisement
    K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires 00:00:00, flags: CJ
    RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
    Outgoing interface list:
        GigabitEthernet 10/11

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00, flags: CJ
    RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
    Outgoing interface list:
        GigabitEthernet 10/11

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00, flags: CJ
    RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
    Outgoing interface list:
        GigabitEthernet 10/11

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires 00:00:00, flags: CJ
    RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
    Outgoing interface list:
        GigabitEthernet 10/11

FTOS
Private VLAN (PVLAN)

Commands

This chapter describes the following commands:

- ip local-proxy-arp
- private-vlan mode
- private-vlan mapping secondary-vlan
- show interfaces private-vlan
- show vlan private-vlan
- show vlan private-vlan mapping
- switchport mode private-vlan

For more information, also refer to the following commands. The command output is augmented in FTOS 7.8.1.0 to provide PVLAN data:

- show arp in Chapter 21, IPv4 Routing
- show vlan in Chapter 28, Layer 2

Private virtual local area networks (VLANs) extend the Dell Networking operating software (FTOS) security suite by providing Layer 2 isolation between ports within the same private VLAN. A private VLAN partitions a traditional VLAN into subdomains identified by a primary and secondary VLAN pair.

The FTOS private VLAN implementation is based on RFC 3069.
Private VLAN Concepts

Primary VLAN:
The primary VLAN is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — community VLAN and isolated VLAN:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

Community VLAN:
A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all promiscuous ports in the primary VLAN and vice-versa.
- Devices on a community VLAN can communicate with each other via member ports, while devices in an isolated VLAN cannot.

Isolated VLAN:
An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice-versa.

Port types:

- **Community port**: A community port is, by definition, a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.
- **Isolated port**: An isolated port is, by definition, a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- **Promiscuous port**: A promiscuous port is, by definition, a port that is allowed to communicate with any other port type.
- **Trunk port**: A trunk port, by definition, carries VLAN traffic across switches:
  - A trunk port in a PVLAN is always tagged.
  - Primary or secondary VLAN traffic is carried by the trunk port in tagged mode. The tag on the packet helps identify the VLAN to which the packet belongs.
  - A trunk port can also belong to a regular VLAN (non-private VLAN).

```
ip local-proxy-arp
```

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

**Syntax**

```
[no] ip local-proxy-arp
```

To disable Layer 3 communication between secondary VLANs in a private VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the primary VLAN.
To disable Layer 3 communication in a particular secondary VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the selected secondary VLAN.

**Note:** Even after `ip-local-proxy-arp` is disabled (no `ip-local-proxy-arp`) in a secondary VLAN, Layer 3 communication may happen between some secondary VLAN hosts, until the ARP timeout happens on those secondary VLAN hosts.

**Defaults**
Layer 3 communication is disabled between secondary VLANs in a private VLAN.

**Command Modes**
INTERFACE VLAN

**Command History**
- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**
- `private-vlan mode`
  Sets the mode of the selected VLAN to community, isolated, or primary.
- `private-vlan mapping secondary-vlan`
  Maps the secondary VLANs to the selected primary VLAN.
- `show arp`
  Displays the ARP table.
- `show interfaces private-vlan`
  Displays the type and status of the PVLAN interfaces.
- `show vlan private-vlan`
  Displays PVLANs and/or interfaces that are part of a PVLAN.
- `switchport mode private-vlan`
  Sets PVLAN mode of the selected port.

---

### private-vlan mode

Set PVLAN mode of the selected VLAN to community, isolated, or primary.

**Syntax**

```
[no] private-vlan mode {community | isolated | primary}
```

To remove the PVLAN configuration, use the `no private-vlan mode {community | isolated | primary}` command.

**Parameters**

- **community**
  Enter `community` to set the VLAN as a community VLAN, as described above.
- **isolated**
  Enter `isolated` to configure the VLAN as an isolated VLAN, as described above.
- **primary**
  Enter `primary` to configure the VLAN as a primary VLAN, as described above.

**Defaults**
none

**Command Modes**
INTERFACE VLAN

**Command History**
- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**
The VLAN:
- Can be in only one mode, either community, isolated, or primary.
- Mode can be set to community or isolated even before associating it to a primary VLAN. This secondary VLAN will continue to work normally as a normal VLAN even though it is not associated to a primary VLAN. (A syslog message indicates this.)
- Must not have a port in it when the VLAN mode is being set.
Only ports (and port channels) configured as promiscuous, host, or PVLAN trunk ports (as described above) can be added to the PVLAN. No other regular ports can be added to the PVLAN.

After using this command to configure a VLAN as a primary VLAN, use the `private-vlan mapping secondary-vlan` command to map secondary VLANs to this VLAN.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>private-vlan mapping secondary-vlan</code></td>
<td>Sets the mode of the selected VLAN to primary and then associate secondary VLANs to it.</td>
</tr>
<tr>
<td><code>show interfaces private-vlan</code></td>
<td>Displays the type and status of PVLAN interfaces.</td>
</tr>
<tr>
<td><code>show vlan private-vlan</code></td>
<td>Displays the PVLANs and/or interfaces that are part of a PVLAN.</td>
</tr>
<tr>
<td><code>show vlan private-vlan mapping</code></td>
<td>Displays the primary-secondary VLAN mapping.</td>
</tr>
<tr>
<td><code>switchport mode private-vlan</code></td>
<td>Sets the PVLAN mode of the selected port.</td>
</tr>
</tbody>
</table>

**private-vlan mapping secondary-vlan**

Map secondary VLANs to the selected primary VLAN.

**Syntax**

```plaintext
[no] private-vlan mapping secondary-vlan vlan-list
```

To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan` command.

**Parameters**

- `vlan-list` Enter the list of secondary VLANs to associate with the selected primary VLAN, as described above. The list can be in comma-delimited or hyphenated-range format, following the convention for range input.

**Defaults**

none

**Command Modes**

INTERFACE VLAN

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

The list of secondary VLANs can be:

- Specified in comma-delimited or hyphenated-range format.
- Specified with this command even before they have been created.
- Amended by specifying the new secondary VLAN to be added to the list.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>private-vlan mode</code></td>
<td>Sets the mode of the selected VLAN to community, isolated, or primary.</td>
</tr>
<tr>
<td><code>show interfaces private-vlan</code></td>
<td>Displays the type and status of PVLAN interfaces.</td>
</tr>
<tr>
<td><code>show vlan private-vlan</code></td>
<td>Displays the PVLANs and/or interfaces that are part of a PVLAN.</td>
</tr>
<tr>
<td><code>show vlan private-vlan mapping</code></td>
<td>Displays the primary-secondary VLAN mapping.</td>
</tr>
<tr>
<td><code>switchport mode private-vlan</code></td>
<td>Sets the PVLAN mode of the selected port.</td>
</tr>
</tbody>
</table>
show interfaces private-vlan
Display type and status of PVLAN interfaces.

Syntax
show interfaces private-vlan [interface interface]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface</td>
<td>(OPTIONAL) Enter the keyword interface, followed by the ID of the specific interface for which to display PVLAN status.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>EXEC Privilege</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

Usage Information

This command has two types of display — a list of all PVLAN interfaces or for a specific interface. Examples of both types of output are shown below.

Examples

**Figure 37-1. show interfaces private-vlan Command Example**

```
FTOS# show interfaces private-vlan
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
TenGig 2/1 10   Primary    Promiscuous    Up
TenGig 2/2 100  Isolated   Host           Down
TenGig 2/3 10   Primary    Trunk          Up
TenGig 2/4 101  Community  Host           Up
```

**Figure 37-2. show interfaces private-vlan (Specific) Command Example**

```
FTOS# show interfaces private-vlan TenGig 2/2
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
TenGig 2/2 100  Isolated   Host Up
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays type of interface and associated slot and port number</td>
</tr>
<tr>
<td>Vlan</td>
<td>Displays the VLAN ID of the designated interface</td>
</tr>
<tr>
<td>PVLAN-Type</td>
<td>Displays the type of VLAN in which the designated interface resides</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Displays the PVLAN port type of the designated interface.</td>
</tr>
<tr>
<td>Status</td>
<td>States whether the interface is operationally up or down.</td>
</tr>
</tbody>
</table>

Table 37-1 defines the fields in the output, above.

**Table 37-1. show interfaces Command Description**

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>private-vlan mode</td>
<td>Sets the mode of the selected VLAN to community, isolated, or primary.</td>
</tr>
<tr>
<td>show vlan private-vlan</td>
<td>Displays the PVLANs and/or interfaces that are part of a PVLAN.</td>
</tr>
</tbody>
</table>
show vlan private-vlan

Display PVLANs and/or interfaces that are part of a PVLAN.

**Syntax**

show vlan private-vlan [community | interface | isolated | primary | primary_vlan | interface interface]

**Parameters**

- **community**: (OPTIONAL) Enter the keyword community to display VLANs configured as community VLANs, along with their interfaces.
- **interface**: (OPTIONAL) Enter the keyword community to display VLANs configured as community VLANs, along with their interfaces.
- **isolated**: (OPTIONAL) Enter the keyword isolated to display VLANs configured as isolated VLANs, along with their interfaces.
- **primary**: (OPTIONAL) Enter the keyword primary to display VLANs configured as primary VLANs, along with their interfaces.
- **primary_vlan**: (OPTIONAL) Enter a private VLAN ID or secondary VLAN ID to display interface details about the designated PVLAN.
- **interface interface**: (OPTIONAL) Enter the keyword interface and an interface ID to display the PVLAN configuration of the designated interface.

**Defaults**

none

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Examples of all types of command output are shown below. The first type of output is the result of not entering an optional keyword. It displays a detailed list of all PVLANs and their member VLANs and interfaces. The other types of output show details about PVLAN subsets.

**Examples**

Figure 37-3. show vlan private-vlan Command Example

<table>
<thead>
<tr>
<th>FTOS# show vlan private-vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td>101</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>200</td>
</tr>
<tr>
<td>201</td>
</tr>
<tr>
<td>202</td>
</tr>
</tbody>
</table>
If the VLAN ID is that of a primary VLAN, then the entire private VLAN output will be displayed, as shown in Figure 37-8. If the VLAN ID is a secondary VLAN, only its primary VLAN and its particular secondary VLAN properties will be displayed, as shown in Figure 37-9.

### Figure 37-4. show vlan private-vlan Command Example (Primary)

<table>
<thead>
<tr>
<th>Primary Secondary Type</th>
<th>Active Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>TenGig 2/1,3</td>
</tr>
<tr>
<td>primary</td>
<td>TenGig 3/1,3</td>
</tr>
</tbody>
</table>

### Figure 37-5. show vlan private-vlan Command Example (Isolated)

<table>
<thead>
<tr>
<th>Primary Secondary Type</th>
<th>Active Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>TenGig 2/1,3</td>
</tr>
<tr>
<td>isolated</td>
<td>TenGig 2/2,4-6</td>
</tr>
<tr>
<td>isolated</td>
<td>TenGig 3/2,4-6</td>
</tr>
</tbody>
</table>

### Figure 37-6. show vlan private-vlan Command Example (Community)

<table>
<thead>
<tr>
<th>Primary Secondary Type</th>
<th>Active Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>TenGig 2/1,3</td>
</tr>
<tr>
<td>community</td>
<td>TenGig 2/7-10</td>
</tr>
<tr>
<td>primary</td>
<td>Po 10, 12-13</td>
</tr>
<tr>
<td>community</td>
<td>TenGig 3/1</td>
</tr>
<tr>
<td>community</td>
<td>TenGig 3/11-12</td>
</tr>
</tbody>
</table>

### Figure 37-7. show vlan private-vlan Command Example (Interface)

<table>
<thead>
<tr>
<th>Primary Secondary Type</th>
<th>Active Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>TenGig 2/1</td>
</tr>
</tbody>
</table>

### Figure 37-8. Output of show vlan private-vlan (primary)

<table>
<thead>
<tr>
<th>Primary Secondary Type</th>
<th>Active Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>TenGig 2/1,3</td>
</tr>
<tr>
<td>102 isolated</td>
<td>TenGig 0/4</td>
</tr>
<tr>
<td>101 community</td>
<td>TenGig 2/7-10</td>
</tr>
</tbody>
</table>

### Figure 37-9. Output of show vlan private-vlan (secondary)

<table>
<thead>
<tr>
<th>Primary Secondary Type</th>
<th>Active Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Po 1</td>
</tr>
<tr>
<td>isolated</td>
<td>TenGig 0/2</td>
</tr>
<tr>
<td>isolated</td>
<td>TenGig 0/4</td>
</tr>
</tbody>
</table>
Table 37-2 defines the fields in the output.

### Table 37-2. show interfaces Command Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Displays the VLAN ID of the designated or associated primary VLAN(s)</td>
</tr>
<tr>
<td>Secondary</td>
<td>Displays the VLAN ID of the designated or associated secondary VLAN(s)</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of VLAN in which the listed interfaces reside</td>
</tr>
<tr>
<td>Active</td>
<td>States whether the interface is operationally up or down</td>
</tr>
<tr>
<td>Ports</td>
<td>Displays the interface IDs in the listed VLAN.</td>
</tr>
</tbody>
</table>

The output of this command (Figure 37-10), displays the community and isolated VLAN IDs that are associated with each primary VLAN.

Figure 37-10. show vlan private-vlan mapping Command Output

FTOS# show vlan private-vlan mapping
Private_vlan:
    Primary : 100
    Isolated: 102
    Community: 101
    Unknown : 200

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>private-vlan mode</td>
<td>Sets the mode of the selected VLAN to either community or isolated.</td>
</tr>
<tr>
<td>show interfaces private-vlan</td>
<td>Displays the type and status of PVLAN interfaces.</td>
</tr>
<tr>
<td>show vlan private-vlan mapping</td>
<td>Displays the primary-secondary VLAN mapping.</td>
</tr>
<tr>
<td>switchport mode private-vlan</td>
<td>Sets the PVLAN mode of the selected port.</td>
</tr>
</tbody>
</table>
**switchport mode private-vlan**

Set PVLAN mode of the selected port.

**Syntax**

```
[no] switchport mode private-vlan {host | promiscuous | trunk}
```

To remove the PVLAN mode from the selected port, use the `no switchport mode private-vlan` command.

**Parameters**

- **host**: Enter `host` to configure the selected port or port channel as an isolated interface in a PVLAN, as described above.
- **promiscuous**: Enter `promiscuous` to configure the selected port or port channel as an promiscuous interface, as described above.
- **trunk**: Enter `trunk` to configure the selected port or port channel as a trunk port in a PVLAN, as described above.

**Defaults**

disabled

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is demonstrated below.

**Example**

```
Figure 37-11. switchport mode private-vlan Command Example

FTOS(conf)
FTOS(conf)#interface TenGigabitEthernet 2/1
FTOS(conf-if-te-2/1)#switchport mode private-vlan promiscuous

FTOS(conf)
FTOS(conf)#interface TenGigabitEthernet 2/2
FTOS(conf-if-te-2/2)#switchport mode private-vlan host

FTOS(conf)
FTOS(conf)#interface TenGigabitEthernet 2/3
FTOS(conf-if-te-2/3)#switchport mode private-vlan trunk

FTOS(conf)
FTOS(conf)#interface port-channel 10
FTOS(conf-if-te-2/3)#switchport mode private-vlan promiscuous
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>private-vlan mode</td>
<td>Sets the mode of the selected VLAN to either community or isolated.</td>
</tr>
<tr>
<td>private-vlan mapping</td>
<td>Sets the mode of the selected VLAN to primary and then associate secondary VLANs to it.</td>
</tr>
<tr>
<td>secondary-vlan</td>
<td></td>
</tr>
<tr>
<td>show interfaces private-vlan</td>
<td>Displays the type and status of PVLAN interfaces.</td>
</tr>
<tr>
<td>show vlan private-vlan mapping</td>
<td>Display the primary-secondary VLAN mapping.</td>
</tr>
</tbody>
</table>
Per-VLAN Spanning Tree Plus (PVST+)

Overview

The FTOS implementation of PVST+ (Per-VLAN Spanning Tree plus) is based on the IEEE 802.1w standard Spanning Tree Protocol, but it creates a separate spanning tree for each VLAN configured.

Commands

The FTOS PVST+ commands are:

- disable
- description
- edge-port bpdufilter default
- protocol spanning-tree pvst
- show spanning-tree pvst
- spanning-tree pvst
- spanning-tree pvst err-disable
- tc-flush-standard
- vlan bridge-priority
- vlan forward-delay
- vlan hello-time
- vlan max-age

Note: For easier command line entry, the plus (+) sign is not used at the command line.

disable

Disable PVST+ globally.

Syntax
disable

To enable PVST+, enter no disable.

Defaults
PVST+ is disabled

Command Modes
CONFIGURATION (conf-pvst)

Command History

<table>
<thead>
<tr>
<th>Version 8.3.16.1</th>
<th>Introduced on MXL 10/40GbE Switch IO Module</th>
</tr>
</thead>
</table>

Per-VLAN Spanning Tree Plus (PVST+) | 741
Related Commands

---

**description**

Enter a description of the PVST+

**Syntax**

description {description}

To remove the description, use the no description {description} command.

**Parameters**

- **description**
  
  Enter a description to identify the Spanning Tree (80 characters maximum).

**Defaults**

No default behavior or values

**Command Modes**

SPANNING TREE PVST+ (The prompt is “config-pvst”)

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- protocol spanning-tree pvst Enter SPANNING TREE mode on the switch.

---

**edge-port bpdufilter default**

Enable BPDU Filter globally to filter transmission of BPDU on port fast enabled interfaces.

**Syntax**

degree-port bpdufilter default

To disable global bpdu filter default, use the no edge-port bpdufilter default command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION (The prompt is “config-pvst”.)

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
extend system-id

Use Extend System ID to augment the Bridge ID with a VLAN ID so that PVST+ differentiate between BPDUs for each VLAN. If for some reason a VLAN receives a BPDU meant for another VLAN, PVST+ will then not detect a loop, and both ports can remain in forwarding state.

Syntax
extend system-id

Defaults
Disabled

Command Modes
PROTOCOL PVST

Command History

Figure 38-1. Command Example

FTOS(conf-pvst)#do show spanning-tree pvst vlan 2 brief
VLAN 2
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32768, Address 001e.c9f1.00f3
We are the root of Vlan 2
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally

Interface Name         PortID     Prio Cost    Sts      Cost    Bridge ID
PortID                ----------     ------ ------  -------  ----------
--------------------  -------- ------- ------ ----------
Po 23                 128.24  128  1600    FWD   0  32768
001e.c9f1.00f3  128.24
Te 5/41                128.450 128  2000    DIS   0  32768
001e.c9f1.00f3  128.450
Te 5/50                128.459 128  2000    FWD   0  32768
001e.c9f1.00f3  128.459

Interface Name        Role  PortID     Prio Cost    Sts      Cost    Link-type
NameEdge BpduFilter  ----------     ------ ------  -------  ----------
--------  --------     -------- ------- ------ ----------
Po 23 Desg  128.24  128  1600    FWD   0  P2P  No
No
Te 5/41 Dis  128.450 128  2000    DIS   0  P2P  No
No
Te 5/50 Desg  128.459 128  2000    FWD   0  P2P  No

Related Commands
protocol spanning-tree pvst Enter SPANNING TREE mode on the switch.
**protocol spanning-tree pvst**
Enter the PVST+ mode to enable PVST+ on a device.

**Syntax**

```plaintext
protocol spanning-tree pvst
```

To disable PVST+, use the `disable` command.

**Defaults**

This command has no default value or behavior.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

Figure 38-2. Configuring with protocol spanning-tree pvst Command

```plaintext
FTOS#conf
FTOS(conf)#protocol spanning-tree pvst
FTOS(conf-pvst)#no disable
FTOS(conf-pvst)#vlan 2 bridge-priority 4096
FTOS(conf-pvst)#vlan 3 bridge-priority 16384
FTOS(conf-pvst)#
FTOS(conf-pvst)#show config
!
protocol spanning-tree pvst
no disable
vlan 2 bridge-priority 4096
vlan 3 bridge-priority 16384
FTOS#
```

**Usage Information**

Once PVST+ is enabled, the device runs an STP instance for each VLAN it supports.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disable PVST+.</td>
</tr>
<tr>
<td>show spanning-tree pvst</td>
<td>Display the PVST+ configuration.</td>
</tr>
</tbody>
</table>

**show spanning-tree pvst**

View the Per-VLAN Spanning Tree configuration.

**Syntax**

```plaintext
show spanning-tree pvst [vlan vlan-id] [brief] [guard]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan vlan-id</td>
<td>(OPTIONAL) Enter the keyword <code>vlan</code> followed by the VLAN ID. Range: 1 to 4094</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword <code>brief</code> to view a synopsis of the PVST+ configuration information.</td>
</tr>
</tbody>
</table>
Per-VLAN Spanning Tree Plus (PVST+)

- **Interface**: (OPTIONAL) Enter one of the interface keywords along with the slot/port information:
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

- **guard**: (OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on a PVST interface and the current port state.

**Defaults**: No default behavior or values

**Command Modes**: EXEC

**EXEC Privilege**

**Command History**: Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example 1**

**Figure 38-3. show spanning-tree pvst brief Command**

```
FTOS# show spanning-tree pvst vlan 2 brief
VLAN 2
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 001e.c9f1.00f3
We are the root of Vlan 2
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally

<table>
<thead>
<tr>
<th>Interface</th>
<th>PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts</th>
<th>Cost</th>
<th>Designated Bridge ID</th>
<th>PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Po 23</td>
<td>128.24</td>
<td>128</td>
<td>1600</td>
<td>FWD</td>
<td>0</td>
<td>32768 001e.c9f1.00f3</td>
<td>128.24</td>
</tr>
<tr>
<td>Te 5/41</td>
<td>128.450</td>
<td>128</td>
<td>2000</td>
<td>DIS</td>
<td>0</td>
<td>32768 001e.c9f1.00f3</td>
<td>128.450</td>
</tr>
<tr>
<td>Te 5/50</td>
<td>128.459</td>
<td>128</td>
<td>2000</td>
<td>FWD</td>
<td>0</td>
<td>32768 001e.c9f1.00f3</td>
<td>128.459</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts</th>
<th>Cost</th>
<th>Link-type</th>
<th>Edge</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Po 23</td>
<td>Desg</td>
<td>128.24</td>
<td>128</td>
<td>1600</td>
<td>FWD</td>
<td>0</td>
<td>P2P</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Te 5/41</td>
<td>Desg</td>
<td>128.450</td>
<td>128</td>
<td>2000</td>
<td>DIS</td>
<td>0</td>
<td>P2P</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Te 5/50</td>
<td>Desg</td>
<td>128.459</td>
<td>128</td>
<td>2000</td>
<td>FWD</td>
<td>0</td>
<td>P2P</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

FTOS#
Example 2  
**Figure 38-4. show spanning-tree pvst vlan Command**

```
FTOS#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 32768, Address 001e.c9f1.00f3
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally
We are the root of VLAN 2
Current root has priority 32768, Address 001e.c9f1.00f3
Number of topology changes 0, last change occurred 3d1h ago on

Port 24 (Port-channel 23) is designated Discarding
Port path cost 1600, Port priority 128, Port Identifier 128.24
Designated root has priority 32768, address 001e.c9f1.00f3
Designated bridge has priority 32768, address 001e.c9f1.00f3
Designated port id is 128.24 , designated path cost 0
Number of transitions to forwarding state 0
BPDU sent 8, received 0
The port is not in the Edge port mode, bpdu filter is disabled

Port 450 (TenGigabitEthernet 5/41) is disabled Discarding
Port path cost 2000, Port priority 128, Port Identifier 128.450
Designated root has priority 32768, address 001e.c9f1.00f3
Designated bridge has priority 32768, address 001e.c9f1.00f3
Designated port id is 128.450 , designated path cost 0
Number of transitions to forwarding state 0
BPDU sent 0, received 0
The port is not in the Edge port mode, bpdu filter is disabled

Port 459 (TenGigabitEthernet 5/50) is designated Forwarding
Port path cost 2000, Port priority 128, Port Identifier 128.459
Designated root has priority 32768, address 001e.c9f1.00f3
Designated bridge has priority 32768, address 001e.c9f1.00f3
Designated port id is 128.459 , designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 16, received 0
The port is not in the Edge port mode, bpdu filter is disabled
```

Example 3  
**Figure 38-5. show spanning-tree pvst command with EDS and LBK**

```
FTOS#show spanning-tree pvst vlan 2 interface tengigabitethernet 1/0
TenGigabitEthernet 1/0 of VLAN 2 is LBK_INC discarding
Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu filter :disable
Bpdu guard :disable
Bpdu guard shutdown-on-violation :disable
Root Guard: disable
Bpdu sent 152, received 27562
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID
--------- -------- ---- ------- --- ------- -------------------- --------
TenGig 1/0 128.1223 128 20000 EDS O 32768 0001.e800.a12b 128.1223
```
Example 4  
**Figure 38-6. show spanning-tree pvst with EDS and PVID**

```
FTOS#show spanning-tree pvst vlan 2 interface tengigabitethernet 1/0
TenGigabitEthernet 1/0 of VLAN 2 is PVID INC discarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Bpdu guard : disable
Bpdu guard shutdown-on-violation : disable
Root Guard: disable
Bpdu sent 1, received 0
Interface Designated
Name PortID Prio Cost Sts Cost Bridge ID PortID
----------------- -------- ---- ------- --- ------- -------------------- --------
TenGig 1/0 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example 5  
**Figure 38-7. show spanning-tree pvst guard Command**

```
FTOS#show spanning-tree pvst vlan 5 guard
Interface
Name Instance Sts Guard type Bpdu Filter
--------- -------- --------- ---------- -----------
TenGig 0/1 0 INCON(Root) Rootguard No
TenGig 0/2 0 FWD Loopguard No
TenGig 0/3 0 EDS(Shut) Bpduguard No
```

Table 38-1. **show spanning-tree pvst guard Command Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>PVST interface</td>
</tr>
<tr>
<td>Instance</td>
<td>PVST instance</td>
</tr>
<tr>
<td>Sts</td>
<td>Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut)</td>
</tr>
<tr>
<td>Guard Type</td>
<td>Type of STP guard configured (Root, Loop, or BPDU guard)</td>
</tr>
</tbody>
</table>
| Bpdu Filter         | Yes - Bpdu filter Enabled
|                     | No - Bpdu filter Disabled                                                  |

**Related Commands**

`spanning-tree pvst` Configure PVST+ on an interface.
spanning-tree pvst

Configure a PVST+ interface with one of the following settings: edge port with optional Bridge Port Data Unit (BPDU) guard, BPDU filter, port disablement if an error condition occurs, port priority or cost for a VLAN range, or root guard.

**Syntax**

```
spanning-tree pvst {edge-port [bpduguard [shutdown-on-violation] | bpdufilter] | err-disable | vlan vlan-range {cost number | priority value} | rootguard}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edge-port</td>
<td>Enter the keyword <code>edge-port</code> to configure the interface as a PVST+ edge port.</td>
</tr>
<tr>
<td>bpduguard</td>
<td>(OPTIONAL) Enter the keyword <code>bpduguard</code> to disable the port when it receives a BPDU.</td>
</tr>
<tr>
<td>shutdown-on-violation</td>
<td>(OPTIONAL) Enter the keyword <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.</td>
</tr>
<tr>
<td>bpdufilter</td>
<td>(OPTIONAL) Enter the keyword <code>bpdufilter</code> to stop sending and receiving BPDUs on port fast enabled ports.</td>
</tr>
<tr>
<td>err-disable</td>
<td>Enter the keyword <code>err-disable</code> to enable the port to be put into error-disable state (EDS) if an error condition occurs.</td>
</tr>
<tr>
<td>vlan vlan-range</td>
<td>Enter the keyword <code>vlan</code> followed by the VLAN number(s). Range: 1 to 4094.</td>
</tr>
<tr>
<td>cost number</td>
<td>Enter the keyword <code>cost</code> followed by the port cost value. Range: 1 to 200000.</td>
</tr>
<tr>
<td>priority value</td>
<td>Enter the keyword <code>priority</code> followed the Port priority value in increments of 16. Range: 0 to 240. Default: 128.</td>
</tr>
<tr>
<td>rootguard</td>
<td>Enter the keyword <code>rootguard</code> to enable root guard on a PVST+ port or port-channel interface.</td>
</tr>
</tbody>
</table>

**Defaults**

Not Configured

**Command Modes**

INTERFACE

**Command History**

| Version | Introduced on MXL 10/40GbE Switch IO Module |

**Usage Information**

The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an error disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action. When BPDU guard and BPDU filter is enabled on the port, then BPDU filter takes the highest precedence.
By default bpdu filtering on an interface is disabled.

**Note:** A port configured as an edge port, on a PVST switch, will immediately transition to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

![Example Figure 38-8. spanning-tree pvst vlan Command Example]

```
FTOS(conf-if-te-1/1)#spanning-tree pvst vlan 3 cost 18000
FTOS(conf-if-te-1/1)#end
FTOS(conf-if-te-1/1)#show config
!
interface TenGigabitEthernet 1/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
FTOS(conf-if-te-1/1)#end
FTOS#
```

**Related Commands**

- `show spanning-tree pvst` View PVST+ configuration

---

**spanning-tree pvst err-disable**

Place ports in an err-disabled state if they receive a PVST+ BPDU when they are members an untagged VLAN.

**Syntax**

```
spanning-tree pvst err-disable cause invalid-pvst-bpdu
```

**Defaults**

Enabled; ports are placed in err-disabled state if they receive a PVST+ BPDU when they are members of an untagged VLAN.

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Some non-Dell Networking systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1w BPDU and an untagged PVST+ BPDU.

Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, FTOS places the port in error-disable state. This behavior might result in the network not converging. To prevent FTOS from executing this action, use the command `no spanning-tree pvst err-disable cause invalid-pvst-bpdu`.

**Related Commands**

- `show spanning-tree pvst` View the PVST+ configuration.
**tc-flush-standard**

Enable the MAC address flushing upon receiving every topology change notification.

**Syntax**

tc-flush-standard

To disable, use the no tc-flush-standard command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

By default FTOS implements an optimized flush mechanism for PVST+. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this knob command can be turned on to enable flushing MAC addresses upon receiving every topology change notification.

**vlan bridge-priority**

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

**Syntax**

vlan <vlan-id> bridge-priority value

To return to the default value, enter no vlan bridge-priority command.

**Parameters**

- **vlan vlan-range**
  - Enter the keyword vlan followed by the VLAN number(s).
  - Range: 1 to 4094

- **bridge-priority value**
  - Enter the keyword bridge-priority followed by the bridge priority value in increments of 4096.
  - Range: 0 to 61440
  - Default: 32768

**Defaults**

32768

**Command Modes**

CONFIGURATION (conf-pvst)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- **vlan forward-delay** Change the time interval before FTOS transitions to the forwarding state
- **vlan hello-time** Change the time interval between BPDUs
- **vlan max-age** Change the time interval before PVST+ refreshes
- **show spanning-tree pvst** Display the PVST+ configuration
**vlan forward-delay**

Set the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

**Syntax**

```
vlan <vlan-id> forward-delay seconds
```

To return to the default setting, enter no vlan forward-delay command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan-range</code></td>
<td>Enter the keyword <code>vlan</code> followed by the VLAN number(s). Range: 1 to 4094</td>
</tr>
<tr>
<td><code>forward-delay</code></td>
<td>Enter the keyword <code>forward-delay</code> followed by the time interval, in seconds, that FTOS waits before transitioning PVST+ to the forwarding state. Range: 4 to 30 seconds Default: 15 seconds</td>
</tr>
</tbody>
</table>

**Defaults**

15 seconds

**Command Modes**

CONFIGURATION (conf-pvst)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `vlan bridge-priority`: Set the bridge-priority value
- `vlan hello-time`: Change the time interval between BPDUs
- `vlan max-age`: Change the time interval before PVST+ refreshes
- `show spanning-tree pvst`: Display the PVST+ configuration

---

**vlan hello-time**

Set the time interval between generation of PVST+ Bridge Protocol Data Units (BPDUs).

**Syntax**

```
vlan <vlan-id> hello-time seconds
```

To return to the default value, enter no vlan hello-time command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan-range</code></td>
<td>Enter the keyword <code>vlan</code> followed by the VLAN number(s). Range: 1 to 4094</td>
</tr>
<tr>
<td><code>hello-time</code></td>
<td>Enter the keyword <code>hello-time</code> followed by the time interval, in seconds, between transmission of BPDUs. Range: 1 to 10 seconds Default: 2 seconds</td>
</tr>
</tbody>
</table>

**Defaults**

2 seconds

**Command Modes**

CONFIGURATION (conf-pvst)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Per-VLAN Spanning Tree Plus (PVST+)

vlan max-age

Set the time interval for the PVST+ bridge to maintain configuration information before refreshing that information.

Syntax

```
vlan vlan-range max-age seconds
```

To return to the default, use the `no vlan max-age` command.

Parameters

- **vlan vlan-range**: Enter the keyword `vlan` followed by the VLAN number(s).
  Range: 1 to 4094
- **max-age seconds**: Enter the keyword `max-age` followed by the time interval, in seconds, that FTOS waits before refreshing configuration information.
  Range: 6 to 40 seconds
  Default: 20 seconds

Defaults

20 seconds

Command Modes

- CONFIGURATION (conf-pvst)

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- `vlan bridge-priority`: Set the bridge-priority value
- `vlan forward-delay`: Change the time interval before FTOS transitions to the forwarding state
- `vlan hello-time`: Change the time interval between BPDUs
- `show spanning-tree pvst`: Display the PVST+ configuration
Quality of Service (QoS)

Overview

The Dell Networking operating software (FTOS) commands for quality of service (QoS) include traffic conditioning and congestion control. This chapter contains the following sections:

• Global Configuration Commands
• Policy-Based QoS Commands

Global Configuration Commands

• qos-rate-adjust
• service-class dot1p-mapping

qos-rate-adjust

By default, for rate policing and rate shaping, FTOS does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC Destination Address to the CRC are used for forwarding and are included in these rate metering calculations. You can optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

Syntax

qos-rate-adjustment overhead-bytes

Parameters

overhead-bytes Include a specified number of bytes of packet overhead to include in rate policing, and rate shaping calculations.
Range: 1-31

Defaults

QoS rate adjustment is disabled by default, and no qos-rate-adjust is listed in the running-configuration.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
service-class dot1p-mapping

This command maps an 802.1p priority to an internal traffic class.

Syntax

service-class dot1p-mapping user-priority trafficclass

The user-priority value can range from 0-7 and traffic class can range from 0-6.

The no form of this command is not supported.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Per-Port QoS Commands

Per-port QoS (“port-based QoS”) allows users to defined QoS configuration on a per-physical-port basis. The commands include:

- dot1p-priority
- rate police
- rate shape
- service-class dynamic dot1p
- strict-priority unicast

dot1p-priority

Assign a value to the IEEE 802.1p bits on the traffic received by this interface.

Syntax

dot1p-priority priority-value

To delete the IEEE 802.1p configuration on the interface, use the no dot1p-priority command.

Parameters

<table>
<thead>
<tr>
<th>priority-value</th>
<th>Enter a value from 0 to 7.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1p</td>
<td>Queue Number</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

INTERFACE
The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.

When you set the priority for a Port Channel, the physical interfaces assigned to the Port Channel are configured with the same value. You cannot assign `dot1p-priority` command to individual interfaces in a Port Channel.

## rate police

Police the incoming traffic rate on the selected interface.

### Syntax

```
rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kbps</td>
<td>Enter this keyword to specify the rate police in Kilobits per second (Kbps). On MXL Switch make the following value a multiple of 64. The default granularity is Megabits per second (Mbps). Range: 0 to 40000000 (Kbps)</td>
</tr>
<tr>
<td>committed-rate</td>
<td>Enter a number as the bandwidth in Mbps. Range: 0 to 10000</td>
</tr>
<tr>
<td>burst-KB</td>
<td>(OPTIONAL) Enter a number as the burst size in KB. Range: 16 to 200000 Default: 50</td>
</tr>
<tr>
<td>peak peak-rate</td>
<td>(OPTIONAL) Enter the keyword <code>peak</code> followed by a number to specify the peak rate in Mbps. Range: 0 to 10000</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(OPTIONAL) Enter the keyword <code>vlan</code> followed by a VLAN ID to police traffic to those specific VLANs. Range: 1 to 4094</td>
</tr>
</tbody>
</table>

### Defaults

Granularity for `committed-rate` and `peak-rate` is Mbps unless the `kbps` option is used.

### Command Mode

`INTERFACE`

### Command History

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

### Usage Information

- **Note:** Per Port rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate police is supported on only tagged ports with Layer 2 switched traffic.

On **one** interface, you can configure the `rate police` command for a VLAN or you can configure the `rate police` command for an interface. For each physical interface, you can configure three `rate police` commands specifying different VLANs.

After configuring VLANs in the `rate police` command, if this error message appears:

```
%Error: Specified VLANs overlap with existing config.
```
rate shape

Shape the traffic output on the selected interface.

Syntax

rate shape [kbps] rate [burst-KB]

Parameters

- **kbps**
  - Enter this keyword to specify the rate shape in Kilobits per second (Kbps). On MXL Switch, make the following value a multiple of 64. The default granularity is Megabits per second (Mbps).
  - Range: 0-40000000 (Kbps)

- **rate**
  - Enter the outgoing rate in multiples of 10 Mbps.
  - Range: 10 to 10000

- **burst-KB**
  - (OPTIONAL) Enter a number as the burst size in KB.
  - Range: 0 to 10000
  - Default: 50

Defaults

Granularity for rate is Mbps unless the kbps option is used.

Command Modes

INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
</table>
| 8.3.16.1| MXL 10/40GbE Switch IO Module

Related Commands

- rate-shape Shapes the traffic output as part of the designated policy.

service-class dynamic dot1p

Honor all 802.1p markings on incoming switched traffic on an interface (from INTERFACE mode) or on all interfaces (from CONFIGURATION mode). A CONFIGURATION mode entry supersedes INTERFACE mode entries.

Syntax

service-class dynamic dot1p

To return to the default setting, use the no service-class dynamic dot1p command.

Defaults

All dot1p traffic is mapped to Queue 0 unless you enable the service-class dynamic dot1p command. Then the default mapping is as follows:

Table 39-1. Default dot1p to Queue Mapping

<table>
<thead>
<tr>
<th>dot1p</th>
<th>Queue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>
Enter this command to honor all incoming 802.1p markings, on incoming switched traffic, on the interface. By default, this facility is not enabled (that is, the 802.1p markings on incoming traffic are not honored).

This command can be applied on both physical interfaces and port channels. When you set the service-class dynamic for a port channel, the physical interfaces assigned to the port channel are automatically configured; you cannot assign the service-class dynamic command to individual interfaces in a port channel.

On the MXL Switch, all traffic is by default mapped to the same queue, Queue 0. If you honor dot1p on ingress, then you can create service classes based the queueing strategy using the command `service-class dynamic dot1p` from INTERFACE mode. You may apply this queuing strategy to all interfaces by entering this command from CONFIGURATION mode.

- All dot1p traffic is mapped to Queue 0 unless `service-class dynamic dot1p` is enabled on an interface or globally.
- Layer 2 or Layer 3 service policies supercede dot1p service classes.

### service-class bandwidth-percentage

Specify a minimum bandwidth for queues

**Syntax**

```plaintext
service-class bandwidth-percentage queue0 number queue1 number queue2 number queue3 number
```

**Parameters**

- `number`
  - Enter the bandwidth-weight. The value must be a power of 2.
  - Range: 1-100.

**Defaults**

- none

**Command Modes**

- INTERFACE
- CONFIGURATION

---

**Table 39-1. Default dot1p to Queue Mapping (continued)**

<table>
<thead>
<tr>
<th>dot1p</th>
<th>Queue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

**Command Modes**

- INTERFACE
- CONFIGURATION

**Version 8.3.16.1**

Introduced on MXL 10/40GbE Switch IO Module
 Guarantee a minimum bandwidth to different queues globally using the command `service-class bandwidth-percentage` from CONFIGURATION mode. The DCB ETS supersedes the global and policy based QoS bandwidth configurations.

When you enable ETS, the egress QoS features in the output QoS policy-map (such as `service-class bandwidth-percentage` and `bandwidth-percentage`), the default bandwidth allocation ratio for egress queues are superseded by ETS configurations. This is to provide compatibility with DCBX. Hence, it is recommended to have ETS disabled when you wish to apply these features exclusively. Once ETS is disabled on an interface, configured parameters will be applied.

### strict-priority unicast

Configure a unicast queue as a strict-priority (SP) queue.

**Syntax**

```
strict-priority unicast queue number
```

**Parameters**

- `unicast number`
  - Enter the keyword `unicast` followed by the queue number.
  - Range: 1 to 3

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

After a unicast queue is configured as strict-priority, that particular queue, on the entire chassis, is treated as strict-priority queue. Traffic for a strict priority is scheduled before any other queues are serviced. For example, if you send 100% line rate traffic over the SP queue, it will **starve** all other queues on the ports on which this traffic is flowing. To assign the strict priority schedule type to egress queues, use the `scheduler strict` command in QOS-POLICY-OUT mode. FTOS does not support bandwidth configuration on strict priority scheduler queues.

When you enable ETS, egress QoS features in the output QoS policy-map (such as `strict priority unicast <0-3>` and `scheduler strict`), default scheduler for egress queues are superseded by ETS configurations. This is to provide compatibility with DCBX. Hence, it is recommended to have the ETS disabled when you wish to apply these features exclusively. Once ETS disabled on an interface, configured parameters will be applied.
Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of four classes in the MXL Switch. FTOS enables you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANS, or loopbacks. The commands are:

- bandwidth-percentage
- class-map
- clear qos statistics
- description
- match ip access-group
- match ip dscp
- match ip precedence
- match mac access-group
- match mac dot1p
- match mac vlan
- policy-aggregate
- policy-map-input
- policy-map-output
- qos-policy-input
- qos-policy-output
- rate-police
- rate-shape
- service-policy input
- service-policy output
- service-queue
- set
- show qos class-map
- show qos policy-map
- show qos policy-map-input
- show qos policy-map-output
- show qos qos-policy-input
- show qos qos-policy-output
- show qos statistics
- show qos wred-profile
- test cam-usage
- trust
- wred
- wred-profile
bandwidth-percentage

Assign a percentage of weight to class/queue.

Syntax

bandwidth-percentage percentage

To remove the bandwidth percentage, use the no bandwidth-percentage command.

Parameters

percentage Enter the percentage assignment of weight to class/queue. Range: 1 to 100% (granularity 1%)

Defaults

none

Command Modes

CONFIGURATION (conf-qos-policy-out)

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The unit of bandwidth percentage is 1%. A bandwidth percentage of 0 is allowed and will disable the scheduling of that class. If the sum of the bandwidth percentages given to all four classes exceeds 100%, the bandwidth percentage will automatically scale down to 100%.

Related Commands

qos-policy-output Creates a QoS output policy.

class-map

Create/access a class map. Class maps differentiate traffic so that you can apply separate quality of service policies to each class.

Syntax

class-map {match-all | match-any} class-map-name [layer2]

Parameters

match-all Determines how packets are evaluated when multiple match criteria exist. Enter the keyword match-all to determine that the packets must meet all the match criteria in order to be considered a member of the class.

match-any Determines how packets are evaluated when multiple match criteria exist. Enter the keyword match-any to determine that the packets must meet at least one of the match criteria in order to be considered a member of the class.

class-map-name Enter a name of the class for the class map in a character format (32 character maximum).

layer2 Enter the keyword layer2 to specify a Layer 2 Class Map. Default: Layer 3

Defaults

Layer 3

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Packets arriving at the input interface are checked against the match criteria, configured using this command, to determine if the packet belongs to that class. This command accesses the CLASS-MAP mode, where the configuration commands include match ip and match mac options.

### clear qos statistics

Clears matched packets, matched bytes, and dropped packets.

**Syntax**

```
clear qos statistics interface-name.
```

**Parameters**

- `interface-name` Enter one of the following keywords:
  - For a 40-Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

**Defaults**

```
none
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When you issue this command, statistical information stored regarding QoS is cleared and reset to 0. These statistics can be accessed using the `show qos statistics` command in EXEC mode. When the traffic pattern matches the QoS classification criteria flows, the corresponding counters are incremented.

**Related Commands**

- `show qos statistics` Displays the qos statistics.
match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

**Syntax**

```
match ip access-group access-group-name [set-ip-dscp value]
```

To remove ACL match criteria from a class map, use the `no match ip access-group access-group-name [set-ip-dscp value]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group-name</td>
<td>Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class specified by class-map.</td>
</tr>
<tr>
<td>set-ip-dscp value</td>
<td>(OPTIONAL) Enter the keyword <code>set-ip-dscp</code> followed by the IP DSCP value. The matched traffic will be marked with the DSCP value. Range: 0 to 63</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CLASS-MAP CONFIGURATION (config-class-map)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must enter the class-map command in order to access this command. After the class map is identified, you can configure the match criteria. For class-map match-any, a maximum of five ACL match criteria are allowed. For class-map match-all, only one ACL match criteria is allowed.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map</td>
<td>Identifies the class map.</td>
</tr>
</tbody>
</table>

**description**

Add a description to the selected policy map or QoS policy.

**Syntax**

```
description {description}
```

To remove the description, use the `no description {description}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Enter a description to identify the policies (80 characters maximum).</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-map-input</td>
<td>Creates an input policy map.</td>
</tr>
<tr>
<td>policy-map-output</td>
<td>Creates an output policy map.</td>
</tr>
<tr>
<td>qos-policy-input</td>
<td>Creates an input QOS-policy on the router.</td>
</tr>
</tbody>
</table>
match ip dscp

Use a differentiated services code point (DSCP) value as a match criteria.

Syntax

match ip dscp dscp-list [set-ip-dscp value]

To remove a DSCP value as a match criteria, use the no match ip dscp dscp-list [[multicast] set-ip-dscp value] command.

Parameters

dscp-list

Enter the IP DSCP value(s) that is to be the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3).

Range: 0 to 63

set-ip-dscp value

(Optional) Enter the keyword set-ip-dscp followed by the IP DSCP value. The matched traffic will be marked with the DSCP value.

Range: 0 to 63

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

You must enter the class-map command in order to access this command. After the class map is identified, you can configure the match criteria.

The match ip dscp and match ip precedence commands are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DCSP values 0, 1, 2, 3, 4, 5, 6, 7, enter either the command match ip dscp 0,1,2,3,4,5,6,7 or match ip dscp 0-7.

Note: Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values need to match.

Related Commands

class-map

Identifies the class map.

match ip precedence

Use IP precedence values as a match criteria.

Syntax

match ip precedence ip-precedence-list [set-ip-dscp value]

To remove IP precedence as a match criteria, use the no match ip precedence ip-precedence-list [set-ip-dscp value] command.
**match ip precedence**

Configure a match criterion for a class map, based on the contents of the designated IP ACL.

**Syntax**

```
match ip precedence \{ip-precedence-list\}
```

**Parameters**

- **ip-precedence-list**
  
  Enter the IP precedence value(s) as the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3).
  
  Range: 0 to 7

**Command Modes**

CLASS-MAP CONFIGURATION (conf-class-map)

**Defaults**

- none

**Usage Information**

You must enter the `class-map` command in order to access this command. After the class map is identified, you can configure the match criteria.

The `match ip precedence` command and the `match ip dscp` command are mutually exclusive.

Up to eight precedence values can be matched in one match statement. For example, to indicate the IP precedence values 0 1 2 3 enter either the command `match ip precedence 0-3` or `match ip precedence 0,1,2,3`.

**Note:** Only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values need to match.

**Related Commands**

- **class-map**
  
  Identifies the class map.

**match mac access-group**

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

**Syntax**

```
match mac access-group \{mac-acl-name\}
```

**Parameters**

- **mac-acl-name**
  
  Enter a MAC ACL name. Its contents will be used as the match criteria in the class map.

**Defaults**

- none

**Command Modes**

CLASS-MAP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must enter the `class-map` command in order to access this command. After the class map is identified, you can configure the match criteria.
match mac dot1p

Configure a match criterion for a class map, based on a dot1p value.

**Syntax**

match mac dot1p {dot1p-list}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1p-list</td>
<td>Enter a dot1p value.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 7</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CLASS-MAP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must enter the class-map command in order to access this command. After the class map is identified, you can configure the match criteria.

**Related Commands**

class-map Identifies the class map.

match mac vlan

Configure a match criterion for a class map based on VLAN ID.

**Syntax**

match mac vlan number

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 4094</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CLASS-MAP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must first enter the class-map command in order to access this command. You can match against only one VLAN ID.

**Related Commands**

class-map Creates/accesses a class map.
policy-aggregate

Allow an aggregate method of configuring per-port QoS via policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

**Syntax**

```
policy-aggregate qos-policy-name
```

To remove a policy aggregate configuration, use the `no policy-aggregate qos-policy-name` command.

**Parameters**

- `qos-policy-name` Enter the name of the policy map in character format (32 characters maximum)

**Defaults**

- none

**Command Modes**

- CONFIGURATION (policy-map-input and policy-map-output)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Aggregate input/output QoS policy applies to all the port ingoing/outgoing traffic. Aggregate input/output QoS policy can co-exist with per queue input/output QoS policies.

1. If only aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) will apply. Any marking configurations in aggregate input QoS policy will be ignored.
2. If aggregate input QoS policy and per class input QoS policy co-exist, then aggregate input QoS policy will preempt per class input QoS policy on input traffic conditioning (rate-police). In other words, if rate police configuration exists in aggregate QoS policy, the configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.

**Related Commands**

- `policy-map-input` Creates an input policy map
- `policy-map-output` Creates an output policy map

policy-map-input

Create an input policy map.

**Syntax**

```
policy-map-input policy-map-name [layer2]
```

To remove an input policy map, use the `no policy-map-input policy-map-name [layer2]` command.

**Parameters**

- `policy-map-name` Enter the name for the policy map in character format (32 characters maximum).
- `layer2` (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. Default: Layer 3

**Defaults**

- Layer 3

**Command Modes**

- CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Input policy map is used to classify incoming traffic to different flows using class-map, QoS policy, or simply using incoming packets DSCP. This command enables policy-map-input configuration mode (conf-policy-map-in).

**Related Commands**

- **service-queue**
  Assigns a class map and QoS policy to different queues.

- **policy-aggregate**
  Allows an aggregate method of configuring per-port QoS via policy maps.

- **policy-map-input**
  Applies an input policy map to the selected interface.

---

**policy-map-output**

Create an output policy map.

**Syntax**

```
policy-map-output policy-map-name
```

To remove a policy map, use the no policy-map-output policy-map-name command.

**Parameters**

- **policy-map-name**
  Enter the name for the policy map in character format (16 characters maximum).

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Output policy map is used to assign traffic to different flows using QoS policy. This command enables the policy-map-output configuration mode (conf-policy-map-out).

**Related Commands**

- **service-queue**
  Assigns a class map and QoS policy to different queues.

- **policy-aggregate**
  Allows an aggregate method of configuring per-port QoS via policy maps.

- **service-policy output**
  Applies an output policy map to the selected interface.

---

**qos-policy-input**

Create a QoS input policy on the router.

**Syntax**

```
qos-policy-input qos-policy-name [layer2]
```

To remove an existing input QoS policy from the router, use the no qos-policy-input qos-policy-name [layer2] command.

**Parameters**

- **qos-policy-name**
  Enter your input QoS policy name in character format (32 character maximum).

- **layer2**
  (OPTIONAL) Enter the keyword layer2 to specify a Layer 2 Class Map. Default: Layer 3

**Defaults**

Layer 3
### Command Modes

<table>
<thead>
<tr>
<th>Command History</th>
<th>CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage Information</td>
<td>Use this command to specify the name of the input QoS policy. After input policy is specified, rate-police can be defined. This command enables the qos-policy-input configuration mode—(conf-qos-policy-in). When changing a service-queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the &quot;show qos statistics&quot; command is reset.</td>
</tr>
</tbody>
</table>

### Related Commands

- **rate-police**
  - Incoming traffic policing function

## qos-policy-output

Create a QoS output policy.

**Syntax**
```
qos-policy-output qos-policy-name
```

To remove an existing output QoS policy, use the no qos-policy-output qos-policy-name command.

**Parameters**

- **qos-policy-name**
  - Enter your output QoS policy name in character format (32 character maximum).

**Defaults**

none

**Command Modes**

<table>
<thead>
<tr>
<th>Command History</th>
<th>CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage Information</td>
<td>Use this command to specify the name of the output QoS policy. After output policy is specified, rate-limit, bandwidth-percentage, and WRED can be defined. This command enables the qos-policy-output configuration mode—(conf-qos-policy-out). When changing a service-queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the show qos statistics command is reset.</td>
</tr>
</tbody>
</table>

**Related Commands**

- **bandwidth-percentage**
  - Assigns weight to class/queue percentage.

- **wred**
  - Assigns yellow or green drop precedence.
**rate-police**

Specify the policing functionality on incoming traffic.

**Syntax**

```
rate-police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]]
```

**Parameters**

- **kbps**: Enter this keyword to specify the rate limit in Kilobits per second (Kbps). On MXL Switch, make the following value a multiple of 64. The default granularity is Megabits per second (Mbps).
  
  Range: 0-40000000 (Kbps)

- **committed-rate**: Enter the committed rate in Mbps.
  
  Range: 0 to 10000 Mbps

- **burst-KB**: (OPTIONAL) Enter the burst size in KB.
  
  Range: 16 to 200000 KB
  
  Default: 100 KB

- **peak peak-rate**: (OPTIONAL) Enter the keyword `peak` followed by the peak rate in Mbps.
  
  Range: 0 to 10000 Mbps
  
  Default: Same as designated for `committed-rate`

**Defaults**

Burst size is 100 KB. `peak-rate` is by default the same as `committed-rate`. Granularity for `committed-rate` and `peak-rate` is Mbps unless the `kbps` option is used.

**Command Modes**

QOS-POLICY-IN

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `rate-shape`: Shape traffic output as part of the designated policy.
- `qos-policy-input`: Creates a QoS output policy.

**rate-shape**

Shape traffic output as part of the designated policy.

**Syntax**

```
rate-shape [kbps] rate [burst-KB]
```

**Parameters**

- **kbps**: Enter this keyword to specify the rate limit in Kilobits per second (Kbps). On MXL Switch, make the following value a multiple of 64. The default granularity is Megabits per second (Mbps).
  
  Range: 0-40000000 (Kbps)

- **rate**: Enter the outgoing rate in multiples of 10 Mbps.
  
  Range: 10 to 10000

- **burst-KB**: (OPTIONAL) Enter a number as the burst size in KB.
  
  Range: 0 to 10000
  
  Default: 50

**Defaults**

Burst size is 50 KB. Granularity for `rate` is Mbps unless the `kbps` option is used.

**Command Modes**

QOS-POLICY-OUT
When rate-shape in QoS policy is applied both on queue level and aggregate mode, the queue-based shaping occurs first followed by the aggregate rate shaping.

Related Commands

- **rate shape**
  - Shapess the traffic output of the selected interface.

- **qos-policy-output**
  - Creates a QoS output policy.

### service-policy input

Apply an input policy map to the selected interface.

**Syntax**

```
service-policy input policy-map-name [layer2]
```

To remove the input policy map from the interface, use the `no service-policy input policy-map-name [layer2]` command.

**Parameters**

- **policy-map-name**
  - Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

- **layer2**
  - (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. Default: Layer 3

**Defaults**

Layer 3

**Command Modes**

INTERFACE

**Usage Information**

A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

**Note:** The `service-policy` commands are not allowed on a port channel. The `service-policy input policy-map-name` command and the `service-class dynamic dot1p` command are not allowed simultaneously on an interface.

**Related Commands**

- **policy-map-input**
  - Creates an input policy map.

### service-policy output

Apply an output policy map to the selected interface.

**Syntax**

```
service-policy output policy-map-name
```

To remove the output policy map from the interface, use the `no service-policy output policy-map-name` command.
A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

**Related Commands**

- **service-queue**

  Assign a class map and QoS policy to different queues.

  **Syntax**
  
  ```
  service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]
  ```

  To remove the queue assignment, use the no service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name] command.

  **Parameters**

  - **queue-id**
    - Enter the value used to identify a queue.
    - Range: 0-3 (four queues per interface; four queues are reserved for control traffic.)

  - **class-map class-map-name**
    - (OPTIONAL) Enter the keyword class-map followed by the class map name assigned to the queue in character format (16 character maximum).
    - **Note:** This option is available under policy-map-input only.

  - **qos-policy qos-policy-name**
    - (OPTIONAL) Enter the keyword qos-policy followed by the QoS policy name assigned to the queue in text format (16 characters maximum). This specifies the input QoS policy assigned to the queue under policy-map-input and output QoS policy under policy-map-output context.

  **Defaults**
  
  none

  **Command Modes**
  
  CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

  **Command History**
  
  - **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

  **Usage Information**
  
  There are four (4) queues per interface on the MXL Switch. This command assigns a class map or QoS policy to different queues.

  **Related Commands**

  - **class-map**
    - Identifies the class map.
  
  - **service-policy input**
    - Applies an input policy map to the selected interface.
  
  - **service-policy output**
    - Applies an output policy map to the selected interface.
set

Mark outgoing traffic with a Differentiated Service Code Point (DSCP) or dot1p value.

**Syntax**

set {ip-dscp value | mac-dot1p value}

**Parameters**

- **ip-dscp value**  
  (OPTIONAL) Enter the keyword `ip-dscp` followed by the IP DSCP value.
  Range: 0 to 63

- **mac-dot1p value**  
  Enter the keyword `mac-dot1p` followed by the dot1p value.
  Range: 0 to 7
  On the MXL Switch, allowed values are: 0, 2, 4, 6

**Defaults**

none

**Command Modes**

CONFIGURATION (conf-qos-policy-in)

**Command History**

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

After the IP DSCP bit is set, other QoS services can then operate on the bit settings.

---

show qos class-map

View the current class map information.

**Syntax**

show qos class-map [class-name]

**Parameters**

- **class-name**  
  (OPTIONAL) Enter the name of a configured class map.

**Defaults**

none

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

**Example**

Figure 39-1. show qos class-map Command Example

```
FTOS#show qos class-map
Class-map match-any CM
  Match ip access-group ACL
```

**Related Commands**

- class-map  
  Identifies the class map.
show qos policy-map

View the QoS policy map information.

**Syntax**
show qos policy-map {summary [interface] | detail [interface]}

**Parameters**

- **summary interface**
  - To view a policy map interface summary, enter the keyword `summary` and optionally one of the following keywords and slot/port or number information:
    - For a Forty Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` followed by the slot/port information.
    - For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

- **detail interface**
  - To view a policy map interface in detail, enter the keyword `detail` and optionally one of the following keywords and slot/port or number information:
    - For a FortyGigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` followed by the slot/port information.
    - For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**Example 1**

*Figure 39-2. show qos policy-map detail (IPv4) Command Example*

```
FTOS#show qos policy-map detail tengigabitethernet 0/0

Interface TenGigabitEthernet 4/1
Policy-map-input policy
Trust different
Queue#   Class-map-name   Qos-policy-name
   0                      q0
   1                  CM1  q1
   2                  CM2  q2
   3                  CM3  q3
FTOS#
```

**Example 2**

*Figure 39-3. show qos policy-map summary (IPv4) Command Example*

```
FTOS#show qos policy-map summary

Interface       policy-map-input   policy-map-output
TenGig 4/1       PM1               PMOut
TenGig 4/2       PM2               PMOut
FTOS#
```
show qos policy-map-input

View the input QoS policy map details.

Syntax

show qos policy-map-input [policy-map-name] [class class-map-name] [qos-policy-input qos-policy-name]

Parameters

- **policy-map-name**: Enter the policy map name.
- **class class-map-name**: Enter the keyword class followed by the class map name.
- **qos-policy-input qos-policy-name**: Enter the keyword qos-policy-input followed by the QoS policy name.

Defaults

- none

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example 1

Figure 39-4. show qos policy-map-input (IPv4) Command Example

```
FTOS#show qos policy-map-input
Policy-map-input PolicyMapInput
Aggregate Qos-policy-name AggPolicyIn
Queue#   Class-map-name          Qos-policy-name
0      ClassMap1               qosPolicyInput
FTOS#
```

show qos policy-map-output

View the output QoS policy map details.

Syntax

show qos policy-map-output [policy-map-name] [qos-policy-output qos-policy-name]

Parameters

- **policy-map-name**: Enter the policy map name.
- **qos-policy-output qos-policy-name**: Enter the keyword qos-policy-output followed by the QoS policy name.

Defaults

- none

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
show qos qos-policy-input
View the input QoS policy details.

Syntax
show qos qos-policy-input [qos-policy-name]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos-policy-name</td>
<td>Enter the QoS policy name.</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```sh
Figure 39-6. show qos qos-policy-input Command Example
FTOS# show qos qos-policy-input
Qos-policy-input QosInput
 Rate-police 100 50 peak 100 50
 Dscp 32
FTOS#
```

show qos qos-policy-output
View the output QoS policy details.

Syntax
show qos qos-policy-output [qos-policy-name]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos-policy-name</td>
<td>Enter the QoS policy name.</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```sh
Figure 39-6. show qos qos-policy-input Command Example
FTOS# show qos policy-map-output
Policy-map-output PolicyMapOutput
 Aggregate Qos-policy-name AggPolicyOut
 Queue# Qos-policy-name
 0 qosPolicyOutput
FTOS#
```
**show qos statistics**

View QoS statistics.

**Syntax**

```
show qos statistics {wred-profile [interface] | [interface]}
```

**Parameters**

- `wred-profile interface` Enter the keyword `wred-profile` and optionally one of the following keywords and slot/port or number information:
  - For a Forty Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` followed by the slot/port information.
  - For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

- `interface` Enter one of the following keywords and slot/port or number information:
  - For a Forty Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` followed by the slot/port information.
  - For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

**Defaults**

`none`

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example 1**

```
FTOS#show qos statistics
Interface Te 0/20
Queue#  Matched Pkts
 0    0
 1    0
 2    0
 3    0
FTOS#
```
Table 39-2.  show qos statistics Command Description (ED and EE Series)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue #</td>
<td>Queue Number</td>
</tr>
<tr>
<td>Matched Pkts</td>
<td>The number of packets that matched the class-map criteria.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When trust is configured, matched packet counters are not incremented in this field.</td>
</tr>
</tbody>
</table>

Example 2

Figure 39-9.  show qos statistics wred-profile Command Example

```
FTOS#show qos statistics wred-profile
Interface Te 0/20
Drop-statistic Dropped Pkts
Green           0
Yellow          0
Out of Profile  0
FTOS#
```

Table 39-3.  show qos statistics wred-profile Command Description (ED, EE, and EF Series)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue #</td>
<td>Queue Number</td>
</tr>
<tr>
<td>Drop-statistic</td>
<td>Drop statistics for green, yellow and out-of-profile packets</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The number of packets dropped for green, yellow and out-of-profile packets</td>
</tr>
</tbody>
</table>

Related Commands

- `clear qos statistics` Clears counters as shown in show qos statistics

show qos wred-profile

View the WRED profile details.

Syntax

```
show qos wred-profile wred-profile-name
```

Parameters

- `wred-profile-name` Enter the WRED profile name to view the profile details.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
test cam-usage

Check the Input Policy Map configuration for the CAM usage.

Syntax

test cam-usage service-policy input policy-map stack-unit {[number] | [all]}

Parameters

| policy-map | Enter the policy map name. |
| stack-unit number | (OPTIONAL) Enter the keyword stack-unit followed by the stack-unit number. |
| stack-unit all | (OPTIONAL) Enter the keywords stack-unit all to indicate all stack units. |

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Example Figure 39-11. test cam-usage service-policy input policy-map stack-unit all Command Example

FTOS# test cam-usage service-policy input pmap_l2 stack-unit all
For a L2 Input Policy Map pmap_l2, the output must be as follows,

<table>
<thead>
<tr>
<th>Stack-unit Status</th>
<th>Portpipe</th>
<th>CAM Partition</th>
<th>Available CAM</th>
<th>Estimated CAM</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>L2ACL</td>
<td>500</td>
<td>200</td>
<td>Allowed (2)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L2ACL</td>
<td>100</td>
<td>200</td>
<td>Exception</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>L2ACL</td>
<td>1000</td>
<td>200</td>
<td>Allowed (5)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>L2ACL</td>
<td>0</td>
<td>200</td>
<td>Exception</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>L2ACL</td>
<td>400</td>
<td>200</td>
<td>Allowed (2)</td>
</tr>
</tbody>
</table>

Note: In a Layer 2 Policy Map, IPv4 rules are not allowed and hence the output contains only L2ACL CAM partition entries.
This feature allows you to determine if the CAM has enough space available before applying the configuration on an interface.

An input policy map with both Trust and Class-map configuration, the Class-map rules are ignored and only the Trust rule is programmed in the CAM. In such an instance, the Estimated CAM output column will contain the size of the CAM space required for the Trust rule and **not** the Class-map rule.

### Usage Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit</td>
<td>Indicates the stack-unit number.</td>
</tr>
<tr>
<td>Portpipe</td>
<td>Indicates the portpipe number.</td>
</tr>
<tr>
<td>CAM Partition</td>
<td>The CAM space where the rules are added.</td>
</tr>
<tr>
<td>Available CAM</td>
<td>Indicates the free CAM space, in the partition, for the classification rules.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, can not be used as a policy map for the classification rules.</td>
</tr>
<tr>
<td>Estimated CAM per Port</td>
<td>Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.</td>
</tr>
<tr>
<td>Status (Allowed ports)</td>
<td>Indicates if the input policy map configuration on an interface belonging to a stack-unit/port-pipe is successful—Allowed (n)—or not successful—Exception. The allowed number (n) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.</td>
</tr>
</tbody>
</table>

### trust

Specify dynamic classification (DSCP) or dot1p to trust.

**Syntax**

```
trust {diffserv [fallback] | dot1p [fallback]}
```

**Parameters**

- **diffserv**
  - Enter the keyword **diffserv** to specify trust of DSCP markings.
- **dot1p**
  - Enter the keyword **dot1p** to specify trust dot1p configuration.
- **fallback**
  - Enter this keyword to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.

**Defaults**

```
one
```

**Command Modes**

```
CONFIGURATION (conf-policy-map-in)
```

**Command History**

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```
When trust is configured, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The default mapping table is detailed in the following table.

### Table 39-5. Standard Default DSCP Mapping Table

<table>
<thead>
<tr>
<th>DSCP/CP hex range (XXX)</th>
<th>DSCP Definition</th>
<th>Traditional IP Precedence</th>
<th>MXL Switch Internal Queue ID</th>
<th>DSCP/CP decimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>111XXX</td>
<td>Network Control</td>
<td>3</td>
<td></td>
<td>48–63</td>
</tr>
<tr>
<td>110XXX</td>
<td>Internetwork Control</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>101XXX</td>
<td>EF (Expedited Forwarding)</td>
<td>CRITIC/ECP</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>100XXX</td>
<td>AF4 (Assured Forwarding)</td>
<td>Flash Override</td>
<td>2</td>
<td>32–47</td>
</tr>
<tr>
<td>011XXX</td>
<td>AF3</td>
<td>Flash</td>
<td>1</td>
<td>16–31</td>
</tr>
<tr>
<td>010XXX</td>
<td>AF2</td>
<td>Immediate</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>001XXX</td>
<td>AF1</td>
<td>Priority</td>
<td>0</td>
<td>0–15</td>
</tr>
<tr>
<td>000XXX</td>
<td>BE (Best Effort)</td>
<td>Best Effort</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**wred**

Designate the WRED profile to yellow or green traffic.

**Syntax**

```
wred [((yellow | green) profile-name] ecn]
```

To remove the WRED drop precedence, use the `no wred {yellow | green} [profile-name]` command.

**Parameters**

- `yellow | green` Enter the keyword `yellow` for yellow traffic. DSCP value of `xxx110` and `xxx100` maps to yellow. Enter the keyword `green` for green traffic. DSCP value of `xxx010` maps to green.
- `profile-name` Enter your WRED profile name in character format (16 character maximum). Or use one of the 5 pre-defined WRED profile names. Pre-defined Profiles:
  - wred_drop, wred_teng_y, wred_teng_red,
- `ecn` When `wred ecn <cr>` command is configured, instead of dropping the packets exponentially, Explicit Congestion Notification (ECN) marking is made on the packets.

**Defaults**

`none`

**Command Modes**

`CONFIGURATION (conf-qos-policy-out)`

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Use this command to assign drop precedence to green or yellow traffic. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>wred-profile</strong></td>
<td>Creates a WRED profile and name that profile</td>
</tr>
<tr>
<td><strong>trust</strong></td>
<td>Defines the dynamic classification to trust DSCP</td>
</tr>
</tbody>
</table>

**wred-profile**

Create a WRED profile and name that profile.

**Syntax**

```
wred-profile wred-profile-name
```

To remove an existing WRED profile, use the `no wred-profile` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wred-profile-name</code></td>
<td>Enter your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names. You can configure up to 26 WRED profiles plus the 5 pre-defined profiles, for a total of 31 WRED profiles. Pre-defined Profiles: wred_drop, wred_ge_y, wred_ge_g, wred_teng_y, wred_teng_g</td>
</tr>
</tbody>
</table>

**Defaults**

The five pre-defined WRED profiles. When a new profile is configured, the minimum and maximum threshold defaults to predefined wred_ge_g values

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Use the default pre-defined profiles or configure your own profile. You can not delete the pre-defined profiles or their default values. This command enables the WRED configuration mode—(conf-wred).
Routing Information Protocol (RIP)

Overview

Routing information protocol (RIP) is a distance vector routing protocol. The Dell Networking operating software (FTOS) supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2).

The FTOS implementation of RIP is based on IETF RFCs 2453 and RFC 1058. For more information about configuring RIP, refer to the FTOS Configuration Guide.

Commands

The following commands allow you to configure RIP:

- auto-summary
- clear ip rip
- debug ip rip
- default-information originate
- default-metric
- description
- distance
- distribute-list in
- distribute-list out
- ip poison-reverse
- ip rip receive version
- ip rip send version
- ip split-horizon
- maximum-paths
- neighbor
- network
- offset-list
- output-delay
- passive-interface
- redistribute
- redistribute ospf
- router rip
- show config
- show ip rip database
auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

Syntax

auto-summary

To send sub-prefix routing information, use the no auto-summary command.

Default

Enabled.

Command Modes

ROUTER RIP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

clear ip rip

Update all the RIP routes in the FTOS routing table.

Syntax

clear ip rip

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

This command triggers updates of the main RIP routing tables.

debug ip rip

Examine RIP routing information for troubleshooting.

Syntax


To turn off debugging output, use the no debug ip rip command.
default-information originate

Generate a default route for the RIP traffic.

Syntax
default-information originate [always] [metric metric-value] [route-map map-name]

To return to the default values, use the no default-information originate command.

Parameters

- **always** (OPTIONAL) Enter the keyword always to enable the switch software to always advertise the default route.

- **metric metric-value** (OPTIONAL) Enter the keyword metric followed by a number as the metric value. Range: 1 to 16 Default: 1

- **route-map map-name** (OPTIONAL) Enter the keyword route-map followed by the name of a configured route-map.

Defaults

Disabled

metric: 1

Command Modes

ROUTER RIP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The default route must be present in the switch routing table for the default-information originate command to take effect.
**default-metric**

Change the default metric for routes. Use this command with the redistribute command to ensure that all redistributed routes use the same metric value.

**Syntax**

default-metric number

To return the default metric to the original values, use the no default-metric command.

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Specify a number. Range: 1 to 16. The default is 1.</td>
</tr>
</tbody>
</table>

**Default**

1

**Command Modes**

ROUTER RIP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

This command ensures that route information being redistributed is converted to the same metric value.

**Related Commands**

- redistribute - Allows you to redistribute routes learned by other methods.

**description**

Enter a description of the RIP routing protocol

**Syntax**

description \{description\}

To remove the description, use the no description \{description\} command.

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Enter a description to identify the RIP protocol (80 characters maximum).</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

ROUTER RIP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- router rip - Enters ROUTER mode on the switch.

**distance**

Assign a weight (for prioritization) to all routes in the RIP routing table or to a specific route. Lower weights (“administrative distance”) are preferred.

**Syntax**

distance weight [ip-address mask [prefix-name]]

To return to the default values, use the no distance weight [ip-address mask] command.
Routing Information Protocol (RIP) | 787

**Parameters**

**weight**

Enter a number from 1 to 255 for the weight (for prioritization).
The default is 120.

**ip-address**

(Optional) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric.

**mask**

If you enter an IP address, you must also enter a mask for that IP address, in either dotted decimal format or /prefix format (/x)

**prefix-name**

(Optional) Enter a configured prefix list name.

**Defaults**

weight = 120

**Command Modes**

ROUTER RIP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

distribute-list in

Configure a filter for incoming routing updates.

**Syntax**

distribute-list prefix-list-name in [interface]

To delete the filter, use the no distribute-list prefix-list-name in command.

**Parameters**

**prefix-list-name**

Enter the name of a configured prefix list.

**interface**

(Optional) Identifies the interface type slot/port as one of the following:

- For a Port Channel interface, enter the keyword port-channel followed by a number:
  Range: 1-128
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.
- For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

ROUTER RIP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

ip prefix-list Enters PREFIX-LIST mode and configures a prefix list.

**distribute-list out**

Configure a filter for outgoing routing updates.
Syntax

distribute-list prefix-list-name out [interface | bgp | connected | ospf | static]

To delete the filter, use the no distribute-list prefix-list-name out command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-list-name</td>
<td>Enter the name of a configured prefix list.</td>
</tr>
<tr>
<td>interface</td>
<td>(OPTIONAL) Identifies the interface type slot/port as one of the following:</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 128</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.</td>
</tr>
<tr>
<td>connected</td>
<td>(OPTIONAL) Enter the keyword connected to filter only directly connected routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>(OPTIONAL) Enter the keyword ospf to filter all OSPF routes.</td>
</tr>
<tr>
<td>static</td>
<td>(OPTIONAL) Enter the keyword static to filter manually configured routes.</td>
</tr>
</tbody>
</table>

Defaults
Not configured.

Command Modes
ROUTER RIP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

ip prefix-list Enters PREFIX-LIST mode and configures a prefix list.

ip poison-reverse

Set the prefix of the RIP routing updates to the RIP infinity value.

Syntax

ip poison-reverse

To disable poison reverse, use the no ip poison-reverse command.

Defaults
Disabled.

Command Modes
INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

ip split-horizon Sets the RIP routing updates to exclude routing prefixes.

ip rip receive version

Set the interface to receive specific versions of RIP. The RIP version you set on the interface overrides the version command in ROUTER RIP mode.
Syntax

ip rip receive version [1] [2]

To return to the default, use the no ip rip receive version command.

Parameters

1 (OPTIONAL) Enter the number 1 for RIP version 1.
2 (OPTIONAL) Enter the number 2 for RIP version 2.

Defaults

RIPv1 and RIPv2

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

If you want the interface to receive both versions of RIP, use ip rip receive version 1 2.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rip send version</td>
<td>Sets the RIP version to be used for sending RIP traffic on an interface.</td>
</tr>
<tr>
<td>version</td>
<td>Sets the RIP version to be used for the switch software.</td>
</tr>
</tbody>
</table>

**ip rip send version**

Set the interface to send a specific version of RIP. The version you set on the interface overrides the version command in ROUTER RIP mode.

Syntax

ip rip send version [1] [2]

To return to the default value, use the no ip rip send version command.

Parameters

1 (OPTIONAL) Enter the number 1 for RIP version 1.
2 (OPTIONAL) Enter the number 2 for RIP version 2.

The default is RIPv1.

Defaults

RIPv1

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

To enable the interface to send both version of RIP packets, use ip rip send version 1 2.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip rip receive version</td>
<td>Sets the RIP version for the interface to receive traffic.</td>
</tr>
<tr>
<td>version</td>
<td>Sets the RIP version to be used for the switch software.</td>
</tr>
</tbody>
</table>
ip split-horizon

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

Syntax

ip split-horizon

To disable split-horizon, enter no ip split-horizon.

Defaults

Enabled

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

ip poison-reverse Sets the prefix for RIP routing updates.

maximum-paths

Set RIP to forward packets over multiple paths.

Syntax

maximum-paths number

To return to the default values, use the no maximum-paths command.

Parameters

number Enter the number of paths.

Range: 1 to 16.

The default is 4 paths.

Defaults

4

Command Modes

ROUTER RIP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

RIP supports a maximum of 16 ECMP paths.

neighbor

Define a neighbor router with which to exchange RIP information.

Syntax

neighbor ip-address

To delete a neighbor setting, use the no neighbor ip-address command.

Parameters

ip-address Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults

Not configured.
### Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>ROUTER RIP</th>
</tr>
</thead>
</table>

### Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Version 8.3.16.1</th>
<th>Introduced on MXL 10/40GbE Switch IO Module</th>
</tr>
</thead>
</table>

### Usage Information

When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible.

Use the `passive-interface` command in conjunction with the `neighbor` command to ensure that only specific interfaces are receiving and sending data.

### Related Commands

- `passive-interface` : Sets the interface to only listen to RIP broadcasts.

---

### network

Enable RIP for a specified network. Use this command to enable RIP on all networks connected to the switch.

**Syntax**

```
network ip-address
```

To disable RIP for a network, use the `no network ip-address` command.

**Parameter**

- `ip-address` : Specify an IP network address in dotted decimal format. You cannot specify a subnet.

**Defaults**

No RIP network is configured.

**Command Modes**

ROUTER RIP

**Command History**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Version 8.3.16.1</th>
<th>Introduced on MXL 10/40GbE Switch IO Module</th>
</tr>
</thead>
</table>

**Usage Information**

You can enable an unlimited number of RIP networks.

RIP operates over interfaces configured with any address specified by the `network` command.

---

### offset-list

Specify a number to add to the incoming or outgoing route metrics learned via RIP.

**Syntax**

```
offset-list prefix-list-name {in | out} offset [interface]
```

To delete an offset list, use the `no offset-list prefix-list-name {in | out} offset [interface]` command.

**Parameters**

- `prefix-list-name` : Enter the name of an established Prefix list to determine which incoming routes will be modified.
### Commands

**offset**
- **Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified.**
- **If you set an offset value to zero (0), no action is taken.**

**interface**
- **(OPTIONAL) Enter the following keywords and slot/port or number information:**
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **Range:** 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**
Not configured.

**Command Modes**
ROUTER RIP

**Command History**
- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**
When the offset metric is applied to an interface, that value takes precedence over an offset value that is not extended to an interface.

**Related Commands**
- `ip prefix-list` Enters PREFIX-LIST mode and configures a prefix list.

---

**output-delay**
Set the interpacket delay of successive packets to the same neighbor.

**Syntax**
```
output-delay delay
```

**Parameters**
- **delay**
  - Specify a number of milliseconds as the delay interval.
  - **Range:** 8 to 50

**Default**
Not configured.

**Command Modes**
ROUTER RIP

**Command History**
- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**
This command is intended for low-speed interfaces.

---

**passive-interface**
Suppress routing updates on a specified interface.

**Syntax**
```
passive-interface interface
```
To delete a passive interface, use the `no passive-interface interface` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Enter the following information:</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Not configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>ROUTER RIP</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Information**

Although the passive interface neither sends nor receives routing updates, the network on that interface is still included in RIP updates sent via other interfaces.

**Related Commands**

- `neighbor` Enables RIP for a specified network.
- `network` Defines a neighbor.

---

**redistribute**

Redistribute information from other routing instances.

**Syntax**

`redistribute {connected | static}

To disable redistribution, use the `no redistribute {connected | static}` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>Enter the keyword <code>connected</code> to specify that information from active routes on interfaces is redistributed.</td>
</tr>
<tr>
<td>static</td>
<td>Enter the keyword <code>static</code> to specify that information from static routes is redistributed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Not configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>ROUTER RIP</td>
</tr>
</tbody>
</table>

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

**Related Commands**

- `default-information originate` Generates a default route for RIP traffic.
redistribute ospf

Redistribute routing information from an OSPF process.

Syntax

redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name]

To disable redistribution, use the no redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name] command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter a number that corresponds to the OSPF process ID to be redistributed. Range: 1 to 65535.</td>
</tr>
<tr>
<td>match external {1</td>
<td>2}</td>
</tr>
<tr>
<td>match internal</td>
<td>(OPTIONAL) Enter the keywords match internal to indicate that internal routes should be redistributed.</td>
</tr>
<tr>
<td>metric metric-value</td>
<td>(OPTIONAL) Enter the keyword metric followed by a number as the metric value. Range: 0 to 16</td>
</tr>
<tr>
<td>route-map map-name</td>
<td>(OPTIONAL) Enter the keyword route-map followed by the name of a configured route map.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

router rip

Enter ROUTER RIP mode to configure and enable RIP.

Syntax

router rip

To disable RIP, use the no router rip command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

To enable RIP, you must assign a network address using the network command.

Example

Figure 40-1. router rip Command Example

```
FTOS(conf)#router rip
FTOS(conf-router_rip)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>Enable RIP.</td>
</tr>
<tr>
<td>exit</td>
<td>Return to the CONFIGURATION mode.</td>
</tr>
</tbody>
</table>
**show config**

Display the changes you made to the RIP configuration. Default values are not shown.

**Syntax**

```
show config
```

**Command Modes**

ROUTER RIP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
Figure 40-2. show config Command Example in ROUTER RIP Mode

FTOS(conf-router_rip)#show config
!
router rip
    network 172.31.0.0
    passive-interface TenGigabitEthernet 0/1

FTOS(conf-router_rip)#
```

---

**show ip rip database**

Display the routes learned by RIP. If the switch learned no RIP routes, no output is generated.

**Syntax**

```
show ip rip database [ip-address mask]
```

**Parameters**

- `ip-address`  
  (OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only.
  If you enter an IP address, you must also enter a mask for that IP address.

- `mask`  
  (OPTIONAL) Specify a mask, in /network format, for the IP address.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
Figure 40-3. show ip rip database Command Example (Partial)

FTOS#show ip rip database
Total number of routes in RIP database: 1624
  204.250.54.0/24
    (50/1) via 192.14.1.3, 00:00:12, TenGigabitEthernet 9/15
  204.250.54.0/24  auto-summary
  203.250.49.0/24
    (50/2) via 1.1.18.2, 00:00:14, Vlan 18
    (50/2) via 1.1.130.2, 00:00:12, Port-channel 30
  203.250.49.0/24  auto-summary
  210.250.40.0/24
    (50/2) via 1.1.1.18.2, 00:00:14, Vlan 18
    (50/2) via 1.1.130.2, 00:00:12, Port-channel 30
  210.250.40.0/24  auto-summary
  207.250.53.0/24
    (50/2) via 1.1.120.2, 00:00:55, Port-channel 20
  207.250.53.0/24  auto-summary
  208.250.42.0/24
    (50/2) via 1.1.120.2, 00:00:55, Port-channel 20
    (50/2) via 1.1.130.2, 00:00:12, Port-channel 30
  208.250.42.0/24  auto-summary
```

---
Table 40-1.  show ip rip database Command Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of routes in RIP database</td>
<td>Displays the number of RIP routes stored in the RIP database.</td>
</tr>
<tr>
<td>100.10.10.0/24 directly connected</td>
<td>Lists the route(s) directly connected.</td>
</tr>
<tr>
<td>150.100.0.0 redistributed</td>
<td>Lists the routes learned through redistribution.</td>
</tr>
<tr>
<td>209.9.16.0/24...</td>
<td>Lists the routes and the sources advertising those routes.</td>
</tr>
</tbody>
</table>

**show running-config rip**

Use this feature to display the current RIP configuration.

**Syntax**

```plaintext
show running-config rip
```

**Defaults**

none

**Command Modes**

EXEC Privilege

**Example**

```
Figure 40-4.  show running-config rip Command Example

show running-config rip
!
router rip
distribute-list Test1 in
distribute-list Test21 out
network 10.0.0.0
passive-interface TenGigabitEthernet 2/0
neighbor 20.20.20.20
redistribute ospf 999
version 2
```

**Command History**

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

**timers basic**

Manipulate the RIP timers for routing updates, invalid, holddown times and flush time.

**Syntax**

```plaintext
timers basic update invalid holddown flush
```

To return to the default settings, use the no timers basic command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>update</strong></td>
<td>Enter the number of seconds to specify the rate at which RIP routing updates are sent.</td>
</tr>
<tr>
<td></td>
<td>Range: zero (0) to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>Default: 30 seconds.</td>
</tr>
<tr>
<td><strong>invalid</strong></td>
<td>Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The <strong>invalid</strong> value should be at least three times the <strong>update</strong> timer value.</td>
</tr>
<tr>
<td></td>
<td>Range: zero (0) to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>Default: 180 seconds.</td>
</tr>
</tbody>
</table>
Defaults

•  update = 30 seconds
•  invalid = 180 seconds
•  holddown = 180 seconds
•  flush = 240 seconds.

Command Modes

ROUTER RIP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

If you change the timers on one router, the timers on all routers in the RIP domain must also be synchronized.

version

Specify either RIP version 1 or RIP version 2.

Syntax

version {1 | 2}

To return to the default version setting, use the no version command.

Parameters

1 Enter the keyword 1 to specify RIP version 1.

2 Enter the keyword 2 to specify RIP version 2.

Default

The FTOS sends RIPv1 and receives RIPv1 and RIPv2.

Command Modes

ROUTER RIP

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

ip rip receive version Sets the RIP version to be received on the interface.

ip rip send version Sets the RIP version to be sent out the interface.
Remote Monitoring (RMON)

Overview

Dell Networking operating software (FTOS) remote monitoring (RMON) is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection. FTOS RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, and RFC-3434:

- Ethernet Statistics Table RFC-2819
- Ethernet Statistics High-Capacity Table RFC-3273, 64bits
- Ethernet History Control Table RFC-2819
- Ethernet History Table RFC-2819
- Ethernet History High-Capacity Table RFC-3273, 64bits
- Alarm Table RFC-2819
- High-Capacity Alarm Table (64bits) RFC-3434, 64bits
- Event Table RFC-2819
- Log Table RFC-2819

FTOS RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization

Note: Only the simple network management protocol (SNMP) GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

Commands

The FTOS RMON commands are:

- rmon alarm
- rmon collection history
- rmon collection statistics
- rmon event
- rmon hc-alarm
- show rmon
- show rmon alarms
- show rmon events
- show rmon hc-alarm
rmon alarm

Set an alarm on any MIB object.

Syntax

```
rmon alarm number variable interval {delta | absolute} rising-threshold value event-number
falling-threshold value event-number [owner string]
```

To disable the alarm, use the no rmon alarm number command.

Parameters

- **number**: Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.
- **variable**: The MIB object to monitor. The variable must be in the SNMP OID format, for example, 1.3.6.1.2.1.1.3. The object type must be a 32 bit integer.
- **interval**: Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds
- **delta**: Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.
- **absolute**: Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.
- **rising-threshold value event-number**: Enter the keyword `rising-threshold` followed by the value (32bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
- **falling-threshold value event-number**: Enter the keyword `falling-threshold` followed by the value (32bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
- **owner string**: (Optional) Enter the keyword `owner` followed by the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Default

- **owner**: 

Command Modes

- **CONFIGURATION**

Command History

- **Version 8.3.16.1**: Introduced on MXL 10/40GbE Switch IO Module
**rmon collection history**

Enable the RMON MIB history group of statistics collection on an interface.

**Syntax**
```
rmon collection history {controlEntry integer} [owner name] [buckets number] [interval seconds]
```

To remove a specified RMON history group of statistics collection, use the `no rmon collection history {controlEntry integer}` command.

**Parameters**

- **controlEntry integer**
  - Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON History Table.

- **owner name**
  - (OPTIONAL) Enter the keyword `owner` followed by the owner name to record the owner of the RMON group of statistics.

- **buckets number**
  - (OPTIONAL) Enter the keyword `buckets` followed the number of buckets for the RMON collection history group of statistics. Bucket Range: 1 to 1000
  Default: 50

- **interval seconds**
  - (OPTIONAL) Enter the keyword `interval` followed the number of seconds in each polling cycle.
  Range: 5 to 3600 seconds
  Default: 1800 seconds

**Defaults**
No default behavior

**Command Modes**
CONFIGURATION INTERFACE (config-if)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

---

**rmon collection statistics**

Enable RMON MIB statistics collection on an interface.

**Syntax**
```
rmon collection statistics {controlEntry integer} [owner name]
```

To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics {controlEntry integer}` command.

**Parameters**

- **controlEntry integer**
  - Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON Statistic Table.

- **owner name**
  - (OPTIONAL) Enter the keyword `owner` followed by the owner name to record the owner of the RMON group of statistics.

**Defaults**
none

**Command Modes**
CONFIGURATION INTERFACE (config-if)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### rmon event

Add an event in the RMON event table.

**Syntax**
```
rmon event number [log] [trap community] [description string] [owner name]
```

To disable RMON on an interface, use the `no rmon event number [log] [trap community] [description string]` command.

**Parameters**
- **number**: Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON Event Table.
- **log**: (OPTIONAL) Enter the keyword `log` to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. Default: No log
- **trap community**: (OPTIONAL) Enter the keyword `trap` followed by an SNMP community string to configure the eventType setting in the RMON MIB. This sets either snmp-trap or log-and-trap. Default: public
- **description string**: (OPTIONAL) Enter the keyword `description` followed by a string describing the event.
- **owner name**: (OPTIONAL) Enter the keyword `owner` followed by the name of the owner of this event.

**Defaults**
as described above

**Command Modes**
CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

### rmon hc-alarm

Set an alarm on any MIB object.

**Syntax**
```
rmon hc-alarm number variable interval {delta | absolute} rising-threshold value event-number falling-threshold value event-number [owner string]
```

To disable the alarm, use the `no rmon hc-alarm number` command.

**Parameters**
- **number**: Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.
- **variable**: The MIB object to monitor. The variable must be in the SNMP OID format, for example, `1.3.6.1.2.1.1.3` The object type must be a 64 bit integer.
- **interval**: Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds
- **delta**: Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.
- **absolute**: Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.
show rmon

Display the RMON running status including the memory usage.

Syntax

show rmon

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 41-1. show rmon Command Example

FTOS# show rmon
RMON status
    total memory used 218840 bytes.
    ether statistics table: 8 entries, 4608 bytes
    ether history table: 8 entries, 6000 bytes
    alarm table: 390 entries, 102960 bytes
    alarm table: 390 entries, 102960 bytes
    high-capacity alarm table: 5 entries, 1680 bytes
    event table: 500 entries, 206000 bytes
    log table: 2 entries, 552 bytes

FTOS#

show rmon alarms

Display the contents of the RMON alarm table.

Syntax

show rmon alarms [index] [brief]
### Parameters

<table>
<thead>
<tr>
<th>index</th>
<th>(OPTIONAL) Enter the table index number to display just that entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to display the RMON Alarm Table in an easy-to-read format.</td>
</tr>
</tbody>
</table>

### Defaults

none

### Command Modes

EXEC

### Command History

**Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

### Example 1

**Figure 41-2. show rmon alarms index Command Example**

```plaintext
FTOS#show rmon alarm 1
RMON alarm entry 1
  sample Interval: 5
  object: 1.3.6.1.2.1.1.3
  sample type: absolute value.
  value: 255161
  alarm type: rising or falling alarm.
  rising threshold: 1, RMON event index: 1
  falling threshold: 501, RMON event index: 501
  alarm owner: 1
  alarm status: OK
FTOS#
```

**Example 2**

**Figure 41-3. show rmon alarms brief Command Example**

```plaintext
FTOS#show rmon alarm br
index SNMP OID
---------------------------------------------------------------------------------
1 | 1.3.6.1.2.1.1.3
2 | 1.3.6.1.2.1.1.3
3 | 1.3.6.1.2.1.1.3
4 | 1.3.6.1.2.1.1.3
5 | 1.3.6.1.2.1.1.3
6 | 1.3.6.1.2.1.1.3
7 | 1.3.6.1.2.1.1.3
8 | 1.3.6.1.2.1.1.3
9 | 1.3.6.1.2.1.1.3
10| 1.3.6.1.2.1.1.3
11| 1.3.6.1.2.1.1.3
12| 1.3.6.1.2.1.1.3
13| 1.3.6.1.2.1.1.3
14| 1.3.6.1.2.1.1.3
15| 1.3.6.1.2.1.1.3
16| 1.3.6.1.2.1.1.3
17| 1.3.6.1.2.1.1.3
18| 1.3.6.1.2.1.1.3
19| 1.3.6.1.2.1.1.3
20| 1.3.6.1.2.1.1.3
21| 1.3.6.1.2.1.1.3
22| 1.3.6.1.2.1.1.3
FTOS#
```
show rmon events
Display the contents of RMON event table.

Syntax  
show rmon events [index] [brief]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>(OPTIONAL) Enter the table index number to display just that entry.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to display the RMON Event Table in an easy-to-read format.</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Example 1

Figure 41-4. show rmon event index Command Example

FTOS#show rmon event 1
RMON event entry 1
  description: 1
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner: 1
  event status: OK
FTOS#

Example 2

Figure 41-5. show rmon event brief Command Example

FTOS#show rmon event br
index  description
-------  ---------------
  1       1
  2       2
  3       3
  4       4
  5       5
  6       6
  7       7
  8       8
  9       9
 10      10
 11      11
 12      12
 13      13
 14      14
 15      15
 16      16
 17      17
 18      18
 19      19
 20      20
 21      21
 22      22
FTOS#
show rmon hc-alarm
Display the contents of RMON High-Capacity Alarm Table.

Syntax
show rmon hc-alarm [index] [brief]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>(OPTIONAL) Enter the table index number to display just that entry.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to display the RMON High-Capacity Alarm Table in an easy-to-read format.</td>
</tr>
</tbody>
</table>

Defaults
none

Command Modes
EXEC

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example 1
Figure 41-6. show rmon hc-alarm brief Command Example

FTOS#show rmon hc-alarm brief
index SNMP OID
1 1.3.6.1.2.1.1.3
2 1.3.6.1.2.1.1.3
3 1.3.6.1.2.1.1.3
4 1.3.6.1.2.1.1.3
5 1.3.6.1.2.1.1.3

Example 2
Figure 41-7. show rmon hc-alarm index Command Example

FTOS#show rmon hc-alarm 1
RMON high-capacity alarm entry 1
object: 1.3.6.1.2.1.1.3
sample interval: 5
sample type: absolute value.
value: 185638
alarm type: rising or falling alarm.
alarm rising threshold value: positive.
rising threshold: 1001, RMON event index: 1
alarm falling threshold value: positive.
falling threshold: 999, RMON event index: 6
alarm sampling failed 0 times.
alarm owner: 1
alarm storage type: non-volatile.
alarm status: OK

show rmon history
Display the contents of the RMON Ethernet History table.

Syntax
show rmon history [index] [brief]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>(OPTIONAL) Enter the table index number to display just that entry.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to display the RMON Ethernet History table in an easy-to-read format.</td>
</tr>
</tbody>
</table>

Defaults
none
show rmon log

Display the contents of RMON log table.

Syntax

show rmon log [index] [brief]

Parameters

index (OPTIONAL) Enter the log index number to display just that entry.
brief (OPTIONAL) Enter the keyword brief to display the RMON Log Table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example 1

Figure 41-10. show rmon log index Command Example

FTOS#show rmon log 2
RMON log entry, alarm table index 2, log index 1
log time: 14638 (THU AUG 12 22:10:40 2004)
description: 2

FTOS#
Figure 41-11. show rmon log brief Command Example

```
FTOS#show rmon log br
eventIndex description
-----------------------------------------------
  2               2
  4               4
FTOS#
```

Usage Information

The log table has a maximum of 500 entries. If the log exceeds that maximum, the oldest log entry is purged to allow room for the new entry.

**show rmon statistics**

Display the contents of RMON ethernet statistics table.

**Syntax**

```
show rmon statistics [index] [brief]
```

**Parameters**

- `index` (OPTIONAL) Enter the index number to display just that entry.
- `brief` (OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet Statistics table in an easy-to-read format.

**Defaults**

none

**Command Modes**

EXEC

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example 1  Figure 41-12. show rmon statistics index Command Example

```plaintext
FTOS#show rmon statistics 6001
RMON statistics entry 6001
    interface: ifIndex.100974631 TenGigabitEthernet 2/1
    packets dropped: 0
    bytes received: 0
    packets received: 0
    broadcast packets: 0
    multicast packets: 0
    CRC error: 0
    under-size packets: 0
    over-size packets: 0
    fragment errors: 0
    jabber errors: 0
    collision: 0
    64bytes packets: 0
    65-127 bytes packets: 0
    128-255 bytes packets: 0
    256-511 bytes packets: 0
    512-1023 bytes packets: 0
    1024-1518 bytes packets: 0
    owner: 1
    status: OK
    <high-capacity data>
    HC packets received overflow: 0
    HC packets received: 0
    HC bytes received overflow: 0
    HC bytes received: 0
    HC 64bytes packets overflow: 0
    HC 64bytes packets: 0
    HC 65-127 bytes packets overflow: 0
    HC 65-127 bytes packets: 0
    HC 128-255 bytes packets overflow: 0
    HC 128-255 bytes packets: 0
    HC 256-511 bytes packets overflow: 0
    HC 256-511 bytes packets: 0
    HC 512-1023 bytes packets overflow: 0
    HC 512-1023 bytes packets: 0
    HC 1024-1518 bytes packets overflow: 0
    HC 1024-1518 bytes packets: 0
```
Rapid Spanning Tree Protocol (RSTP)

Overview

The Dell Networking operating software (FTOS) implementation of the rapid spanning tree protocol (RSTP) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a bridged local area network (LAN) that is comprised of LANs interconnected by bridges.

Commands

The FTOS RSTP commands are:

- bridge-priority
- debug spanning-tree rstp
- description
- forward-delay
- hello-time
- max-age
- edge-port bpdufilter default
- protocol spanning-tree rstp
- show config
- show spanning-tree rstp
- spanning-tree rstp
- tc-flush-standard

bridge-priority

Set the bridge priority for RSTP.

Syntax

bridge-priority priority-value

To return to the default value, use the no bridge-priority command.

Parameters

<table>
<thead>
<tr>
<th>priority-value</th>
<th>Enter a number as the bridge priority value in increments of 4096.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>0 to 61440</td>
</tr>
<tr>
<td>Default</td>
<td>32768</td>
</tr>
</tbody>
</table>

Defaults

32768
**debug spanning-tree rstp**

Enable debugging of RSTP and view information on the protocol.

**Syntax**

d debug spanning-tree rstp [all | bpdu interface {in | out} | events]

To disable debugging, use the no debug spanning-tree rstp command.

**Parameters**

- **all** (OPTIONAL) Enter the keyword all to debug all spanning tree operations.
- **bpdu interface {in | out}** (OPTIONAL) Enter the keyword bpdu to debug Bridge Protocol Data Units. Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following:
  - For a Port Channel interface, enter the keyword port-channel followed by a number: Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGige followed by the slot/port information.
  Optionally, enter an in or out parameter in conjunction with the optional interface:
    - For Receive, enter in
    - For Transmit, enter out
- **events** (OPTIONAL) Enter the keyword events to debug RSTP events.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#debug spanning-tree rstp bpdu tengigabitethernet 2/0 ?
in Receive (in) out Transmit (out)
```

**description**

Enter a description of the rapid spanning tree

**Syntax**

description {description}

To remove the description, use the no description {description} command.
### disable

Disable RSTP globally on the system.

**Syntax**

disable

To enable rapid spanning tree protocol, use the **no disable** command.

**Defaults**

RSTP is disabled

**Command Modes**

CONFIGURATION RSTP (conf-rstp)

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `protocol spanning-tree rstp` — Enters SPANNING TREE mode on the switch.

### forward-delay

Configure the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

**Syntax**

forward-delay *seconds*

To return to the default setting, use the **no forward-delay** command.

**Parameters**

- **seconds**
  - Enter the number of seconds that FTOS waits before transitioning RSTP to the forwarding state.
  - Range: 4 to 30
  - Default: 15 seconds

**Defaults**

15 seconds

**Command Modes**

CONFIGURATION RSTP (conf-rstp)

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `protocol spanning-tree rstp` — Enters Rapid Spanning Tree mode
hello-time

Set the time interval between generation of RSTP bridge protocol data units (BPDUs).

Syntax

```
hello-time [milli-second] seconds
```

To return to the default value, use the `no hello-time` command.

Parameters

- **seconds**: Enter a number as the time interval between transmission of BPDUs.
  - Range: 1 to 10 seconds
  - Default: 2 seconds.

- **milli-second**: Enter this keyword to configure a hello time on the order of milliseconds.
  - Range: 50 - 950 milliseconds

Defaults

2 seconds

Command Modes

- CONFIGURATION RSTP (conf-rstp)

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The hello time is encoded in BPDUs in increments of 1/256ths of a second. The standard minimum hello time in seconds is 1 second, which is encoded as 256. Millisecond hello times are encoded using values less than 256; the millisecond hello time equals \((x/1000)\times256\).

When millisecond hellos are configured, the default hello interval of 2 seconds is still used for edge ports; the millisecond hello interval is not used.

Related Commands

- `forward-delay` Changes the wait time before RSTP transitions to the Forwarding state.
- `max-age` Changes the wait time before RSTP refreshes protocol configuration information.

max-age

Set the time interval for the RSTP bridge to maintain configuration information before refreshing that information.

Syntax

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

Parameters

- **max-age**: Enter a number of seconds the FTOS waits before refreshing configuration information.
  - Range: 6 to 40 seconds
  - Default: 20 seconds

Defaults

20 seconds
### edge-port bpdufilter default

Enable BPDU Filter globally to filter transmission of BPDU on port fast enabled interfaces.

**Syntax**

```
edge-port bpdufilter default
```

To disable global bpdu filter default, use the `no edge-port bpdufilter default` command.

**Defaults**

Disabled

**Command Modes**

- CONFIGURATION (conf-rstp)

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

### protocol spanning-tree rstp

Enter the RSTP mode to configure RSTP.

**Syntax**

```
protocol spanning-tree rstp
```

To exit the RSTP mode, use the `exit` command.

**Defaults**

Not configured

**Command Modes**

- CONFIGURATION RSTP (conf-rstp)

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 42-2. protocol spanning-tree rstp Command Example**

```
FTOS(conf)#protocol spanning-tree rstp
FTOS(conf-rstp)#no disable
```

**Usage Information**

RSTP is not enabled when you enter RSTP mode. To enable RSTP globally on the system, use the `no description` command from RSTP mode.

**Related Commands**

- `description` - Disable RSTP globally on the system.
show config

View the current configuration for the mode. Only non-default values are displayed.

Syntax
show config

Command Modes
CONFIGURATION RSTP (conf-rstp)

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 42-3. show config Command Example for RSTP Mode

```
FTOS(conf-rstp)#show config
!
protocol spanning-tree rstp
no disable
bridge-priority 16384
```

show spanning-tree rstp

Display the RSTP configuration.

Syntax
show spanning-tree rstp [brief] [guard]

Parameters
brief (OPTIONAL) Enter the keyword brief to view a synopsis of the RSTP configuration information.

guard (OPTIONAL) Enter the keyword guard to display the type of guard enabled on an RSTP interface and the current port state.

Command Modes
EXEC

EXEC Privilege
FTOS#show spanning-tree rstp brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 8192, Address 0001.e805.e306
Root Bridge hello time 4, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally

<table>
<thead>
<tr>
<th>Interface</th>
<th>Designated PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts Cost</th>
<th>Bridge ID</th>
<th>PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGig 4/0</td>
<td>128.418</td>
<td>128</td>
<td>20000</td>
<td>FWD 20000</td>
<td>16384 0001.e801.6aa8</td>
<td>128.418</td>
</tr>
<tr>
<td>TenGig 4/1</td>
<td>128.419</td>
<td>128</td>
<td>20000</td>
<td>FWD 20000</td>
<td>16384 0001.e801.6aa8</td>
<td>128.419</td>
</tr>
<tr>
<td>TenGig 4/8</td>
<td>128.426</td>
<td>128</td>
<td>20000</td>
<td>FWD 20000</td>
<td>8192 0001.e805.e306</td>
<td>128.130</td>
</tr>
<tr>
<td>TenGig 4/9</td>
<td>128.427</td>
<td>128</td>
<td>20000</td>
<td>BLK 20000</td>
<td>8192 0001.e805.e306</td>
<td>128.131</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Bpdu PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts Cost</th>
<th>Link-type</th>
<th>Edge</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGig 4/0</td>
<td>128.418</td>
<td>128</td>
<td>20000</td>
<td>FWD 20000</td>
<td>P2P</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>TenGig 4/1</td>
<td>128.419</td>
<td>128</td>
<td>20000</td>
<td>FWD 20000</td>
<td>P2P</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>TenGig 4/8</td>
<td>128.426</td>
<td>128</td>
<td>20000</td>
<td>FWD 20000</td>
<td>P2P</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>TenGig 4/9</td>
<td>128.427</td>
<td>128</td>
<td>20000</td>
<td>BLK 20000</td>
<td>P2P</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

FTOS#
**Example 2**

**Figure 42-5. show spanning-tree rstp with EDS and LBK**

```
FTOS#show spanning-tree rstp br
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root
Configured hello time 2, max age 20, forward delay 15

Interface          Designated
Name               PortID  Prio  Cost  Sts  Cost     Bridge ID          PortID
------------------ -------- ---- ------- --- ------- -------------------- --------
          TenGig 0/0 128.257   128  20000   EDS   0     32768 0001.e801.6aa8 128.257

```

```
FTOS#show spanning-tree rstp
Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 0
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 0
We are the root
Current root has priority 32768, Address 0001.e801.6aa8
Number of topology changes 1, last change occurred 00:00:31 ago on TenGig 0/0
Port 257 (TenGigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU : sent 27, received 9
The port is not in the Edge port mode, bpdu filter is disabled

```

**Example 3**

**Figure 42-6. show spanning-tree rstp guard Command Example**

```
FTOS#show spanning-tree rstp guard

<table>
<thead>
<tr>
<th>Interface</th>
<th>Instance</th>
<th>Sts</th>
<th>Guard type</th>
<th>Bpdu Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGig 0/1</td>
<td>0</td>
<td>INCON(Root) Rootguard</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>TenGig 0/2</td>
<td>0</td>
<td>FWD</td>
<td>Loopguard</td>
<td>No</td>
</tr>
<tr>
<td>TenGig 0/3</td>
<td>0</td>
<td>BLK</td>
<td>Bpduguard</td>
<td>No</td>
</tr>
</tbody>
</table>

```

**Table 42-1. show spanning-tree rstp guard Command Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>RSTP interface</td>
</tr>
<tr>
<td>Instance</td>
<td>RSTP instance</td>
</tr>
<tr>
<td>Sts</td>
<td>Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), disabled (DIS), or shut down (EDS Shut)</td>
</tr>
<tr>
<td>Guard Type</td>
<td>Type of STP guard configured (Root, Loop, or BPDU guard)</td>
</tr>
<tr>
<td>BPDU Filter</td>
<td>Yes - BPDU Filter enabled</td>
</tr>
<tr>
<td></td>
<td>No - BPDU Filter disabled</td>
</tr>
</tbody>
</table>
spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional Bridge Port Data Unit (BPDU) guard, port priority, loop guard, or root guard.

**Syntax**

```
spanning-tree rstp {cost port-cost | edge-port [bpduguard [shutdown-on-violation] | bpdufilter] | priority priority | {rootguard}}
```

**Parameters**

- **cost port-cost**
  - Enter the keyword `cost` followed by the port cost value.
  - Range: 1 to 200000
  - Defaults:
    - 10-Gigabit Ethernet interface = 2000
    - 40-Gigabit Ethernet interface = 1400
    - Port Channel interface with one 10-Gigabit Ethernet = 2000
    - Port Channel interface with one 40-Gigabit Ethernet = 1400
    - Port Channel with two 10-Gigabit Ethernet = 1800
    - Port Channel with two 40-Gigabit Ethernet = 600

- **edge-port**
  - Enter the keyword `edge-port` to configure the interface as a Rapid Spanning Tree edge port.

- **bpduguard**
  - (OPTIONAL) Enter the keyword `bpduguard` to disable the port when it receives a BPDU.

- **shutdown-on-violation**
  - (OPTIONAL) Enter the keyword `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

- **bpdufilter**
  - (OPTIONAL) Enter the keyword `bpdufilter` to enable BPDU Filter to stop sending and receiving BPDUs on port enabled interfaces.

- **priority priority**
  - Enter keyword `priority` followed by a value in increments of 16 as the priority.
  - Range: 0 to 240
  - Default: 128

- **rootguard**
  - Enter the keyword `rootguard` to enable root guard on an RSTP port or port-channel interface.

**Defaults**

Not configured

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40Gbe Switch IO Module

---

**Note:** Loop guard is not supported in the `show spanning-tree rstp guard` command.
The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is mis-configured, or is subject to a DOS attack. This option places the port into an error disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.

**Note:** A port configured as an edge port on an RSTP switch, immediately transitions to the Forwarding state. Only ports connected to end-hosts should be configured as edge ports. Consider an edge port similar to a port with a spanning-tree portfast enabled.

If you do not enable the `shutdown-on-violation` command, BPDUs are still sent to the CPU.

You cannot enable STP root guard and loop guard at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed:

```
% Error: RootGuard is configured. Cannot configure LoopGuard.
```

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent blocking state and no traffic is forwarded on the port.

**Example Figure 42-7. spanning-tree rstp edge-port Command Example**

```
FTOS(conf)#interface tengigabitethernet 4/0
FTOS(conf-if-teng-4/0)#spanning-tree rstp edge-port
FTOS(conf-if-teng-4/0)#show config

interface TenGigabitEthernet 4/0
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
FTOS#
```

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

**Syntax**

```
tc-flush-standard
```

To disable, use the `no tc-flush-standard` command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
By default FTOS implements an optimized flush mechanism for RSTP. This helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on this knob command to enable flushing MAC addresses after receiving every topology change notification.
Security

Commands

This chapter describes various types of security commands in the Dell Networking operating software (FTOS), in the following sections:

• AAA Accounting Commands
• Authorization and Privilege Commands
• Authentication and Password Commands
• RADIUS Commands
• TACACS+ Commands
• SSH Server and SCP Commands
• Secure DHCP Commands

For configuration details, refer to the Security chapter in the FTOS Configuration Guide.

Note: Starting with FTOS version 7.2.1.0, LEAP with MSCHAP v2 supplicant is implemented.

AAA Accounting Commands

AAA accounting enables tracking of services that users are accessing and the amount of network resources being consumed by those services. When you enable AAA accounting, the network server reports user activity to the terminal access controller access control system (TACACS+) security server in the form of accounting records. Each accounting record is comprised of accounting Attribute/Value (AV) pairs and is stored on the access control server.

As with authentication and authorization, you must configure AAA accounting by defining named list of accounting methods, and then applying that list to various interfaces. The commands in this section are:

• aaa accounting
• aaa accounting suppress
• accounting
• show accounting
aaa accounting

Enable AAA accounting and create a record for monitoring the accounting function.

**Syntax**

```plaintext
aaa accounting {system | exec | commands level} {name | default} {start-stop | wait-start | stop-only} {tacacs+}
```

To disable AAA Accounting, use the `no aaa accounting {system | exec | command level} {name | default} {start-stop | wait-start | stop-only} {tacacs+}` command.

**Parameters**

- **system**
  - Enter the keyword `system` to send accounting information of any other AAA configuration.

- **exec**
  - Enter the keyword `exec` to send accounting information when a user has logged in to the EXEC mode.

- **commands level**
  - Enter the keyword `command` followed by a privilege level for accounting of commands executed at that privilege level.

- **name | default**
  - Enter one of the following:
    - For `name`, a user-defined name of a list of accounting methods
    - `default` for the default accounting methods

- **start-stop**
  - Enter the keyword `start-stop` to send a “start accounting” notice at the beginning of the requested event and a “stop accounting” notice at the end of the event.

- **wait-start**
  - Enter the keyword `wait-start` to ensure that the TACACS+ security server acknowledges the start notice before granting the user’s process request.

- **stop-only**
  - Enter the keyword `stop-only` to instruct the TACACS+ security server to send a “stop record accounting” notice at the end of the requested user process.

- **tacacs+**
  - Enter the keyword `tacacs+` to use TACACS+ data for accounting. FTOS currently only supports TACACS+ accounting.

**Defaults**

none

**Command Modes**

- **CONFIGURATION**

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

**Example**

```plaintext
FTOS(conf)# aaa accounting exec default start-stop tacacs+
FTOS(conf)# aaa accounting command 15 default start-stop tacacs+
```

**Usage Information**

In Figure 43-1, TACACS+ accounting is used to track all usage of EXEC command and commands on privilege level 15.

Privilege level 15 is the default. If you want to track usage at privilege level 1, for example, use `aaa accounting command 1`.

**Related Commands**

- `enable password` Changes the password for the enable command.
- `login authentication` Enables AAA login authentication on terminal lines.
- `password` Creates a password.
- `tacacs-server host` Specifies a TACACS+ server host.
aaa accounting suppress

Prevent the generation of accounting records of users with user name value of NULL.

Syntax

```
aaa accounting suppress null-username
```

To permit accounting records to users with user name value of NULL, use the no aaa accounting suppress null-username command

Defaults

Accounting records are recorded for all users.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

FTOS issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the aaa authentication login method-list none command is applied. Use aaa accounting suppress command to prevent accounting records from being generated for sessions that do not have user names associated to them.

accounting

Apply an accounting method list to terminal lines.

Syntax

```
accounting \{exec | commands level\} method-list
```

Parameters

- `exec` Enter this keyword to apply an EXEC level accounting method list.
- `commands level` Enter this keyword to apply an EXEC and CONFIGURATION level accounting method list.
- `method-list` Enter a method list that you defined using the command `aaa accounting exec` or `aaa accounting commands`.

Defaults

none

Command Modes

LINE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

`aaa accounting` Enables AAA Accounting and create a record for monitoring the accounting function.

show accounting

Display the active accounting sessions for each online user.

Syntax

```
show accounting
```

Defaults

none
Authorization and Privilege Commands

Set command line authorization and privilege levels with the following commands:

- authorization
- aaa authorization commands
- aaa authorization config-commands
- aaa authorization exec
- privilege level (CONFIGURATION mode)
- privilege level (LINE mode)

authorization

Apply an authorization method list to terminal lines.

Syntax

```
authorization {exec | commands level} method-list
```

Parameters

- `exec` Enter this keyword to apply an EXEC level authorization method list.
- `commands level` Enter this keyword to apply an EXEC and CONFIGURATION level authorization method list.
- `method-list` Enter a method list that you defined using the command `aaa authorization exec` or `aaa authorization commands`.

Defaults

none

Command Modes

LINE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

This command steps through all active sessions and then displays the accounting records for the active account functions.
aaa authorization commands
Set parameters that restrict (or permit) a user’s access to EXEC and CONFIGURATION level commands.

**Syntax**
```
aaa authorization commands level {name | default} {local || tacacs+ || none}
```
To undo a configuration, use the `no aaa authorization commands level {name | default} {local || tacacs+ || none}` command.

**Parameters**
- `commands level` Enter the keyword commands followed by the command privilege level for command level authorization.
- `name` Define a name for the list of authorization methods.
- `default` Define the default list of authorization methods.
- `local` Use the authorization parameters on the system to perform authorization.
- `tacacs+` Use the TACACS+ protocol to perform authorization.
- `none` Enter this keyword to apply no authorization.

**Defaults**
none

**Command Modes**
CONFIGURATION

**Command History**
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

aaa authorization exec
Sets the parameters that restrict (or permit) a user’s access to EXEC level commands.

**Syntax**
```
aaa authorization exec
```

**Usage Information**
By default, the `aaa authorization commands` command configures the system to check both EXEC level and CONFIGURATION level commands. To enable only EXEC-level command checking, use the `no aaa authorization config-commands` command.

aaa authorization config-commands
Set parameters that restrict (or permit) a user’s access to EXEC level commands.

**Syntax**
```
aaa authorization config-commands
```
To disable authorization checking for CONFIGURATION level commands, use the `no aaa authorization config-commands` command.

**Defaults**
Enabled when you configure `aaa authorization commands` command.

**Command Modes**
CONFIGURATION

**Command History**
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
aaa authorization exec

Set parameters that restrict (or permit) a user’s access to EXEC-level commands.

**Syntax**

```plaintext
aaa authorization exec {name | default} {local || tacacs+ || if-authenticated || none}
```

To disable authorization checking for EXEC level commands, use the `no aaa authorization exec` command.

**Parameters**

- **name**
  - Define a name for the list of authorization methods.

- **default**
  - Define the default list of authorization methods.

- **local**
  - Use the authorization parameters on the system to perform authorization.

- **tacacs+**
  - Use the TACACS+ protocol to perform authorization.

- **none**
  - Enter this keyword to apply no authorization.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on M XL 10/40Gbe Switch IO Module

---

**privilege level (CONFIGURATION mode)**

Change the access or privilege level of one or more commands.

**Syntax**

```plaintext
privilege mode {level level command | reset command}
```

To delete access to a level and command, use the `no privilege mode level level command` command.

**Parameters**

- **mode**
  - Enter one of the following keywords as the mode for which you are controlling access:
    - configure for the CONFIGURATION mode
    - exec for the EXEC mode
    - interface for the INTERFACE modes
    - line for the LINE mode
    - route-map for theROUTE-MAP mode
    - router for the ROUTER OSPF, ROUTER RIP, and ROUTER BGP modes.

- **level**
  - Enter the keyword `level` followed by a number for the access level.
  - Range: 0 to 15.
  - Level 1 is the EXEC mode and Level 15 allows access to all CLI modes and commands.

- **reset**
  - Enter the keyword `reset` to return the security level to the default setting.

- **command**
  - Enter the command’s keywords to assign the command to a certain access level. You can enter one or all of the keywords.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION
To define a password for the level to which you are assigning privilege or access, use the `enable password` command.

**privilege level (LINE mode)**

Change the access level for users on the terminal lines.

**Syntax**

```
privilege level level
```

To delete access to a terminal line, use the `no privilege level level` command.

**Parameters**

- `level level`
  
  Enter the keyword `level` followed by a number for the access level.
  
  Range: 0 to 15.
  
  Level 1 is the EXEC mode and Level 15 allows access to all CLI modes.

**Defaults**

`level = 15`

**Command Modes**

LINE

---

**Authentication and Password Commands**

This section contains the following commands controlling management access to the system:

- `aaa authentication enable`
- `aaa authentication login`
- `access-class`
- `enable password`
- `enable restricted`
- `enable secret`
- `login authentication`
- `password`
- `password-attributes`
- `privilege level (CONFIGURATION mode)`
- `privilege level (LINE mode)`
- `service password-encryption`
- `show privilege`
- `show users`
- `timeout login response`
- `username`
aaa authentication enable

Configure AAA Authentication method lists for user access to the EXEC privilege mode (the “Enable” access).

**Syntax**

```plaintext
aaa authentication enable {default | method-list-name} method [... method2]
```

To return to the default setting, use the `no aaa authentication enable {default | method-list-name} method [... method2]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enter the keyword <code>default</code> followed by the authentication methods to use as the default sequence of methods to be used for the Enable log-in. Default: <code>default enable</code></td>
</tr>
<tr>
<td>method-list-name</td>
<td>Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at log in.</td>
</tr>
<tr>
<td>method</td>
<td>Enter one of the following methods:</td>
</tr>
<tr>
<td></td>
<td>• <code>enable</code> - use the password defined by the <code>enable password</code> command in the CONFIGURATION mode.</td>
</tr>
<tr>
<td></td>
<td>• <code>line</code> - use the password defined by the <code>password</code> command in the LINE mode.</td>
</tr>
<tr>
<td></td>
<td>• <code>none</code> - no authentication.</td>
</tr>
<tr>
<td></td>
<td>• <code>radius</code> - use the RADIUS server(s) configured with the <code>radius-server host</code> command.</td>
</tr>
<tr>
<td></td>
<td>• <code>tacacs+</code> - use the TACACS+ server(s) configured with the <code>tacacs-server host</code> command.</td>
</tr>
<tr>
<td>method2</td>
<td>(OPTIONAL) In the event of a “no response” from the first method, FTOS applies the next configured method.</td>
</tr>
</tbody>
</table>

**Defaults**

Use the `enable password`.  

**Command Modes**

CONFIGURATION

**Command History**

*Version 8.3.16.1* Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

By default, the Enable password is used. If you configure `aaa authentication enable default`, FTOS uses the methods defined for Enable access instead.

Methods configured with the `aaa authentication enable` command are evaluated in the order they are configured. If authentication fails using the primary method, FTOS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, FTOS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable password</code></td>
<td>Changes the password for the <code>enable</code> command.</td>
</tr>
<tr>
<td><code>login authentication</code></td>
<td>Enables AAA login authentication on terminal lines.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Creates a password.</td>
</tr>
<tr>
<td><code>radius-server host</code></td>
<td>Specifies a RADIUS server host.</td>
</tr>
<tr>
<td><code>tacacs-server host</code></td>
<td>Specifies a TACACS+ server host.</td>
</tr>
</tbody>
</table>
aaa authentication login

Configure AAA Authentication method lists for user access to the EXEC mode (Enable log-in).

Syntax

```
aaa authentication login {method-list-name | default} method [... method4]
```

To return to the default setting, use the `no aaa authentication login {method-list-name | default}` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>method-list-name</code></td>
<td>Enter a text string (up to 16 characters long) as the name of a user-configured method list that can be applied to different lines.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Enter the keyword <code>default</code> to specify that the method list specified is the default method for all terminal lines.</td>
</tr>
<tr>
<td><code>method</code></td>
<td>Enter one of the following methods:</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- use the password defined by the <code>enable password</code> command in the CONFIGURATION mode.</td>
</tr>
<tr>
<td><code>line</code></td>
<td>- use the password defined by the <code>password</code> command in the LINE mode.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>- use the user name/password defined by the in the local configuration.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>- no authentication.</td>
</tr>
<tr>
<td><code>radius</code></td>
<td>- use the RADIUS server(s) configured with the <code>radius-server host</code> command.</td>
</tr>
<tr>
<td><code>tacacs+</code></td>
<td>- use the TACACS+ server(s) configured with the <code>tacacs-server host</code> command.</td>
</tr>
<tr>
<td>... <code>method4</code></td>
<td>(OPTIONAL) Enter up to four additional methods. In the event of a “no response” from the first method, FTOS applies the next configured method (up to four configured methods).</td>
</tr>
</tbody>
</table>

Default

Not configured (that is, no authentication is performed)

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

By default, the locally configured username password is used. If you configure `aaa authentication login default`, FTOS uses the methods defined by this command for login instead.

Methods configured with the `aaa authentication login` command are evaluated in the order they are configured. If users encounter an error with the first method listed, FTOS applies the next method configured. If users fail the first method listed, no other methods are applied. The only exception is the local method. If the user’s name is not listed in the local database, the next method is applied. If the correct user name/password combination are not entered, the user is not allowed access to the switch.

```
Note: If authentication fails using the primary method, FTOS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, FTOS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.
```

After configuring the `aaa authentication login` command, to enable the authentication scheme on terminal lines, configure the `login authentication` command.
Connections to the SSH server works with the following login mechanisms: local, radius, and tacacs.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>login authentication</td>
</tr>
<tr>
<td>password</td>
</tr>
<tr>
<td>radius-server host</td>
</tr>
<tr>
<td>tacacs-server host</td>
</tr>
</tbody>
</table>

**access-class**

Restrict incoming connections to a particular IP address in a defined IP access control list (ACL).

**Syntax**

```plaintext
global access-class access-list-name
```

To delete a setting, use the `no access-class` command.

**Parameters**

- **access-list-name**
  - Enter the name of an established IP Standard ACL.

**Defaults**

Not configured.

**Command Modes**

LINE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- **line**
  - Applies an authentication method list to designated terminal lines.
- **ip access-list standard**
  - Names (or selects) a standard access list to filter based on IP address.
- **ip access-list extended**
  - Names (or selects) an extended access list based on IP addresses or protocols.

**enable password**

Change the password for the `enable` command.

**Syntax**

```plaintext
enable password [level level] [encryption-type] password
```

To delete a password, use the `no enable password [encryption-type] password [level level]` command.

**Parameters**

- **level level**
  - (OPTIONAL) Enter the keyword `level` followed by a number as the level of access.
  - Range: 1 to 15

- **encryption-type**
  - (OPTIONAL) Enter the number 7 or 0 as the encryption type.
  - Enter a 7 followed by a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router.
  - Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.

- **password**
  - Enter a text string, up to 32 characters long, as the clear text password.
Use this command to define a password for a level. Use the privilege level (CONFIGURATION mode) command to control access to command modes.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, you must use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type “abcd CNTL v ] e”. When the password is created, you do not use the CNTL + v key combination and enter “abcd]e”.

**Note:** The question mark (?) and the tilde (~) are not supported characters.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Views the current configuration.</td>
</tr>
<tr>
<td><code>privilege level (CONFIGURATION mode)</code></td>
<td>Controls access to command modes within the switch.</td>
</tr>
</tbody>
</table>

### enable restricted

**Syntax**

```
enable restricted [encryption-type] password
```

**Parameters**

- `encryption-type` (OPTIONAL) Enter the number 7 as the encryption type. Enter 7 followed a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.

- `password` Enter a text string, up to 32 characters long, as the clear text password.

**Command Modes**

Not configured.

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Only Dell Networking Technical Support staff use this command.
enable secret

Change the password for the enable command.

**Syntax**

```plaintext
enable secret [level level] [encryption-type] password
```

To delete a password, use the `no enable secret [encryption-type] password [level level]` command.

**Parameters**

- **level level** *(OPTIONAL)* Enter the keyword `level` followed by a number as the level of access.
  - Range: 1 to 15
- **encryption-type** *(OPTIONAL)* Enter the number 5 or 0 as the encryption type.
  - Enter a 5 followed by a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
- **password** Enter a text string, up to 32 characters long, as the clear text password.

**Defaults**

No password is configured. `level = 15`

**Command Modes**

- `CONFIGURATION`

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Use this command to define a password for a level. Use the `privilege level (CONFIGURATION mode)` command to control access to command modes.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, you must use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type `abcd CNTL v] e` and when the password is created, you do not use the CNTL + v key combination and enter `abcd] e`.

**Note:** The question mark (?) and the tilde (~) are not supported characters.

**Related Commands**

- `show running-config` Views the current configuration.
- `privilege level (CONFIGURATION mode)` Controls access to command modes.

---

**login authentication**

Apply an authentication method list to designated terminal lines.

**Syntax**

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

To use the local user/password database for login authentication, use the `no login authentication` command.
Parameters

- `method-list-name` Enter the `method-list-name` to specify that method list, created in the `aaa authentication login` command, to be applied to the designated terminal line.

- `default` Enter the keyword `default` to specify that the default method list, created in the `aaa authentication login` command, is applied to the terminal line.

Defaults

No authentication is performed on the console lines, and local authentication is performed on the virtual terminal and auxiliary lines.

Command Modes

LINE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

If you configure the `aaa authentication login default` command, the `login authentication default` command automatically is applied to all terminal lines.

Related Commands

- `aaa authentication login` Selects login authentication methods.

---

**password**

Specify a password for users on terminal lines.

**Syntax**

`password [encryption-type] password`

To delete a password, use the `no password password` command.

**Parameters**

- `encryption-type` (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the `password` entered. The options are:
  - 0 is the default and means the password is not encrypted and stored as clear text.
  - 7 means that the password is encrypted and hidden.

- `password` Enter a string up to 32 characters long. The first character of the `password` must be a letter. You cannot use spaces in the password.

**Defaults**

No password is configured.

**Command Modes**

LINE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

FTOS prompts users for these passwords when the method for authentication or authorization used is “line”.

**Related Commands**

- `enable password` Sets the password for the `enable` command.
- `login authentication` Configures an authentication method to log in to the switch.
- `service password-encryption` Encrypts all passwords configured in FTOS.
password-attributes

Configure the password attributes (strong password).

**Syntax**

```
password-attributes [min-length number] [max-retry number] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]
```

To return to the default, use the `no password-attributes [min-length number] [max-retry number] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]` command.

**Parameters**

- **min-length number**
  - (OPTIONAL) Enter the keyword `min-length` followed by the number of characters.
  - Range: 0 - 32 characters

- **max-retry number**
  - (OPTIONAL) Enter the keyword `max-retry` followed by the number of maximum password retries.
  - Range: 0 - 16

- **character-restriction**
  - (OPTIONAL) Enter the keyword `character-restriction` to indicate a character restriction for the password.

- **upper number**
  - (OPTIONAL) Enter the keyword `upper` followed by the upper number.
  - Range: 0 - 31

- **lower number**
  - (OPTIONAL) Enter the keyword `lower` followed by the lower number.
  - Range: 0 - 31

- **numeric number**
  - (OPTIONAL) Enter the keyword `numeric` followed by the numeric number.
  - Range: 0 - 31

- **special-char number**
  - (OPTIONAL) Enter the keyword `special-char` followed by the number of special characters permitted.
  - Range: 0 - 31

**Defaults**

- none

**Command Modes**

- CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `password` Specifies a password for users on terminal lines.
service password-encryption
Encrypt all passwords configured in FTOS.

Syntax
service password-encryption

To store new passwords as clear text, use the no service password-encryption command.

Defaults
Enabled.

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Caution: Encrypting passwords with this command does not provide a high level of security. When the passwords are encrypted, you cannot return them to plain text unless you re-configure them. To remove an encrypted password, use the no password password command.

Usage Information
To keep unauthorized people from viewing passwords in the switch configuration file, use the service password-encryption command. This command encrypts the clear-text passwords created for user name passwords, authentication key passwords, the privileged command password, and console and virtual terminal line access passwords.

To view passwords, use the show running-config command.

show privilege
View your access level.

Syntax
show privilege

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example
Figure 43-3. show privilege Command Example

FTOS#show privilege
Current privilege level is 15
FTOS#

Related Commands
privilege level (CONFIGURATION mode) Assigns access control to different command modes.
show users

View information on all users logged into the switch.

**Syntax**

```
show users [all]
```

**Parameters**

- `all` *(OPTIONAL)* Enter the keyword `all` to view all terminal lines in the switch.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#show users
Line            User                      Host(s)    Location
  0 console 0    admin                     idle
  *           3 vty 1         admin                     idle       172.31.1.4
FTOS#
```

Table 1 describes the information in the `show users` command example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(untitled)</td>
<td>Indicates with an asterisk (*) which terminal line you are using.</td>
</tr>
<tr>
<td>Line</td>
<td>Displays the terminal lines currently in use.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the user name of all users logged in.</td>
</tr>
<tr>
<td>Host(s)</td>
<td>Displays the terminal line status.</td>
</tr>
<tr>
<td>Location</td>
<td>Displays the IP address of the user.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `username` Enables a user.

timeout login response

Specify how long the software will wait for login input (for example, user name and password) before timing out.

**Syntax**

```
timeout login response seconds
```

To return to the default values, use the `no timeout login response` command.

**Parameters**

- `seconds` Enter a number of seconds the software will wait before logging you out. Range: 
  - `VTY`: 1 to 30 seconds, default: 30 seconds. 
  - `Console`: 1 to 300 seconds, default: 0 seconds (no timeout). 
  - `AUX`: 1 to 300 seconds, default: 0 seconds (no timeout).

**Defaults**

see above
username

Establish an authentication system based on user names.

Syntax

```
username name [access-class access-list-name] [nopassword | {password | secret} [encryption-type] password] [privilege level]
```

If you do not want a specific user to enter a password, use the `nopassword` option.

To delete authentication for a user, use the no username name command.

Parameters

- **name**: Enter a text string for the name of the user up to 63 characters.
- **access-class access-list-name**: Enter the keyword access-class followed by the name of a configured access control list (either an IP access control list or MAC access control list).
- **nopassword**: Enter the keyword nopassword to specify that the user should not enter a password.
- **password**: Enter the keyword password followed by the encryption-type or the password.
- **secret**: Enter the keyword secret followed by the encryption-type or the password.
- **encryption-type**: Enter an encryption type for the password that you will enter.
  - 0 directs FTOS to store the password as clear text. It is the default encryption type when using the password option.
  - 7 to indicate that a password encrypted using a DES hashing algorithm will follow. This encryption type is available with the password option only.
  - 5 to indicate that a password encrypted using an MD5 hashing algorithm will follow. This encryption type is available with the secret option only, and is the default encryption type for this option.
- **password**: Enter a string up to 32 characters long.
- **privilege level**: Enter the keyword privilege followed by a number from zero (0) to 15.
- **secret**: Enter the keyword secret followed by the encryption type.

Defaults

- The default encryption type for the password option is 0. The default encryption type for the secret option is 0.

Command Modes

- CONFIGURATION

Usage Information

To view the defined user names, use the show running-config user command.
RADIUS Commands

The RADIUS commands supported by FTOS are:

- debug radius
- ip radius source-interface
- radius-server deadtime
- radius-server host
- radius-server key
- radius-server retransmit
- radius-server timeout

**debug radius**

View RADIUS transactions to assist with troubleshooting.

**Syntax**

```text
debug radius
```

To disable debugging of RADIUS, use the `no debug radius` command.

**Defaults**

Disabled.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**ip radius source-interface**

Specify an interface’s IP address as the source IP address for RADIUS connections.

**Syntax**

```text
ip radius source-interface interface
```

To delete a source interface, use the `no ip radius source-interface` command.
radius-server deadtime

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

Syntax

```
radius-server deadtime seconds
```

To disable this function or return to the default value, use the `no radius-server deadtime` command.

Parameters

- **seconds**
  - Enter a number of seconds during which non-responsive RADIUS servers are skipped.
  - Range: 0 to 2147483647 seconds.
  - Default: 0 seconds.

Defaults

0 seconds

Command Modes

CONFIGURATION

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

radius-server host

Configure a RADIUS server host.

Syntax

```
radius-server host {hostname | ipv4-address} [auth-port port-number] [retransmit retries] [timeout seconds] [key [encryption-type] key]
```

Parameters

- **hostname**
  - Enter the name of the RADIUS server host.

- **ipv4-address**
  - Enter the IPv4 address (A.B.C.D) of the RADIUS server host.
auth-port *port-number* *(OPTIONAL) Enter the keyword auth-port followed by a number as the port number.
Range: zero (0) to 65535
The default *port-number* is 1812.

retransmit *retries* *(OPTIONAL) Enter the keyword retransmit followed by a number as the number of attempts. This parameter overwrites the radius-server retransmit command.
Range: zero (0) to 100
Default: 3 attempts

timeout *seconds* *(OPTIONAL) Enter the keyword timeout followed by the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the radius-server timeout command.
Range: 0 to 1000
Default: 5 seconds

key [encryption-type] *key* *(OPTIONAL) Enter the keyword key followed by an optional encryption-type and a string up to 42 characters long as the authentication key. This authentication key is used by the RADIUS host server and the RADIUS daemon operating on this switch.
For the encryption-type, enter either zero (0) or 7 as the encryption type for the *key* entered. The options are:
• 0 is the default and means the password is not encrypted and stored as clear text.
• 7 means that the password is encrypted and hidden.
Configure this parameter last because leading spaces are ignored.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
Use this command to configure any number of RADIUS server hosts for each server host that is configured. FTOS searches for the RADIUS hosts in the order they are configured in the software.

The global default values for timeout, retransmit, and key optional parameters are applied, unless those values are specified in the radius-server host or other commands. If you configure timeout, retransmit, or key values, you must include those keywords when entering the no radius-server host command syntax to return to the global default values.

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login authentication</td>
<td>Sets the database to be checked when a user logs in.</td>
</tr>
<tr>
<td>radius-server key</td>
<td>Sets a authentication key for RADIUS communications.</td>
</tr>
<tr>
<td>radius-server retransmit</td>
<td>Sets the number of times the RADIUS server will attempt to send information.</td>
</tr>
<tr>
<td>radius-server timeout</td>
<td>Sets the time interval before the RADIUS server times out.</td>
</tr>
</tbody>
</table>
radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

Syntax

radius-server key [encryption-type] key

To delete a password, use the no radius-server key command.

Parameters

- encryption-type
  - (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the key entered.
  - The options are:
    - 0 is the default and means the key is not encrypted and stored as clear text.
    - 7 means that the key is encrypted and hidden.

- key
  - Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The key configured on the switch must match the key configured on the RADIUS server daemon.

If the key parameter in the radius-server host command is configured, the key configured with the
radius-server key command is the default key for all RADIUS communications.

Related Commands

- radius-server host
  - Configures a RADIUS host.

radius-server retransmit

Configure the number of times the switch attempts to connect with the configured RADIUS host server before declaring the RADIUS host server unreachable.

Syntax

radius-server retransmit retries

To configure zero retransmit attempts, use the no radius-server retransmit command. To return to the default setting, use the radius-server retransmit 3 command.

Parameters

- retries
  - Enter a number of attempts that FTOS tries to locate a RADIUS server.
  - Range: zero (0) to 100.
  - Default: 3 retries.

Defaults

3 retries

Command Modes

CONFIGURATION

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
radius-server timeout

Configure the amount of time the RADIUS client (the switch) waits for a RADIUS host server to reply to a request.

**Syntax**

```
radius-server timeout seconds
```

To return to the default value, use the `no radius-server timeout` command.

**Parameters**

| `seconds` | Enter the number of seconds between an unsuccessful attempt and the FTOS times out. Range: zero (0) to 1000 seconds. Default: 5 seconds. |

**Defaults**

5 seconds

**Command Modes**

CONFIGURATION

**Command History**

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

**Related Commands**

| radius-server host | Configures a RADIUS host. |

---

### TACACS+ Commands

FTOS supports TACACS+ as an alternate method for login authentication. The following are TACACS+ commands:

- `debug tacacs+`
- `ip tacacs source-interface`
- `tacacs-server host`
- `tacacs-server key`

**debug tacacs+**

View TACACS+ transactions to assist with troubleshooting.

**Syntax**

```
depub tacacs+
```

To disable debugging of TACACS+, use the `no debug tacacs+` command.

**Defaults**

Disabled.

**Command Modes**

EXEC Privilege
**ip tacacs source-interface**

Specify an interface’s IP address as the source IP address for TACACS+ connections.

**Syntax**

```
ip tacacs source-interface interface
```

To delete a source interface, use the no ip tacacs source-interface command.

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16838.
    - For the Null interface, enter the keywords `null 0`.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
      - Range: 1 to 128
    - For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
    - For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

Not configured.

**Command Mode**

CONFIGURATION

**tacacs-server host**

Specify a TACACS+ host.

**Syntax**

```
tacacs-server host {hostname | ipv4-address} [port number] [timeout seconds] [key key]
```

**Parameters**

- **hostname**
  - Enter the name of the TACACS+ server host.
- **ipv4-address**
  - Enter the IPv4 address (A.B.C.D) of the TACACS+ server host.
- **port number**
  - (OPTIONAL) Enter the keyword `port` followed by a number as the port to be used by the TACACS+ server.
  - Range: zero (0) to 65535
  - Default: 49
timeout seconds  (OPTIONAL) Enter the keyword timeout followed by the number of seconds the switch waits for a reply from the TACACS+ server.
  Range: 0 to 1000
  Default: 10 seconds

key key  (OPTIONAL) Enter the keyword key followed by a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the tacacs-server key for the TACACS+ daemon.
  Configure this parameter last because leading spaces are ignored.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Usage Information
To list multiple TACACS+ servers to be used by the aaa authentication login command, configure this command multiple times.

If you are not configuring the switch as a TACACS+ server, you do not need to configure the port, timeout and key optional parameters. If you do not configure a key, the key assigned in the tacacs-server key command is used.

Related Commands
aaa authentication login  Specifies the login authentication method.

tacacs-server key  Configures a TACACS+ key for the TACACS server.

tacacs-server key
Configure a key for communication between a TACACS+ server and client.

Syntax
tacacs-server key [encryption-type] key

To delete a key, use the no tacacs-server key key command.

Parameters

encryption-type  (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the key entered. The options are:
  • 0 is the default and means the key is not encrypted and stored as clear text.
  • 7 means that the key is encrypted and hidden.

key  Enter a text string, up to 42 characters long, as the clear text password.
  Leading spaces are ignored.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Usage Information
The key configured with this command must match the key configured on the TACACS+ daemon.
SSH Server and SCP Commands

FTOS supports secure shell (SSH) protocol versions 1.5 and 2.0. SSH is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication. The SSH and SCP commands are:

- crypto key generate
- debug ip ssh
- ip scp topdir
- ip ssh authentication-retries
- ip ssh connection-rate-limit
- ip ssh hostbased-authentication
- ip ssh key-size
- ip ssh password-authentication
- ip ssh pub-key-file
- ip ssh rhostsfile
- ip ssh rsa-authentication (Config)
- ip ssh rsa-authentication (EXEC)
- ip ssh server
- show crypto
- show ip ssh
- show ip ssh client-pub-keys
- show ip ssh rsa-authentication
- ssh

**crypto key generate**

Generate keys for the SSH server.

**Syntax**

crypto key generate {rsa | rsa1}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsa</td>
<td>Enter the keyword rsa followed by the key size to generate a SSHv2 RSA host keys. Range: 1024 to 2048 Default: 1024</td>
</tr>
<tr>
<td>rsa1</td>
<td>Enter the keyword rsa1 followed by the key size to generate a SSHv1 RSA host keys. Range: 1024 to 2048 Default: 1024</td>
</tr>
</tbody>
</table>

**Defaults**

Key size 1024

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Figure 43-5. crypto key generate rsa1 Command Example

FTOS#conf
FTOS(conf)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024>: 1024
Host key already exists. Do you want to replace. [y/n] :y
FTOS(conf)#

Usage Information

The host keys are required for key-exchange by the SSH server. If the keys are not found when the server is enabled (ip ssh server enable), the keys are automatically generated.

This command requires user interaction and generates a prompt prior to overwriting any existing host keys.

Note: Only a user with superuser permissions should generate host-keys.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh server</td>
<td>Enables the SSH server.</td>
</tr>
<tr>
<td>show crypto</td>
<td>Displays the SSH host public keys</td>
</tr>
</tbody>
</table>

```
debug ip ssh
```

Enables collecting SSH debug information.

**Syntax**

debug ip ssh \{client | server\}

To disable debugging, use the no debug ip ssh \{client | server\} command.

**Parameters**

- **client**
  - Enter the keyword client to enable collecting debug information on the client.

- **server**
  - Enter the keyword server to enable collecting debug information on the server.

**Defaults**

Disabled on both client and server.

**Command Modes**

EXEC

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Debug information includes details for key-exchange, authentication, and established session for each connection.

```
ip scp topdir
```

Identify a location for files used in secure copy transfer.

**Syntax**

ip scp topdir *directory*

To return to the default setting, use the no ip scp topdir command.
The internal flash (flash:) is the default directory.

To configure the switch as a SCP server, use the `ip ssh server` command.

This command specifies the maximum number of attempts to authenticate a user on a SSH connection with the remote host for password authentication. SSH disconnects when the number of password failures exceeds authentication-retries.

This command specifies the maximum number of incoming SSH connections allowed per minute.

---

**Parameters**

- `directory` Enter a directory name.

**Defaults**

- The internal flash (flash:) is the default directory.

**Command Modes**

- `CONFIGURATION`

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

To configure the switch as a SCP server, use the `ip ssh server` command.

**Related Commands**

- `ip ssh server` Enables the SSH and SCP server on the switch.

---

**Syntax**

`ip ssh authentication-retries 1-10`

**Parameters**

- `1-10` Enter the number of maximum retries to authenticate a user.
  - Range: 1 to 10
  - Default: 3

**Defaults**

- 3

**Command Modes**

- `CONFIGURATION`

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

This command specifies the maximum number of attempts to authenticate a user on a SSH connection with the remote host for password authentication. SSH disconnects when the number of password failures exceeds authentication-retries.

This command specifies the maximum number of incoming SSH connections allowed per minute.

**Syntax**

`ip ssh connection-rate-limit 1-10`

**Parameters**

- `1-10` Enter the number of maximum number of incoming SSH connections allowed per minute.
  - Range: 1 to 10 per minute
  - Default: 10 per minute

**Defaults**

- 10 per minute

**Command Modes**

- `CONFIGURATION`
ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

Syntax

ip ssh hostbased-authentication enable

To disable hostbased-authentication for SSHv2 server, use the no ip ssh hostbased-authentication enable command.

Parameters

enable Enter the keyword enable to enable hostbased-authentication for SSHv2 server.

Defaults
Disable by default

Command Modes
CONFIGURATION

Usage Information
If you enable this command, clients can login without a password prompt. This provides two levels of authentication:

- rhost-authentication is done with the file specified in the ip ssh rhostfile command
- checking client host-keys is done with the file specified in the ip ssh pub-key-file command

If you execute no ip ssh rsa-authentication enable, host-based authentication is disabled.

Note: Administrators must specify the two files (rhosts and pub-key-file) to configure host-based authentication.

Related Commands

ip ssh pub-key-file Public keys of trusted hosts from a file.
ip ssh rhostsfile Trusted hosts and users for rhost authentication.

ip ssh key-size

Configure the size of the server-generated RSA SSHv1 key.

Syntax

ip ssh key-size 512-869

Parameters

512-869 Enter the key-size number for the server-generated RSA SSHv1 key.
Range: 512 to 869
Default: 768

Defaults
Key size 768

Command Modes
CONFIGURATION
The server-generated key is used for SSHv1 key-exchange.

**ip ssh password-authentication**

Enable password authentication for the SSH server.

**Syntax**

```
ip ssh password-authentication enable
```

To disable password-authentication, use the `no ip ssh password-authentication enable` command.

**Parameters**

| enable | Enter the keyword enable to enable password-authentication for the SSH server. |

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

With password authentication enabled, you can authenticate using local, RADIUS, or TACACS+ password fallback order as configured.

**ip ssh pub-key-file**

Specify the file to be used for host-based authentication.

**Syntax**

```
ip ssh pub-key-file {WORD}
```

**Parameters**

| WORD | Enter the file name for the host-based authentication. |

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#conf
FTOS(conf)# ip ssh pub-key-file flash://knownhosts
FTOS(conf)#
```
This command specifies the file to be used for the host-based authentication. The file creates/overwrites the file flash://ADMIN_DIR/ssh/knownhosts and deletes the user specified file. Even though this is a global configuration command, it does not appear in the running configuration because this command needs to be run just once.

The file contains the OpenSSH compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAAbIwAAAIEAox/QOq8xYhz0xmt07yh4VGPAoUfkgKoiieTHO9G4sNV+uievDWGe3cYAcuU5Lai1MU2ODrzhCwvDnp05tKBU3tReGl08Axl6+iS4iyEmqHzkzBFNVqHzpQc+Rsvp2uozV0F4pRKnaxDhf3Lk4D460HZRlhVrxqenPDpEnW1MPJf0ds= ashwani@poclab4
```

**Note:** For rhostfile and pub-key-file, the administrator must FTP the file to the chassis.

### Related Commands

- `show ip ssh client-pub-keys` Displays the client-public keys used for the host-based authentication.

### ip ssh rhostsfile

Specify the rhost file to be used for host-based authorization.

**Syntax**

```
ip ssh rhostsfile {WORD}
```

**Parameters**

- `{WORD}`
  - Enter the rhost file name for the host-based authentication.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#conf
FTOS(conf)# ip ssh rhostsfile flash://hosts
FTOS(conf)#
```

**Usage Information**

This command specifies the rhost file to be used for host-based authentication. This file creates/overwrites the file flash://ADMIN_DIR/ssh/hosts and deletes the user specified file. Even though this is a global configuration command, it does not appear in the running configuration because this command needs to be run just once.

This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.

**Note:** For rhostfile and pub-key-file, the administrator must FTP the file to the switch.
ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

Syntax

ip ssh rsa-authentication enable

To disable RSA authentication, use the no ip ssh rsa-authentication enable command.

Parameters

enable Enter the keyword enable to enable RSA authentication for the SSHv2 server.

Defaults

RSA authentication is disabled by default.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Enabling RSA authentication allows you to login without being prompted for a password. In addition, the OpenSSH compatible SSHv2 RSA public key must be added to the list of authorized keys (ip ssh rsa-authentication my-authorized-keys device://filename command).

Related Commands

ip ssh rsa-authentication (EXEC) Adds keys for RSA authentication.

ip ssh rsa-authentication (EXEC)

Add keys for the RSA authentication.

Syntax

ip ssh rsa-authentication {my-authorized-keys WORD}

To delete the authorized keys, use the no ip ssh rsa-authentication {my-authorized-keys} command.

Parameters

my-authorized-keys WORD Enter the keyword my-authorized-keys followed by the file name of the RSA authorized-keys.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

If you want to log in without being prompted for a password, log in through RSA authentication. To do that, you must first add the SSHv2 RSA public keys to the list of authorized keys. This command adds the specified RSA keys to the following file:
flash://ADMIN_DIR/ssh/authorized-keys-username (where username is the user associated with this terminal).

Note: The no form of this command deletes the file flash://ADMIN_DIR/ssh/authorized-keys-username
ip ssh server

Configure an SSH server.

**Syntax**

```
ip ssh server {enable | port port-number} [version {1 | 2}]```

To disable SSH server functions, use the `no ip ssh server enable` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enter the key word <code>enable</code> to start the SSH server.</td>
</tr>
<tr>
<td>port port-number</td>
<td>(OPTIONAL) Enter the keyword <code>port</code> followed by the port number of the listening port of the SSH server. Range: 1 to 65535 Default: 22</td>
</tr>
<tr>
<td>version {1</td>
<td>2}</td>
</tr>
</tbody>
</table>

**Defaults**

Default listening port is 22.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.

**Example**

```
FTOS# conf
FTOS(conf)# ip ssh server port 45
FTOS(conf)# ip ssh server enable
FTOS#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
<td>Displays the ssh information</td>
</tr>
</tbody>
</table>

show crypto

Display the public part of the SSH host-keys.

**Syntax**

```
show crypto key mypubkey {rsa | rsa1}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Enter the keyword <code>key</code> to display the host public key.</td>
</tr>
<tr>
<td>mypubkey</td>
<td>Enter the keyword <code>mypubkey</code> to display the host public key.</td>
</tr>
</tbody>
</table>
show crypto

This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

Related Commands

- show crypto key mypubkey rsa
- show crypto key mypubkey rsa1

show ip ssh

Display information about established SSH sessions.

Syntax

show ip ssh

Command Modes

EXEC

EXEC Privilege

Example

Figure 43-10.  show ip ssh Command Example

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
<td></td>
<td>FTOS#show ip ssh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2#show ip ssh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH server            : disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH server version    : v1 and v2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password Authentication: enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hostbased Authentication: disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA Authentication    : disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FTOS#</td>
</tr>
</tbody>
</table>

Related Commands

- ip ssh server
- show ip ssh client-pub-keys
show ip ssh client-pub-keys

Display the client public keys used in host-based authentication.

Syntax

show ip ssh client-pub-keys

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 43-11. show ip ssh client-pub-keys Command Example

```
FTOS#show ip ssh client-pub-keys
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIAwAAAIAOx/Qp8xYhsOnx7y4VGFaoUfgKolxTH09G4sNYx+ui+xW5Ec3cYAcU5Lai1MU2OdrzHCyyDNP05tKBU3tReGl08Axli6+S4hjyEMqHszBFNVqHzpQc+Rs4p2urzV0F4pRKnaXdhF3Lk4D660H0RhVrpXqEnXpPdEnWIMPJ10
    ds= ashwani@poclab4
FTOS#
```

Usage Information

This command displays the contents of the file flash://ADMIN_DIR/ssh/knownhosts

Related Commands

- **ip ssh pub-key-file** Configures the file name for the host-based authentication

show ip ssh rsa-authentication

Display the authorized-keys for the RSA authentication.

Syntax

show ip ssh rsa-authentication {my-authorized-keys}

Parameters

my-authorized-keys Display the RSA authorized keys.

Defaults

none

Command Modes

EXEC

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 43-12. show ip ssh rsa-authentication Command Example

```
FTOS#show ip ssh rsa-authentication my-authorized-keys
AAAAB3NzaC1yc2EAAAABIAwAAAIAEYkY171qFP+Q2DRh1v4c1Vz0S7QqRV1y1X1JOLMeO6Nd0WuYy9rQM4qJACpBtneOF2hF3X2hCMag242g+4nhmCt6Q+9pVYdloofsea5r09kS0xT0CMfHXZ3NuGCq90v33m9+U9tMwhS8vy8AVxdH4x4km3c3t5Jvc= freedom@poclab4
FTOS#
```
ssh

Open an SSH connection specifying the hostname, username, port number and version of the SSH client.

FTOS supports both inbound and outbound SSH sessions using IPv4 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

**Syntax**

```
ssh {hostname | ipv4 address} [-l username | -p port-number | -v {1 | 2}]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>(OPTIONAL) Enter the IP address or the hostname of the remote device.</td>
</tr>
<tr>
<td>ipv4 address</td>
<td>(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.</td>
</tr>
<tr>
<td>-l username</td>
<td>(OPTIONAL) Enter the keyword -l followed by the user name used in this SSH session. Default: The user name of the user associated with the terminal.</td>
</tr>
<tr>
<td>-p port-number</td>
<td>(OPTIONAL) Enter the keyword -p followed by the port number. Range: 1 to 65536 Default: 22</td>
</tr>
<tr>
<td>-v {1</td>
<td>2}</td>
</tr>
</tbody>
</table>

**Defaults**

As above.

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
Figure 43-13. ssh Command Example

FTOS#ssh 123.12.1.123 -l ashwani -p 5005 -v 2
```
Secure DHCP Commands

The dynamic host configuration protocol (DHCP) as defined by RFC 2131 provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks. The DHCP commands are:

- clear ip dhcp snooping
- ip dhcp relay
- ip dhcp snooping
- ip dhcp snooping database
- ip dhcp snooping binding
- ip dhcp snooping database renew
- ip dhcp snooping trust
- ip dhcp source-address-validation
- ip dhcp snooping vlan
- show ip dhcp snooping

**clear ip dhcp snooping**

Clear the DHCP binding table.

**Syntax**
clear ip dhcp snooping binding

**Command Modes**
EXEC Privilege

**Default**
none

**Command History**
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**
show ip dhcp snooping Displays the contents of the DHCP binding table.

**ip dhcp relay**

Enable Option 82.

**Syntax**
ip dhcp relay information-option [trust-downstream]

**Parameters**
trust-downstream Configure the system to trust Option 82 when it is received from the previous-hop router.

**Command Modes**
CONFIGURATION

**Default**
Disabled

**Command History**
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
ip dhcp snooping

Enable DHCP Snooping globally.

Syntax
[no] ip dhcp snooping

Command Modes
CONFIGURATION

Default
Disabled

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
When enabled, no learning takes place until snooping is enabled on a VLAN. After disabling DHCP Snooping, the binding table is deleted, and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

Related Commands
- ip dhcp snooping vlan — Enables DHCP Snooping on one or more VLANs.

ip dhcp snooping database

Delay writing the binding table for a specified time.

Syntax
ip dhcp snooping database write-delay minutes

Parameters
- minutes
  Range: 5 to 21600

Command Modes
CONFIGURATION

Default
none

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

Syntax
[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number

Parameters
- mac address
  Enter the keyword mac followed by the MAC address of the host to which the server is leasing the IP address.
- vlan-id
  Enter the keyword vlan-id followed by the VLAN to which the host belongs. Range: 2 to 4094
- ip ip-address
  Enter the keyword ip followed by the IP address that the server is leasing.
ip dhcp snooping database renew

Renew the binding table.

Syntax

ip dhcp snooping database renew

Command Modes

EXEC

EXEC Privilege

Default

none

Command History

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Related Commands

show ip dhcp snooping  Displays the contents of the DHCP binding table.

ip dhcp snooping trust

Configure an interface as trusted.

Syntax

[no] ip dhcp snooping trust

Command Modes

INTERFACE

Default

Untrusted

Command History

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module
ip dhcp source-address-validation
Enable IP Source Guard.

Syntax
[no] ip dhcp source-address-validation

Command Modes
INTERFACE

Default
Disabled

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ip dhcp snooping vlan
Enable DHCP Snooping on one or more VLANs.

Syntax
[no] ip dhcp snooping vlan name

Parameters
name Enter the name of a VLAN on which to enable DHCP Snooping.

Command Modes
CONFIGURATION

Default
Disabled

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
When enabled, the system begins creating entries in the binding table for the specified VLAN(s). Note that learning only happens if there is a trusted port in the VLAN.

Related Commands
ip dhcp snooping trust Configures an interface as trusted.

show ip dhcp snooping
Display the contents of the DHCP binding table.

Syntax
show ip dhcp snooping binding

Command Modes
EXEC

EXEC Privilege

Default
none

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands
clear ip dhcp snooping Clears the contents of the DHCP binding table.
sFlow

Overview

The Dell Networking operating software (FTOS) sFlow monitoring system includes an sFlow agent and an sFlow collector.

- The sFlow agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow collector.
- The sFlow collector analyses the sFlow datagrams received from the different devices and produces a network-wide view of traffic flows.

Important Points to Remember

- FTOS exports all sFlow packets to the sFlow collector. A small sampling rate can equate to a large number of exported packets. A backoff mechanism is automatically applied to reduce this amount. Some sampled packets may be dropped when the exported packet rate is high and the backoff mechanism is about to or is starting to take effect. The dropEvent counter, in the sFlow packet, is always zero.
- sFlow sampling is done on a per-port basis.
- Community list and local preference fields are not filled up in the extended gateway element in the sFlow datagram.
- The 802.1P source priority field is not filled up in the extended switch element in the sFlow datagram.
- Only Destination and Destination Peer AS numbers are packed in the dst-as-path field in the extended gateway element.
- If the packet being sampled is redirected using policy-based routing (PBR), the sFlow datagram may contain incorrect extended gateway/router information.
- The source virtual local area network (VLAN) field in the extended switch element is not packed in case of a routed packet.
- The destination VLAN field in the extended switch element is not packed in case of a multicast packet.
- The maximum number of packets that can be sampled and processed per second is:
  - 7500 packets when no extended information packing is enabled
  - 7500 packets when only extended-switch information packing is enabled (refer to sflow extended-switch enable)
  - 1600 packets when extended-router and/or extended-gateway information packing is enabled
The sFlow commands are:

- `sflow collector`
- `sflow enable (Global)`
- `sflow enable (Interface)`
- `sflow extended-switch enable`
- `sflow polling-interval (Global)`
- `sflow polling-interval (Interface)`
- `sflow sample-rate (Global)`
- `sflow sample-rate (Interface)`
- `show sflow`
- `show sflow stack-unit`

**sflow collector**

Configure a collector device to which sFlow datagrams are forwarded.

**Syntax**

```
sflow collector {ipv4-address} agent-addr {ipv4-address} [number [max-datagram-size number]] | [max-datagram-size number]
```

To delete a configured collector, use the `no sflow collector {ipv4-address} agent-addr {ipv4-address} [number [max-datagram-size number]] | [max-datagram-size number]` command.

**Parameters**

- `sflow collector ipv4-address`
  - Enter the IPv4 (A.B.C.D) of the sFlow collector device.
- `agent-addr ipv4-address`
  - Enter the IPv4 (A.B.C.D) of the sFlow agent in the router.
- `number`
  - (OPTIONAL) Enter the UDP port number (User Datagram Protocol).
  - Range: 0 to 65535
  - Default: 6343
- `max-datagram-size number`
  - (OPTIONAL) Enter the keyword `max-datagram-size` followed by the size number in bytes.
  - Range: 400 to 1500
  - Default: 1400

**Defaults**

Not configured

**Command Modes**

- CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You can configure up to two sFlow collectors (IPv4). If two collectors are configured, traffic samples are sent to both.

The sFlow agent address is carried in a field in SFlow packets and is used by the collector to identify the sFlow agent.
As part of the sFlow-MIB, if the simple network management protocol (SNMP) request originates from a configured collector, FTOS returns the corresponding configured agent IP in management information base (MIB) requests. FTOS checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, FTOS generates the following error:

%Error: Different agent-addr attempted for an existing collector

sflow enable (Global)

Enable sFlow globally.

Syntax

sflow enable

To disable sFlow, use the no sflow enable command.

Defaults

sFlow is disabled by default

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

In addition to this command, sFlow needs to be enabled on individual interfaces where you want sFlow sampling.

Related Commands

sflow enable (Interface) Enables sFlow on interfaces.

sflow enable (Interface)

Enable sFlow on Interfaces.

Syntax

sflow enable

To disable sFlow, use the no sflow enable command.

Defaults

sFlow is disabled by default on all interfaces

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

When you enable sFlow on an interface, flow sampling is done on any traffic going out of the interface.

Note: After a physical port is a member of a LAG, it inherits the sFlow configuration from the LAG port.

Related Commands

sflow enable (Global) Turns sFlow on globally
sflow extended-switch enable
Enable packing information on a switch only.

Syntax
sflow extended-switch enable

To disable packing information, use the no sflow extended-switch [enable] command.

Parameters

<table>
<thead>
<tr>
<th>enable</th>
<th>Enter the keyword enable to enable global extended information.</th>
</tr>
</thead>
</table>

Defaults
Disabled

Command Modes
CONFIGURATION

Command History

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

Usage Information
FTOS version 7.8.1.0 and later enhances the sflow implementation for real time traffic analysis to provide extended gateway information in cases where the destination IP addresses are learned by different routing protocols and for cases where the destination is reachable over ECMP.

Related Commands

| show sflow | Displays the sFlow configuration |

sflow polling-interval (Global)
Set the sFlow polling interval at a global level.

Syntax
sflow polling-interval interval value

To return to the default, use the no sflow polling-interval interval command.

Parameters

| interval value | Enter the interval value in seconds. Range: 15 to 86400 seconds Default: 20 seconds |

Defaults
20 seconds

Command Modes
CONFIGURATION

Command History

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

Usage Information
The polling interval for an interface is the maximum number of seconds between successive samples of counters to be sent to the collector. This command changes the global default counter polling (20 seconds) interval. You can configure an interface to use a different polling interval.

Related Commands

| sflow polling-interval (Interface) | Sets the polling interval for an interface |
sflow polling-interval (Interface)

Set the sFlow polling interval at an interface (overrides the global-level setting.)

Syntax

```
sflow polling-interval interval value
```

To return to the default, use the `no sflow polling-interval interval` command.

Parameters

- **interval value**: Enter the interval value in seconds.
  - Range: 15 to 86400 seconds
  - Default: The global counter polling interval

Defaults

The same value as the current global default counter polling interval.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

This command sets the counter polling interval for an interface.

Related Commands

- `sflow polling-interval (Global)`: Globally set the polling interval

sflow sample-rate (Global)

Change the global default sampling rate.

Syntax

```
sflow sample-rate value
```

To return to the default sampling rate, use the `no sflow sample-rate` command.

Parameters

- **value**: Enter the sampling rate value.
  - Range: 256 to 8388608 packets
  - Enter values in powers of 2 only, for example 4096, 8192, 16384 etc.
  - Default: 32768 packets

Defaults

32768

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Sample-rate is the average number of packets skipped before the sample is taken. This command changes the global default sampling rate. You can configure an interface to use a different sampling rate than the global sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power of 2 value. Select one of these two packet numbers and re-enter the command.
sflow sample-rate (Interface)

Change the Interface default sampling rate.

Syntax

```
sflow sample-rate value
```

To return to the default sampling rate, use the `no sflow sample-rate` command.

Parameters

- **value**: Enter the sampling rate value.
  - Range: 256 to 8388608 packets
  - Enter values in powers of 2 only, for example 4096, 8192, 16384 etc.
  - Default: 32768 packets

Defaults

The global default sampling

Command Modes

- CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

This command changes the sampling rate for an interface. By default, the sampling rate of an interface is set to the same value as the current global default sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power-of-2 value. Select one of these two number and re-enter the command.

Related Commands

- `sflow sample-rate (Global)`: Changes the sampling rate globally.

show sflow

Display the current sFlow configuration

Syntax

```
show sflow [interface]
```

Parameters

- **interface**: (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 40-Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` followed by the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

Command Modes

- EXEC

EXEC Privilege
show sflow stack-unit

Display the sFlow information on a stack unit.

Syntax

show sflow stack-unit {unit number}

Parameters

unit number (OPTIONAL) Enter a unit number to view information on the stack unit in that slot.

Range: 0 to 5.

Command Modes

EXEC

EXEC Privilege

Example

Figure 44-2. show sflow stack unit Command Example

FTOS#show sflow stack-unit 1
Stack-Unit 1
  Samples rcvd from h/w : 0
  Total UDP packets exported : 0
  UDP packets dropped : 0
FTOS#
Service Provider Bridging

Overview

Service Provider Bridging is composed of virtual local area network (VLAN) Stacking, Layer 2 Protocol Tunneling, and Provider Backbone Bridging as described in the FTOS Configuration Guide Service Provider Bridging chapter.

This chapter includes command line information (CLI) for the Dell Networking operating software (FTOS) Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel.

For more information, refer to VLAN Stacking, Spanning Tree Protocol (STP), and GARP VLAN Registration (GVRP).

Commands

The L2PT commands are:

- debug protocol-tunnel
- protocol-tunnel
- protocol-tunnel destination-mac
- protocol-tunnel enable
- protocol-tunnel rate-limit
- show protocol-tunnel

Important Points to Remember

- L2PT is enabled at the interface VLAN-Stack VLAN level. For more information about Stackable VLAN (VLAN-Stacking) commands, refer to VLAN Stacking.
- The default behavior is to disable protocol packet tunneling through the 802.1q tunnel.
- Rate-limiting is required to protect against bridge protocol data units (BPDU) attacks.
- A port channel (including through link aggregation control protocol (LACP) can be configured as a VLAN-Stack access or trunk port.
- Address resolution protocol (ARP) packets work as expected across the tunnel.
- Far-end failure detection (FEFD) works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (for example, open shortest path first [OSPF]) work as expected and carry over to the other end of the VLAN-Stack VLAN.
**debug protocol-tunnel**

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

**Syntax**

```
debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]
```

To disable debugging, use the `no debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]` command.

**Parameters**

- **interface** Enter one of the following interfaces and slot/port information:
  - For a Port Channel interface, enter the keyword `port-channel` then a number: The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- **in | out | both** Enter the keyword `in`, `out`, or `both` to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.
- **vlan vlan-id** Enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.
- **count value** Enter the keyword `count` then the number of debug outputs. The range is from 1 to 100.

**Defaults**

Debug disabled

**Command Modes**

EXEC Privilege

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**protocol-tunnel**

Enable protocol tunneling on a stacked (Q-in-Q) VLAN for specified protocol packets.

**Syntax**

```
protocol-tunnel {rate-limit rate | stp}
```

To disable protocol tunneling for a Layer 2 protocol, use the `no protocol-tunnel` command.

**Parameters**

- **rate-limit rate** Enter the keyword `rate-limit` followed by a number for the rate-limit for tunneled packets on the VMAN. The range is from 64 to 320.
- **stp** Enter the keyword `stp` to enable protocol tunneling on a spanning tree, including STP, MSTP, RSTP, and PVST.

**Defaults**

None

**Command Modes**

CONF-IF-VLAN

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Example

```
FTOS#conf
FTOS(conf)#interface vlan 2
FTOS(conf-if-vl-2)#vlan-stack compatible
FTOS(conf-if-vl-2)#member Gi1/2-3
FTOS(conf-if-vl-2)#protocol-tunnel stp
FTOS(conf-if-vl-2)#protocol-tunnel enable
```

Related Commands

- `show protocol-tunnel` Displays tunneling information for all VLANs.

**protocol-tunnel destination-mac**

Overwrite the BPDU destination MAC address with a specific value.

**Syntax**

```
protocol-tunnel destination-mac xstp address
```

**Parameters**

- `xstp` - Change the default destination MAC address used for L2PT to another value.

**Defaults**

The default destination MAC is 01:01:e8:00:00:00.

**Command Modes**

- **CONFIGURATION**

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When you enable VLAN-Stacking, no protocol packets are tunneled.

**Related Commands**

- `show protocol-tunnel` Displays tunneling information for all VLANs.

**protocol-tunnel enable**

Enable protocol tunneling globally on the system.

**Syntax**

```
protocol-tunnel enable
```

To disable protocol tunneling, use the `no protocol-tunnel enable` command.

**Defaults**

Disabled

**Command Modes**

- **CONFIGURATION**

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

FTOS must have the default CAM profile with the default microcode before you enable L2PT.
**protocol-tunnel rate-limit**

Enable traffic rate limiting per box.

**Syntax**

```
protocol-tunnel rate-limit rate
```

To reset the rate limit to the default, use the no protocol-tunnel rate-limit rate command.

**Parameters**

- **rate**
  
Enter the rate in frames per second. The range is from 75 to 3000. The default is 75.

**Defaults**

75 Frames per second

**Command Modes**

CONFIGURATION

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Figure 45-2. protocol-tunnel rate-limit Command Example

FTOS#
FTOS(conf)#
FTOS(conf)#protocol-tunnel rate-limit 1000
FTOS(conf)#
```

**Related Commands**

- `show protocol-tunnel` Displays tunneling information for all VLANs.
- `show running-config` Displays the current configuration.

**show protocol-tunnel**

Display protocol tunnel information for all or a specified VLAN-Stack VLAN.

**Syntax**

```
show protocol-tunnel [vlan vlan-id]
```

**Parameters**

- **vlan vlan-id**
  
  (OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display information for the one VLAN. The range is from 1 to 4094.

**Defaults**

None

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Figure 45-3. show protocol-tunnel Command Example

FTOS#show protocol-tunnel
System Rate-Limit: 75 frames/second
VLAN Protocols Interface
1000 STP,PVST Gi 5/7,Gi 5/6
1001 LLDP,GVRP Gi 5/7,Gi 5/6
1002 MMRP,MVRP Gi 5/7,Gi 5/6
1003 LACP,DOT1X Gi 5/7,Gi 5/6
1004 OAM,PAUSE Gi 5/7,Gi 5/6
1005 E-LMI Gi 5/7,Gi 5/6
```
Example Figure 45-4. show protocol-tunnel command example for a specific VLAN

```plaintext
FTOS#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface       Vlan    Protocol(s)
Gi1/2           2       STP, PVST
FTOS
```

Related Commands

- `show running-config` Displays the current configuration.
Simple Network Management Protocol (SNMP) and Syslog

Overview

This chapter contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog. The chapter contains the following sections:

- SNMP Commands
- Syslog Commands

SNMP Commands

The SNMP commands available in the Dell Networking operating software (FTOS) are:

- show snmp
- show snmp engineID
- show snmp group
- show snmp user
- snmp ifmib ifalias long
- snmp-server community
- snmp-server contact
- snmp-server enable traps
- snmp-server engineID
- snmp-server group
- snmp-server host
- snmp-server location
- snmp-server packetsize
- snmp-server trap-source
- snmp-server user
- snmp-server view
- snmp trap link-status

The SNMP is used to communicate management information between the network management stations and the agents in the network elements. FTOS supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. FTOS sends SNMP traps, which are messages informing an SNMP management system about the network. FTOS supports up to 16 SNMP trap receivers.
Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both local area network (LAN) and wide area network (WAN) applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
  - SNMP Timeout—greater than 3 seconds
  - SNMP Retry count—greater than 2 seconds
- If you are using access control lists (ACLs) in SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a virtual LAN (VLAN).

show snmp

Display the status of SNMP network elements.

Syntax

```
show snmp
```

Command Modes

- EXEC
- EXEC Privilege

Command History

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```

Example

```
FTOS#show snmp
32685 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
96988 Number of requested variables
  0 Number of altered variables
31681 Get-request PDUs
  968 Get-next PDUs
  0 Set-request PDUs
61727 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  9 No such name errors
  0 Bad values errors
  0 General errors
32649 Response PDUs
  29078 Trap PDUs
FTOS#
```

Related Commands

- `snmp-server community` Enables SNMP and set community string.

show snmp engineID

Display the identification of the local SNMP engine and all remote engines that are configured on the router.

Syntax

```
show snmp engineID
```
Command Modes

show snmp group

Display the group name, security model, status, and storage type of each group.

Syntax

show snmp group

Command Modes

EXEC
EXEC Privilege

Example

Figure 46-3 displays a group named ngroup. The ngroup has a security model of version 3 (v3), with authentication (auth), the read and notify name is nview with no write view name specified, and the row status is active.

Related Commands

show snmp user

Display the information configured on each SNMP user name.

Syntax

show snmp user

Related Commands

show snmp user

Configures an SNMP server group.
Command Modes
- EXEC
- EXEC Privilege

Example

Figure 46-4.  show snmp user Command Example

FTOS#show snmp user
User name: v1v2creadu
Engine ID: 0000178B0200001E02014A8
storage-type: nonvolatile   active
Authentication Protocol: None
Privacy Protocol: None
FTOS#

Command History
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

snmp ifmib ifalias long
Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

Syntax
snmp ifmib ifalias long

Defaults
Interface description truncated beyond 63 characters

Command Modes
- CONFIGURATION

Command History
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 46-5.  snmp ifmib ifalias long Command Example

!------command run on host connected to switch: --------------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This is a port connected to Router2. This is a port connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:

!------command run on Dell Force10 switch: --------------!
FTOS#snmp ifmib ifalias long

!------command run on server connected to switch: -------------------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This is a port connected to Router2. This is a port connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:

snmp-server community
Configure a new community string access for SNMPv1, v2, and v3.

Syntax
snmp-server community community-name {ro | rw} [security-name name] [access-list-name]

To remove access to a community, use the no snmp-server community community-string {ro | rw} [security-name name] [access-list-name] command.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community-name</td>
<td>Enter a text string (up to 20 characters long) to act as a password for SNMP.</td>
</tr>
<tr>
<td>ro</td>
<td>Enter the keyword ro to specify read-only permission.</td>
</tr>
<tr>
<td>rw</td>
<td>Enter the keyword rw to specify read-write permission.</td>
</tr>
<tr>
<td>security-name</td>
<td>(OPTIONAL) Enter the keyword security-name followed by the security name as defined by the community MIB.</td>
</tr>
<tr>
<td>access-list-name</td>
<td>(OPTIONAL) Enter a standard IPv4 access list name (a string up to 16 characters long).</td>
</tr>
</tbody>
</table>

### Defaults

none

### Command Modes

CONFIGURATION

### Command History

Version 8.3.16.1
Introduced on MXL 10/40GbE Switch IO Module

### Usage Information

Figure 46-6 configures a community named guest that is mapped to the security named guestuser with Read Only (ro) permissions.

**Example Figure 46-6. snmp-server community Command Example**

FTOS#config
FTOS(conf)# snmp-server community guest ro
FTOS(conf)# snmp-server community guest ro security-name guestuser
FTOS(conf)#

The security-name parameter maps the community string to an SNMPv3 user/security name as defined by the community MIB.

If a community string is configured without a security-name (for example, snmp-server community public ro), the community is mapped to a default security-name/group:

- v1v2creadu / v1v2creadg — maps to a community with ro permissions
- v1v2cwriteu/ v1v2cwriteg — maps to a community with rw permissions

This command is indexed by the community-name parameter.

If you do not configure the snmp-server community command, you cannot query SNMP data. Only Standard IPv4 ACL is supported in the optional access-list-name.

The command options security-name and access-list-name are recursive. In other words, each option can, in turn, accept any of the three options as a sub-option, and each of those sub-options can accept any of the three sub-options as a sub-option, and so forth. Figure 46-7 shows the creation of a standard IPv4 ACL called “snmp-ro-acl” and then assigning it to the SNMP community “guest”:

**Example Figure 46-7. snmp-server community Command Example**

FTOS(conf)# ip access-list standard snmp-ro-acl
FTOS(conf-standard-nacl)#seq 5 permit host 10.10.10.224
FTOS(conf-standard-nacl)#seq 10 deny any count !

FTOS(conf)#snmp-server community guest ro snmp-ro-acl
FTOS(conf)#
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list standard</td>
<td>Names (or selects) a standard access list to filter based on IP address.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the current SNMP configuration and defaults.</td>
</tr>
</tbody>
</table>

**snmp-server contact**

Configure contact information for troubleshooting this SNMP node.

**Syntax**

```plaintext
snmp-server contact text
```

To delete the SNMP server contact information, use the `no snmp-server contact` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>Enter an alphanumeric text string, up to 55 characters long.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**snmp-server enable traps**

Enable SNMP traps.

**Syntax**

```plaintext
snmp-server enable traps [notification-type] [notification-option]
```

To disable traps, use the `no snmp-server enable traps [notification-type] [notification-option]` command.
**snmp-server engineID**

Configure name for both the local and remote SNMP engines on the router.

**Syntax**

```
snmp-server engineID [local engineID] [remote ip-address udp-port port-number engineID]
```

To return to the default, use the `no snmp-server engineID [local engineID] [remote ip-address udp-port port-number engineID]` command.
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local engineID</code></td>
<td>Enter the keyword <code>local</code> followed by the engine ID number that identifies</td>
</tr>
<tr>
<td></td>
<td>the copy of the SNMP on the <code>local</code> device.</td>
</tr>
<tr>
<td><code>remote ip-address</code></td>
<td>Enter the keyword <code>remote</code> followed by the IP address that identifies</td>
</tr>
<tr>
<td></td>
<td>the copy of the SNMP on the <code>remote</code> device.</td>
</tr>
<tr>
<td><code>udp-port port-number engineID</code></td>
<td>Enter the keyword <code>udp-port</code> followed by the UDP (User Datagram</td>
</tr>
<tr>
<td></td>
<td>Protocol) port number on the remote device.</td>
</tr>
</tbody>
</table>

Defaults
As above

Command Modes

**CONFIGURATION**

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Changing the value of the SNMP Engine ID has important side effects. A user’s password (entered on
the command line) is converted to a message digest 5 algorithm (MD5) or secure hash algorithm
(SHA) security digest. This digest is based on both the password and the local Engine ID. The
command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the
local value of the Engine ID changes, the security digests of SNMPv3 users will be invalid, and the
users will have to be reconfigured.

For the remote Engine ID, the host IP and UDP port are the indexes to the command that are matched
to either overwrite or remove the configuration.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show snmp engineID</code></td>
<td>Displays SNMP engine and all remote engines that are configured on the</td>
</tr>
<tr>
<td></td>
<td>router.</td>
</tr>
<tr>
<td><code>show running-config snmp</code></td>
<td>Displays the SNMP running configuration.</td>
</tr>
</tbody>
</table>

**snmp-server group**

Configure a new SNMP group or a table that maps SNMP users to SNMP views.

Syntax

```
snmp-server group [group_name {1 | 2c | 3 {auth | noauth | priv}}] [read name] [write name] [notify name] [access-list-name | access-list-name]
```

To remove a specified group, use the `no snmp-server group [group_name {v1 | v2c | v3 {auth | noauth | priv}}] [read name] [write name] [notify name] [access-list-name | access-list-name]` command.
**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group_name</strong></td>
<td>Enter a text string (up to 20 characters long) as the name of the group. Defaults: The following groups are created for mapping to read/write community/security-names.</td>
</tr>
<tr>
<td>- <strong>vlv2creadg</strong></td>
<td>maps to a community/security-name with ro permissions</td>
</tr>
<tr>
<td>- <strong>vlv2cwriteg</strong></td>
<td>maps to a community/security-name rw permissions</td>
</tr>
<tr>
<td>**1</td>
<td>2c</td>
</tr>
<tr>
<td>- <strong>1</strong></td>
<td>is the least secure version</td>
</tr>
<tr>
<td>- <strong>3</strong></td>
<td>is the most secure of the security modes.</td>
</tr>
<tr>
<td>- <strong>2c</strong></td>
<td>allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. Default: 1</td>
</tr>
<tr>
<td><strong>auth</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>auth</strong> to specify authentication of a packet without encryption.</td>
</tr>
<tr>
<td><strong>noauth</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>noauth</strong> to specify no authentication of a packet.</td>
</tr>
<tr>
<td><strong>priv</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>priv</strong> to specify both authentication and then scrambling of the packet.</td>
</tr>
<tr>
<td><strong>read name</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>read</strong> followed by a name (a string of up to 20 characters long) as the read view name. Default: GlobalView is set by default and is assumed to be every object belonging to the Internet (1.3.6.1) OID space.</td>
</tr>
<tr>
<td><strong>write name</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>write</strong> followed by a name (a string of up to 20 characters long) as the write view name.</td>
</tr>
<tr>
<td><strong>notify name</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>notify</strong> followed by a name (a string of up to 20 characters long) as the notify view name.</td>
</tr>
<tr>
<td><strong>access-list-name</strong></td>
<td>(OPTIONAL) Enter the standard IPv4 access list name (a string up to 16 characters long).</td>
</tr>
</tbody>
</table>

**Defaults**

As defined above

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Figure 46-8 shows the group named **harig** as a version 3 user requiring both authentication and encryption and read access limited to the read named **rview**.

**Example**

```bash
FTOS#conf
FTOS(conf)# snmp-server group harig 3 priv read rview
FTOS#
```

**Note:** The number of configurable groups is limited to 16 groups.

---

Simple Network Management Protocol (SNMP) and Syslog | 885
### Related Commands

- `show snmp group` Displays the group name, security model, view status, and storage type of each group.
- `show running-config snmp` Displays the SNMP running configuration.

### `snmp-server host`

Configure the recipient of an SNMP trap operation.

**Syntax**

```
snmp-server host ip-address [traps | informs] [version 1 | 2c | 3] [auth | no auth | priv] [community-string] [udp-port port-number] [notification-type]
```

To remove the SNMP host, use the `no snmp-server host ip-address [traps | informs] [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type]` command.

**Parameters**

- `ip-address` Enter the keyword `host` followed by the IP address of the host (configurable hosts is limited to 16).
- `traps` (OPTIONAL) Enter the keyword `traps` to send trap notifications to the specified host. Default: traps
- `informs` (OPTIONAL) Enter the keyword `informs` to send inform notifications to the specified host. Default: traps
- `version 1 | 2c | 3` (OPTIONAL) Enter the keyword `version` to specify the security model followed by the security model version number 1, 2c, or 3.
  - Version 1 is the least secure version
  - Version 3 is the most secure of the security modes.
  - Version 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
  Default: Version 1
- `auth` (OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
- `noauth` (OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
- `priv` (OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
- `community-string` Enter a text string (up to 20 characters long) as the name of the SNMP community.

**Note:** For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command, however it is recommended that you set the community string using the `snmp-server community` command before executing this command. For version 3 security model, this string is the USM user security name.
In order to configure the router to send SNMP notifications, you must enter at least one `snmp-server host` command. If you enter the command with no keywords, all trap types are enabled for the host. If you do not enter an `snmp-server host` command, no notifications are sent.

In order to enable multiple hosts, you must issue a separate `snmp-server host` command for each host. You can specify multiple notification types in the command for each host.

When multiple `snmp-server host` commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last `snmp-server host` command will be in effect. For example, if you enter an `snmp-server host inform` command for a host and then enter another `snmp-server host inform` command for the same host, the second command will replace the first.

The `snmp-server host` command is used in conjunction with the `snmp-server enable` command. Use the `snmp-server enable` command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one `snmp-server enable` command and the `snmp-server host` command for that host must be enabled.

**Note:** For v1 / v2c trap configuration, if the community-string is not defined using the `snmp-server community` command prior to using this command, the default form of the `snmp-server community` command will automatically be configured, with the community-name the same as specified in the `snmp-server host` command.
To send a trap, follow these steps:
1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group for this user with access rights.
4. Enable traps.
5. Configure a host to receive informs.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server enable traps</code></td>
<td>Enables the SNMP traps.</td>
</tr>
<tr>
<td><code>snmp-server community</code></td>
<td>Configures a new community SNMPv1 or SNMPv2c.</td>
</tr>
</tbody>
</table>

### snmp-server location

Configure the location of the SNMP server.

**Syntax**

```
snmp-server location text
```

To delete the SNMP location, use the `no snmp-server location` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>text</code></td>
<td>Enter an alpha-numeric text string, up to 55 characters long.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

| Version 8.3.16.1   | Introduced on MXL 10/40GbE Switch IO Module |

### snmp-server packetsize

Set the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply, use the `snmp-server packetsize` global configuration command.

**Syntax**

```
snmp-server packetsize byte-count
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>byte-count</code></td>
<td>Enter one of the following values 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.</td>
</tr>
</tbody>
</table>

**Defaults**

8

**Command Modes**

CONFIGURATION

**Command History**

| Version 8.3.16.1   | Introduced on MXL 10/40GbE Switch IO Module |

Simple Network Management Protocol (SNMP) and Syslog

**snmp-server trap-source**

Configure a specific interface as the source for SNMP traffic.

**Syntax**

```
snmp-server trap-source interface
```

To disable sending traps out a specific interface, use the `no snmp trap-source` command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `interface` | Enter the following keywords and slot/port or number information:
  - For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information. |

**Defaults**
The IP address assigned to the management interface is the default.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

For this `snmp-server trap-source` command to be enabled, you must configure an IP address on the interface and enable the interface configured as an SNMP trap source.

**Related Commands**

- `snmp-server community` — Sets the community string.

**snmp-server user**

Configure a new user to an SNMP group.

**Syntax**

```
snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access-list-name]
```

To remove a user from the SNMP group, use the `no snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access-list-name]` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Enter the name of the user (not to exceed 20 characters), on the host, that connects to the agent.</td>
</tr>
</tbody>
</table>
| `group_name` | Enter a text string (up to 20 characters long) as the name of the group. Defaults: The following groups are created for mapping to read/write community/security-names.
  - `v1v2creadu` — maps to a community with `ro` permissions
  - `v1v2cwriteu` — maps to a community `rw` permissions |
| `remote ip-address` | Enter the keyword `remote` followed by the IP address that identifies the copy of the SNMP on the `remote` device. |
udp-port  port-number  Enter the keyword udp-port followed by the UDP (User Datagram Protocol) port number on the remote device.

Range: 0 to 65535.
Default: 162

1 | 2c | 3  (OPTIONAL) Enter the security model version number (1, 2c, or 3).
•  1 is the least secure version
•  3 is the most secure of the security modes.
•  2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

Default: 1

encrypted  (OPTIONAL) Enter the keyword encrypted to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).

auth  (OPTIONAL) Enter the keyword auth to specify authentication of a packet without encryption.

md5 | sha  (OPTIONAL) Enter the keyword md5 or sha to designate the authentication level.

md5 — Message Digest Algorithm
sha — Secure Hash Algorithm

auth-password  (OPTIONAL) Enter a text string (up to 20 characters long) password that will enable the agent to receive packets from the host.
Minimum: 8 characters long

priv des56  (OPTIONAL) Enter the keyword priv des56 to initiate a privacy authentication level setting using the CBC-DES privacy authentication algorithm (des56).

priv password  (OPTIONAL) Enter a text string (up to 20 characters long) password that will enables the host to encrypt the contents of the message it sends to the agent.
Minimum: 8 characters long

access-list-name  (OPTIONAL) Enter the standard IPv4 access list name (a string up to 16 characters long).

access-list-name  (OPTIONAL) Enter an IPv4 access list name.

Defaults

As above

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Usage Information

No default values exist for authentication or privacy algorithms and no default password exist. If you forget a password, you cannot recover it; the user must be reconfigured. You can specify either a plain-text password or an encrypted cypher-text password. In either case, the password will be stored in the configuration in an encrypted form and displayed as encrypted in the show running-config command.

If you have an encrypted password, you can specify the encrypted string instead of the plain-text password. Figure 46-9 shows how to specify the command with an encrypted string.

Examples

Figure 46-9.  snmp-server user Command Example (Encrypted)

FTOS# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d90818b2804fe80e3ba8763d priv des56 d0452401a8c3ce42804fe80e3ba8763d
Figure 46-10 shows how to enter a plain-text password as the string authpasswd for user authuser of group v3group.

**Figure 46-10. snmp-server user Command Example (Plain-text)**

```
FTOS#conf
FTOS(conf)# snmp-server user authuser v3group v3 auth md5 authpasswd
```

Figure 46-11 configures a remote user named n3user with a v3 security model and a security level of authNOPriv.

**Figure 46-11. config Command Example**

```
FTOS#conf
FTOS(conf)# snmp-server user n3user ngroup remote 172.31.1.3 udp-port 5009 3 auth md5 authpasswd
```

Note: The number of configurable users is limited to 16.

### Related Commands

- **show snmp user**
  Displays the information configured on each SNMP user name.

### snmp-server view

Configure an SNMPv3 view.

**Syntax**

```
snmp-server view view-name oid-tree (included | excluded)
```

To remove an SNMPv3 view, use the `no snmp-server view view-name oid-tree (included | excluded)` command.

**Parameters**

- **view-name**
  Enter the name of the view (not to exceed 20 characters).
- **oid-tree**
  Enter the OID sub tree for the view (not to exceed 20 characters).
- **included**
  (OPTIONAL) Enter the keyword included to include the MIB family in the view.
- **excluded**
  (OPTIONAL) Enter the keyword excluded to exclude the MIB family in the view.

**Defaults**

- none

**Command Modes**

- CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

The `oid-tree` variable is a full sub-tree starting from 1.3.6 and can not specify the name of a sub-tree or a MIB. Figure 46-12 configures a view named rview that allows access to all objects under 1.3.6.1.

**Example**

**Figure 46-12. snmp-server view Command Example**

```
FTOS#(conf) snmp-server view rview 1.3.6.1 included
```
snmp trap link-status

Enable the interface to send SNMP link traps, which indicate whether the interface is up or down.

Syntax

snmp trap link-status

To disable sending link trap messages, use the no snmp trap link-status command.

Defaults

Enabled.

Command Modes

INTERFACE

Usage Information

If the interface is expected to flap during normal usage, you can disable this command.

Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches:

- clear logging
- default logging buffered
- default logging console
- default logging monitor
- default logging trap
- logging
- logging buffered
- logging console
- logging facility
- logging history
- logging history size
- logging monitor
- logging on
- logging source-interface
- logging synchronous
- logging trap
- show logging
- show logging driverlog stack-unit
- terminal monitor
### clear logging

Clear the messages in the logging buffer.

**Syntax**

clear logging

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>Displays logging settings and system messages in the internal buffer.</td>
</tr>
</tbody>
</table>

### default logging buffered

Return to the default setting for messages logged to the internal buffer.

**Syntax**

default logging buffered

**Defaults**

size = 40960; level = 7 or debugging

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging buffered</td>
<td>Sets the logging buffered parameters.</td>
</tr>
</tbody>
</table>

### default logging console

Return the default settings for messages logged to the console.

**Syntax**

default logging console

**Defaults**

level = 7 or debugging

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging console</td>
<td>Sets the logging console parameters.</td>
</tr>
</tbody>
</table>
default logging monitor

Return to the default settings for messages logged to the terminal.

Syntax
default logging monitor

Defaults
level = 7 or debugging

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands
logging monitor Sets the logging monitor parameters.
terminal monitor Sends system messages to the terminal/monitor.

default logging trap

Return to the default settings for logging messages to the Syslog servers.

Syntax
default logging trap

Defaults
level = 6 or informational

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands
logging trap Limits the messages logged to the Syslog servers based on severity.

logging

Configure an IP address or host name of a Syslog server where logging messages will be sent. Multiple logging servers of IPv4 can be configured.

Syntax
logging {ipv4-address | hostname}

Parameters
ipv4-address Enter an IPv4 address (A.B.C.D).
hostname Enter the name of a host already configured and recognized by the switch.

Defaults
Disabled

Command Modes
CONFIGURATION

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

Syntax

logging buffered [level] [size]

To return to the default values, use the default logging buffered command. To disable logging stored to an internal buffer, use the no logging buffered command.

Parameters

- **level**
  - (OPTIONAL) Indicate a value from 0 to 7 or enter one of the following equivalent words: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
  - Default: 7 or debugging.

- **size**
  - (OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message.
  - Range: 40960 to 524288.
  - Default: 40960 bytes.

Defaults

`level = 7; size = 40960 bytes`

Command Modes

CONFIGURATION

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.

Related Commands

- clear logging
  - Clears the logging buffer.

- default logging buffered
  - Returns the logging buffered parameters to the default setting.

- show logging
  - Displays the logging setting and system messages in the internal buffer.

logging console

Specify which messages are logged to the console.

Syntax

logging console [level]

To return to the default values, use the default logging console command. To disable logging to the console, use the no logging console command.

Parameters

- **level**
  - (OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
  - Default: 7 or debugging.
logging facility

Configure the Syslog facility, used for error messages sent to Syslog servers.

Syntax

logging facility [facility-type]

To return to the default values, use the no logging facility command.

Parameters

facility-type  (OPTIONAL) Enter one of the following parameters.

- auth (authorization system)
- cron (Cron/at facility)
- deamon (system deamons)
- kern (kernel)
- local0 (local use)
- local1 (local use)
- local2 (local use)
- local3 (local use)
- local4 (local use)
- local5 (local use)
- local6 (local use)
- local7 (local use)
- lpr (line printer system)
- mail (mail system)
- news (USENET news)
- sys9 (system use)
- sys10 (system use)
- sys11 (system use)
- sys12 (system use)
- sys13 (system use)
- sys14 (system use)
- syslog (Syslog process)
- user (user process)
- uucp (Unix to Unix copy process)

The default is local7.

Defaults  local7

Command Modes  CONFIGURATION
logging history

Specify which messages are logged to the history table of the switch and the SNMP network management station (if configured).

Syntax

```
logging history level
```

Parameters

- `level`: Indicate a value from 0 to 7 or enter one of the following equivalent words: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 4.

Defaults

4 or warnings

Command Modes

CONFIGURATION

Usage Information

When you configure the `snmp-server trap-source` command, the system messages logged to the history table are also sent to the SNMP network management station.

Related Commands

- `logging`: Enables logging to a Syslog server.
- `logging on`: Enables logging.
- `logging history size`: Specifies the number of messages stored in the FTOS logging history table.
- `show logging history`: Displays information logged to the history buffer.

logging history size

Specify the number of messages stored in the FTOS logging history table.

Syntax

```
logging history size size
```

Parameters

- `size`: Indicate a value as the number of messages to be stored. Range: 0 to 500. Default: 1 message.

Defaults

1 message

Command Modes

CONFIGURATION
<table>
<thead>
<tr>
<th>Usage Information</th>
<th>When the number of messages reaches the limit you set with the <code>logging history size</code> command, older messages are deleted as newer ones are added to the table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Commands</td>
<td><code>show logging history</code> Displays information logged to the history buffer.</td>
</tr>
</tbody>
</table>

### logging monitor

Specify which messages are logged to Telnet applications.

**Syntax**

```
logging monitor [level]
```

To disable logging to terminal connections, use the `no logging monitor` command.

**Parameters**

- `level`
  
  Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
  
  The default is 7 or debugging.

**Defaults**

- 7 or debugging

**Command Modes**

- CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `default logging monitor` Returns the logging monitor parameters to the default setting.

### logging on

Specify that debug or error messages are asynchronously logged to multiple destinations, such as logging buffer, Syslog server, or terminal lines.

**Syntax**

```
logging on
```

To disable logging to logging buffer, Syslog server and terminal lines, use the `no logging on` command.

**Defaults**

- Enabled

**Command Modes**

- CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When you use the `no logging on` command, messages are logged only to the console.

**Related Commands**

- `logging` Enables logging to Syslog server.
- `logging buffered` Sets the logging buffered parameters.
- `logging console` Sets the logging console parameters.
- `logging monitor` Sets the logging parameters for the terminal connections.
logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

**Syntax**

```
logging source-interface interface
```

To disable this command and return to the default setting, use the `no logging source-interface` command.

**Parameters**

- `interface`
  - Enter the following keywords and slot/port or number information:
    - For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16383.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number: Range: 1-128
    - For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
    - For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Syslog messages contain the IP address of the interface used to egress the router. By configuring the `logging source-interface` command, the Syslog packets contain the IP address of the interface configured.

**Related Commands**

- `logging` Enables the logging to another device.

logging synchronous

Synchronize unsolicited messages and FTOS output.

**Syntax**

```
logging synchronous [level level | all] [limit number-of-buffers]
```

To disable message synchronization, use the `no logging synchronous [level level | all] [limit number-of-buffers]` command.

**Parameters**

- `all`
  - Enter the keyword `all` to ensure that all levels are printed asynchronously.

- `level level`
  - Enter the keyword `level` followed by a number as the severity level. A high number indicates a low severity level and visa versa.
  - Range: 0 to 7.
  - Default: 2
Defaults

Disabled. If enabled without level or number-of-buffers options specified, level = 2 and number-of-buffers = 20 are the defaults.

Command Modes

LINE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

When you enable logging synchronous, unsolicited messages appear between software prompts and outputs. Only the messages with a severity at or below the set level are sent to the console.

If the message queue limit is reached on a terminal line and messages are discarded, a system message appears on that terminal line. Messages may continue to appear on other terminal lines.

Related Commands

logging on Enables logging.

logging trap

Specify which messages are logged to the Syslog server based on the message severity.

Syntax

logging trap [level]

To return to the default values, use the default logging trap command. To disable logging, use the no logging trap command.

Parameters

level

Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.

The default is 6.

Defaults

6 or informational.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

logging Enables the logging to another device.

logging on Enables logging.
show logging

Display the logging settings and system messages logged to the internal buffer of the switch.

Syntax

```
show logging [number | history [reverse][number] | reverse [number] | summary]
```

Parameters

- `number` (OPTIONAL) Enter the number of message to be displayed on the output. Range: 1 to 65535
- `history` (OPTIONAL) Enter the keyword `history` to view only information in the Syslog history table.
- `reverse` (OPTIONAL) Enter the keyword `reverse` to view the Syslog messages in FIFO (first in, first out) order.
- `summary` (OPTIONAL) Enter the keyword `summary` to view a table showing the number of messages per type and per slot.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Figure 46-13. show logging Command Example (Partial)

```
FTOS#show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 311 Messages Logged, Size (40960 bytes)
  Trap logging: level informational
Logging to 172.16.1.162
  Logging to 10.10.10.4
  Logging to 10.1.2.4
  Logging to 172.31.1.4
  Logging to 133.33.33.4
May 22 10:21:10: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 ( 10.11.68.22 )by admin
May 22 10:16:35: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 ( 10.11.68.22 )by admin
May 22 09:39:12: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 ( 10.11.68.22 )by admin
May 22 09:03:56: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 ( 10.11.68.22 )by admin
May 22 09:01:51: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 ( 10.11.68.22 )by admin
May 22 08:53:09: %STKUNIT0-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 ( 10.11.68.22 )
May 22 08:53:04: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.11.68.22)
May 19 16:58:32: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty2 (10.11.68.22)
May 19 14:22:48: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty2 ( 10.11.68.22 )by admin
May 19 12:05:43: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty2 ( 10.11.68.22 )by admin
May 19 10:23:59: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 ( 10.11.68.22 )by admin
May 19 10:23:58: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec
-- More --
```
show logging driverlog stack-unit

Display the driver log for the specified stack member.

Syntax

show logging driverlog stack-unit unit#

Parameters

stack-unit unit# Enter the keyword stack-unit followed by the stack member ID of the switch for which you want to display the driver log.

Defaults

none

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

terminal monitor

Configure the FTOS to display messages on the monitor/terminal.

Syntax

terminal monitor

To return to default settings, use the terminal no monitor command.

Defaults

Disabled.

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

logging monitor Sets the logging parameters on the monitor/terminal.
Stacking Commands

Overview

For more information about using the MXL 10/40GbE Switch stacking feature, refer to the Stacking MXL 10/40GbE Switches chapter in the FTOS Configuration Guide.

Commands

The commands described in this chapter are used for managing the stacking of MXL 10/40GbE switch systems. The stacking commands are:

- redundancy disable-auto-reboot
- redundancy force-failover stack-unit
- reset stack-unit
- show redundancy
- show system stack-ports
- show system stack-unit stack-group
- stack-unit stack group
- stack-unit priority
- stack-unit provision
- stack-unit renumber

redundancy disable-auto-reboot

Prevent the MXL 10/40GbE switch stack unit from rebooting if they fail.

Syntax redundancy disable-auto-reboot stack-unit [0-5 | members]

To return to the default, use the no redundancy disable-auto-reboot stack-unit [0-5 | members] command.

Default Disabled (the failed switch is automatically rebooted).

Command Modes CONFIGURATION

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
When the command is given as redundancy disable-auto-reboot stack-unit, it prevents the MXL 10/40GbE switch stack management unit and standby unit from rebooting if they fail.

When a particular unit number in the range 0-5 is issued as part of the CLI, it prevents that particular unit from rebooting upon failure.

When members is issued as part of the CLI, all the units part of the stack are prevented from rebooting upon failure.

The unit does not reboot until it is manually rebooted.

show redundancy
Displays the current redundancy status.

redundancy force-failover stack-unit
Force the backup unit in the stack to become the management unit.

Syntax
redundancy force-failover stack-unit

Defaults
Not enabled

Command Modes
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

reset stack-unit
Reset any designated stack member except the management unit (master unit).

Syntax
reset stack-unit 0-5 hard

Parameters
0-5 Enter the stack member unit identifier of the stack member to reset.

hard Reset the stack unit if the unit is in a problem state.

Default
none

Command Modes
EXEC Privilege

Command History
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information
Resetting the management unit is not allowed (an error message is displayed if you try to do so). Resetting is a soft reboot, including flushing the forwarding tables.

You can run this command directly on the stack standby unit (Standby Master) to reset the standby. You cannot reset any other unit from the standby unit.
Example

Figure 47-1.  reset stack-unit Command Example on the Stack Standby Unit

```
FTOS# show system brief
Stack MAC : 00:1e:c9:f1:00:7b
Reload Type : jump-start [Next boot : normal-reload]

-- Stack Info --
Unit  UnitType    Status    ReqTyp          CurTyp         Version       Ports
-----------------------------------------------------------------------------------
0     Management   online    MXL-10/40GbE    MXL-10/40GbE   9-1-0-853     56
1     Standby      online    MXL-10/40GbE    MXL-10/40GbE   9-1-0-853     56
2     Member       online    MXL-10/40GbE    MXL-10/40GbE   9-1-0-853     56
3     Member       online    MXL-10/40GbE    MXL-10/40GbE   9-1-0-853     56
4     Member       online    MXL-10/40GbE    MXL-10/40GbE   9-1-0-853     56
5     Member       online    MXL-10/40GbE    MXL-10/40GbE   9-1-0-853     56

FTOS# reset stack-unit ?
<0-5>  Unit number id
FTOS# reset stack-unit 0
% Error: Reset of master unit is not allowed.  <<Resetting master not allowed
FTOS(standby)# reset stack-unit 3
% Error: Reset of stack units from standby is not allowed.  <<no reset of other member
FTOS(standby)# reset stack-unit 1  <<Resetting standby unit success!
00:02:50: %STKUNIT4-S:CP %CHMGR-5-STACKUNIT_RESET: Stack unit 4 being reset
00:02:50: %STKUNIT4-S:CP %CHMGR-2-STACKUNIT_DOWN: Stack unit 4 down - reset
00:02:50: %STKUNIT4-S:CP %IFMGR-1-DEL_PORT: Removed port: TenGig 4/1-48
FTOS# rebooting
U-Boot 1.1.4 (June 6 2012 - 00:00:04)
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Reboots FTOS.</td>
</tr>
<tr>
<td>redundancy disable-auto-reboot</td>
<td>Resets the designated stack member.</td>
</tr>
</tbody>
</table>

show redundancy

Display the current redundancy configuration (status of automatic reboot configuration on stack management unit).

Syntax

```
show redundancy
```

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module
Example

Figure 47-2. show redundancy Command Example

FTOS#show redundancy
-- Stack-unit Status --
----------------------------------
Mgmt ID:                          0
Stack-unit ID:                    0
Stack-unit Redundancy Role:       Primary
Stack-unit State:                 Active
Stack-unit SW Version:            E8-3-16-160
Link to Peer:                     Down
Peer Stack-unit:                  not present
-- Stack-unit Redundancy Configuration --
------------------------------------------
Primary Stack-unit:                mgmt-id 0
Auto Data Sync:                    Full
Failover Type:                     Hot Failover
Auto reboot Stack-unit:            Enabled
Auto failover limit:               3 times in 60 minutes
-- Stack-unit Failover Record --
----------------------------------
Failover Count:                   0
Last failover timestamp:          None
Last failover Reason:             None
Last failover type:               None
-- Last Data Block Sync Record:   --
----------------------------------------
Stack Unit Config:                 no block sync done
Start-up Config:                   no block sync done
Runtime Event Log:                 no block sync done
Running Config:                    no block sync done
ACL Mgr:                          no block sync done
LACP:                             no block sync done
STP:                              no block sync done
SPAN:                             no block sync done
FTOS#

Related Commands

redundancy disable-auto-reboot Prevents the system from auto-rebooting if it fails.

show system stack-ports

Display information about the stacking ports on all switches in the MXL 10/40GbE switch stack.

Syntax

show system stack-ports [status | topology]

Parameters

status (OPTIONAL) Enter the keyword status to display the command output without the Connection field.

topology (OPTIONAL) Enter the keyword topology to limit the table to just the Interface and Connection fields.

Defaults

none

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example

**Figure 47-3. show system stack-ports Command Example**

FTOS# show system stack-ports  
Topology: Ring

<table>
<thead>
<tr>
<th>Interface</th>
<th>Connection</th>
<th>Link Speed (Gb/s)</th>
<th>Admin Status</th>
<th>Link Status</th>
<th>Trunk Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/33</td>
<td>1/37</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>0/37</td>
<td>2/33</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>0/41</td>
<td>1/49</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>0/45</td>
<td>2/53</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/33</td>
<td>2/37</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/37</td>
<td>0/33</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/49</td>
<td>0/41</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/53</td>
<td>2/49</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/33</td>
<td>0/37</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/37</td>
<td>1/33</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/49</td>
<td>1/53</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/53</td>
<td>0/45</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
</tbody>
</table>
### Example Figure 47-4. show system stack-ports status Command Example

FTOS# show system stack-ports status
Topology: Ring

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link Speed (Gb/s)</th>
<th>Admin Status</th>
<th>Link Status</th>
<th>Trunk Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/33</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>0/37</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>0/41</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>0/45</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/33</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/37</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/49</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>1/53</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/33</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/37</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/49</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>2/53</td>
<td>40</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
</tbody>
</table>

### Example Figure 47-5. show system stack-ports topology Command Example

FTOS# show system stack-ports
topology: Ring

<table>
<thead>
<tr>
<th>Interface</th>
<th>Connection</th>
<th>Trunk Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/33</td>
<td>1/37</td>
<td></td>
</tr>
<tr>
<td>0/37</td>
<td>2/33</td>
<td></td>
</tr>
<tr>
<td>0/41</td>
<td>1/49</td>
<td></td>
</tr>
<tr>
<td>0/45</td>
<td>2/53</td>
<td></td>
</tr>
<tr>
<td>1/33</td>
<td>2/37</td>
<td></td>
</tr>
<tr>
<td>1/37</td>
<td>0/33</td>
<td></td>
</tr>
<tr>
<td>1/49</td>
<td>0/41</td>
<td></td>
</tr>
<tr>
<td>1/53</td>
<td>2/49</td>
<td></td>
</tr>
<tr>
<td>2/33</td>
<td>0/37</td>
<td></td>
</tr>
<tr>
<td>2/37</td>
<td>1/33</td>
<td></td>
</tr>
<tr>
<td>2/49</td>
<td>1/53</td>
<td></td>
</tr>
<tr>
<td>2/53</td>
<td>0/45</td>
<td></td>
</tr>
</tbody>
</table>
Table 47-1. show system stack-ports Command Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>Lists the topology of stack ports connected: Ring, Daisy chain, or Standalone</td>
</tr>
<tr>
<td>Interface</td>
<td>The unit/port ID of the connected stack port on this unit</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Link Speed of the stack port in Gb/s</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The only currently listed status is Up.</td>
</tr>
<tr>
<td>Connection</td>
<td>The stack port ID to which this unit’s stack port is connected</td>
</tr>
</tbody>
</table>

Related Commands

- redundancy
disable-auto-reboot: Resets the designated stack member.
- show hardware stack-unit: Displays the data plane or management plane input and output statistics of the designated component of the designated stack member.
- show system: Displays the current status of all stack members or a specific member.

show system stack-unit stack-group
Display the stack-groups present/configured for a MXL 10/40GbE switch stack unit.

Syntax

```
show system stack-unit <unit-number> stack-group [configured]
```

Parameters

- `unit number <0-5>`: Number of the member stack unit. Valid values: 0 to 5. Default: 0.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Related Commands

- `reload`: Reboots FTOS.
- `show system`: Displays the current status of all stack members or a specific member.

stack-unit stack group
Configure a 40GbE port for stacking mode.

Syntax

```
stack-unit <unit number> stack-group <group number>
```

Parameters

- `unit number <0-5>`: Number of the member stack unit. Valid values: 0 to 5.
- `group number <0-5>`: Number of the stacked port on the unit. Valid values: 0 to 5.

Command Modes

CONFIGURATION
stack-unit priority

Configure the ability of an MXL 10/40GbE switch to become the management unit of a stack.

**Syntax**
```
stack-unit [0-5] priority [1-14]
```

**Parameters**
- **0-5**: Enter the stack member unit identifier, from 0 to 5, of the switch on which you want to set the management priority.
- **1-14**: This preference parameter allows you to specify the management priority of one backup switch over another, with 1 the lowest priority and 14 the highest. The switch with the highest priority value will be chosen to become the management unit.

**Defaults**

0

**Command Modes**
CONFIGURATION

---

**Related Commands**

- `reload`: Reboots FTOS.
- `show system`: Displays the current status of all stack members or a specific member.

---

stack-unit provision

Pre-configure a logical stacking ID of a switch that will join the stack. This is an optional command that is executed on the management unit.

**Syntax**
```
stack-unit [0-5] provision \{MXL-10/40GbE\}
```

**Parameters**
- **0-5**: Enter a stack member identifier, from 0 to 5, of the switch that you want to add to the stack.
- **MXL-10/40GbE**: Enter the model identifier of the switch to be added as a stack member. This identifier is also referred to as the provision type.

**Command Modes**
CONFIGURATION

---

**Related Commands**

- `reload`: Reboots FTOS.
- `show system`: Displays the current status of all stack members or a specific member.
stack-unit renumber

Change the stack member ID of any stack member or a stand-alone switch.

**Syntax**

```
stack-unit 0-5 renumber 0-5
```

**Parameters**

- **0-5**
  - The first instance of this value is the stack member unit identifier, from 0 to 5, of the switch that you want to add to the stack.
  - The second instance of this value is the desired new unit identifier number.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You can renumber any switch, including the management unit or a stand-alone unit. You cannot renumber a unit to a number of an active member in the stack.

When executing this command on the Master, the stack reloads. When the members are renumbered, only that specific unit resets and comes up with the new unit number.

**Example**

Figure 47-6. stack-unit renumber Command Example

```
FTOS#stack-unit 0 renumber 2
Renumbering master unit will reload the stack. Proceed to renumber [confirm yes/no]:
```

**Related Commands**

- **reload**  Reboots FTOS.
- **redundancy disable-auto-reboot**  Resets the designated stack member.
- **show system**  Displays the current status of all stack members or a specific member.
Storm Control

Overview

The Dell Networking operating software (FTOS) storm control feature allows users to limit or suppress traffic during a traffic storm.

Commands

The storm control commands are:

- show storm-control broadcast
- show storm-control multicast
- show storm-control unknown-unicast
- storm-control broadcast (Configuration)
- storm-control broadcast (Interface)
- storm-control multicast (Configuration)
- storm-control multicast (Interface)
- storm-control unknown-unicast (Configuration)
- storm-control unknown-unicast (Interface)

Important Points to Remember

- You can only apply interface commands on physical interfaces (virtual local area networks [VLANs] and link aggregation group [LAG] interfaces are not supported).
- An INTERFACE-level command only supports storm control configuration on ingress.
- An INTERFACE-level command overrides any CONFIGURATION-level ingress command for that physical interface, if both are configured.
- Do not apply per-VLAN quality of service (QoS) on an interface that has storm control enabled (either on an interface or globally).

show storm-control broadcast

Display the storm control broadcast configuration.

Syntax

show storm-control broadcast [interface]
show storm-control broadcast

Display the storm control broadcast configuration.

Syntax

show storm-control broadcast [interface]

Parameters

interface (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration.
  • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  • For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

Defaults

none

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Figure 48-1. show storm-control broadcast Command Example

FTOS#show storm-control broadcast tengigabitethernet 3/24
Broadcast storm control configuration
Interface   Direction   Packets/Second
------------------------   --------   -----------------
TenGig 3/24      Ingress         1000

FTOS#

show storm-control multicast

Display the storm control multicast configuration.

Syntax

show storm-control multicast [interface]

Parameters

interface (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration.
  • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  • For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

Defaults

none

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
**show storm-control unknown-unicast**
Display the storm control unknown-unicast configuration

**Syntax**
```plaintext
show storm-control unknown-unicast [interface]
```

**Parameters**
- `interface` (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

**Defaults**
none

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
FTOS#show storm-control unknown-unicast tengigabitethernet 3/0
Unknown-unicast storm control configuration
Interface     Direction  Packets/Second
-----------------------------------------------
TenGig 3/0    Ingress     1000
FTOS#
```

**storm-control broadcast (Configuration)**
Configure the packets per second of broadcast traffic.

**Syntax**
```plaintext
storm-control broadcast [packets_per_second] in
```

To disable broadcast rate-limiting, use the `no storm-control broadcast [packets_per_second] in` command.
Storm Control

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>packets_per_second</strong></td>
<td>Enter the packets per second of broadcast traffic allowed from the network.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 33554368.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION (conf)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

Broadcast storm control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

### storm-control broadcast (Interface)

Configure the packets per second of broadcast traffic to be limited on the interface.

**Syntax**

```
storm-control broadcast [packets_per_second] in
```

To disable broadcast storm control on the interface, use the `no storm-control broadcast [packets_per_second] in` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>packets_per_second</strong></td>
<td>Enter the packets per second of broadcast traffic allowed from the network.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 33554368.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

INTERFACE (conf-if-interface-slot/port)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### storm-control multicast (Configuration)

Configure the packets per second (pps) of multicast traffic.

**Syntax**

```
storm-control multicast [packets_per_second] in
```

To disable storm-control for multicast traffic into the network, use the `no storm-control multicast [packets_per_second] in` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>packets_per_second</strong></td>
<td>Enter the packets per second of multicast traffic allowed from the network</td>
</tr>
<tr>
<td></td>
<td>followed by the keyword in.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 33554368.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION (conf)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Broadcast traffic (all 0xFs) should be counted against broadcast storm control meter, not against the multicast storm control meter. It is possible, however, that some multicast control traffic may get dropped when storm control thresholds are exceeded.

**storm-control multicast (Interface)**

Configure the packets per second of multicast traffic allowed on a MXL Switch interface (ingress only).

**Syntax**

```
storm-control multicast [packets_per_second] in
```

To disable multicast storm control on the interface, use the `no storm-control multicast [packets_per_second] in` command.

**Parameters**

- `packets_per_second`
  
Enter the packets per second of broadcast traffic allowed from the network.
  
  Range: 0 to 33554368

**Defaults**

none

**Command Modes**

INTERFACE (conf-if-interface-slot/port)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**storm-control unknown-unicast (Configuration)**

Configure the packets per second of unknown-unicast traffic allowed on a MXL Switch (ingress rate only).

**Syntax**

```
storm-control unknown-unicast [packets_per_second] in
```

To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast [packets_per_second] in` command.

**Parameters**

- `packets_per_second`
  
Enter the packets per second of broadcast traffic allowed from the network.
  
  Range: 0 to 33554368

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.
storm-control unknown-unicast (Interface)

Configure the packets per second of unknown-unicast traffic allowed on a MXL Switch interface (ingress only).

Syntax

```
storm-control unknown-unicast [packets_per_second] in
```

To disable unknown-unicast storm control on the interface, use the `no storm-control unknown-unicast [packets_per_second] in` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets_per_second</td>
<td>Enter the packets per second of broadcast traffic allowed from the network.</td>
</tr>
<tr>
<td>Range</td>
<td>0 to 33554368</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

INTERFACE (conf-if-interface-slot/port)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>
Spanning Tree Protocol (STP)

Overview

The commands described in this chapter configure and monitor the IEEE 802.1d spanning tree protocol (STP). The STP commands are:

- bridge-priority
- debug spanning-tree
- description
- disable
- forward-delay
- hello-time
- max-age
- portfast bpdufilter default
- protocol spanning-tree
- show config
- show spanning-tree 0
- spanning-tree 0

bridge-priority

Set the bridge priority of the switch in an IEEE 802.1D Spanning Tree.

Syntax

```
bridge-priority {priority-value | primary | secondary}
```

To return to the default value, use the no bridge-priority command.

Parameters

- **priority-value**
  - Enter a number as the bridge priority value.
  - Range: 0 to 65535.
  - Default: 32768.
- **primary**
  - Enter the keyword primary to designate the bridge as the root bridge.
- **secondary**
  - Enter the keyword secondary to designate the bridge as a secondary root bridge.

Defaults

```
priority-value = 32768
```

Command Modes

```
SPANNING TREE (The prompt is “conf-stp”.)
```
### debug spanning-tree

Enable debugging of the spanning tree protocol and view information on the protocol.

**Syntax**

```
d debug spanning-tree {stp-id [all | bpdu | events | exceptions] | protocol}
```

To disable debugging, use the `no debug spanning-tree` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>stp-id</strong></td>
<td>Enter zero (0). The switch supports one Spanning Tree group with a group ID of 0.</td>
</tr>
<tr>
<td><strong>protocol</strong></td>
<td>Enter the keyword for the type of STP to debug, either <code>mstp</code>, <code>pvst</code>, or <code>rstp</code>.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>(OPTIONAL) Enter the keyword <code>all</code> to debug all spanning tree operations.</td>
</tr>
<tr>
<td><strong>bpdu</strong></td>
<td>(OPTIONAL) Enter the keyword <code>bpdu</code> to debug Bridge Protocol Data Units.</td>
</tr>
<tr>
<td><strong>events</strong></td>
<td>(OPTIONAL) Enter the keyword <code>events</code> to debug STP events.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

When you enable `debug spanning-tree bpdu` for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

**Related Commands**

- `description` - Enter a description of the spanning tree.
- `portfast bpdudfilter default` - Enters SPANNING TREE mode on the switch.

### description

Enter a description of the spanning tree.

**Syntax**

```
d description {description}
```

To remove the description from the Spanning Tree, use the `no description {description}` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>description</strong></td>
<td>Enter a description to identify the Spanning Tree (80 characters maximum).</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

SPANNING TREE (The prompt is “conf-stp”.)

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `portfast bpdudfilter default` - Enters SPANNING TREE mode on the switch.
**disable**

Disable the spanning tree protocol globally on the switch.

**Syntax**

```
disable
```

To enable STP, use the `no disable` command.

**Defaults**

Enabled (that is, the spanning tree protocol is disabled.)

**Command Modes**

SPANNING TREE

---

**forward-delay**

The amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

**Syntax**

```
forward-delay seconds
```

To return to the default setting, use the `no forward-delay` command.

**Parameters**

- `seconds`
  - Enter the number of seconds the FTOS waits before transitioning STP to the forwarding state.
  - Range: 4 to 30
  - Default: 15 seconds.

**Defaults**

15 seconds

**Command Modes**

SPANNING TREE

---

**hello-time**

Set the time interval between generation of the spanning tree bridge protocol data units (BPDUs).

**Syntax**

```
hello-time seconds
```

To return to the default value, use the `no hello-time` command.

---

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `max-age`
  - Changes the wait time before STP refreshes protocol configuration information.
- `hello-time`
  - Changes the time interval between BPDUs.
max-age

Set the time interval for the spanning tree bridge to maintain configuration information before refreshing that information.

**Syntax**
```
max-age seconds
```

To return to the default values, use the `no max-age` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Enter a number of seconds the FTOS waits before refreshing configuration information. Range: 6 to 40. Default: 20 seconds.</td>
</tr>
</tbody>
</table>

**Defaults**

20 seconds

**Command Modes**

SPANNING TREE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- **forward-delay** Changes the wait time before STP transitions to the Forwarding state.
- **max-age** Changes the wait time before STP refreshes protocol configuration information.

portfast bpdufilter default

Enable BPDU Filter globally to filter transmission of BPDUs on port fast enabled interfaces.

**Syntax**
```
portfast bpdufilter default
```

To disable BPDU Filter default, use the `no edge-port bpdufilter default` command.

**Defaults**

Disabled

**Command Modes**

SPANNING TREE
protocol spanning-tree

Enter SPANNING TREE mode to enable and configure the spanning tree group.

Syntax

```
protocol spanning-tree stp-id
```

To disable the Spanning Tree group, use the `no protocol spanning-tree stp-id` command.

Parameters

```
stp-id
```

- Enter zero (0). FTOS supports one Spanning Tree group, group 0.

Defaults

Not configured.

Command Modes

```
CONFIGURATION
```

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```
Figure 49-1.  protocol spanning-tree Command Example

FTOS(conf)#protocol spanning-tree 0
FTOS(conf-stp)#
```

Usage Information

STP is not enabled when you enter SPANNING TREE mode. To enable STP globally on the switch, use the `no disable` command from SPANNING TREE mode.

Related Commands

- `disable` Disables spanning tree group 0. To enable spanning tree group 0, use the `no disable` command.

show config

Display the current configuration for the mode. Only non-default values are displayed.

Syntax

```
show config
```

Command Modes

```
SPANNING TREE
```

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```
Figure 49-2.  show config Command Example

FTOS(conf-stp)#show config
protocol spanning-tree 0
no disable
FTOS(conf-stp)#
```
show spanning-tree 0

Display the spanning tree group configuration and status of interfaces in the spanning tree group.

Syntax

show spanning-tree 0 [active | brief | guard | interface interface | root | summary]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Enter 0 (zero) to display information about that specific Spanning Tree group.</td>
</tr>
<tr>
<td>active</td>
<td>(OPTIONAL) Enter the keyword active to display only active interfaces in Spanning Tree group 0.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to display a synopsis of the Spanning Tree group configuration information.</td>
</tr>
<tr>
<td>guard</td>
<td>(OPTIONAL) Enter the keyword guard to display the type of guard enabled on an STP interface and the current port state.</td>
</tr>
<tr>
<td>interface</td>
<td>(OPTIONAL) Enter the keyword interface and the type slot/port of the interface you want displayed. Type slot/port options are the following:</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number:</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
<tr>
<td>root</td>
<td>(OPTIONAL) Enter the keyword root to display configuration information on the Spanning Tree group root.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword summary to only the number of ports in the Spanning Tree group and their state.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Usage Information

You must enable spanning tree group 0 prior to using this command.

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example

Figure 49-3. show spanning-tree 0 Command Example

FTOS#show spanning-tree 0
Executing IEEE compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, Address 0001.e800.0a56
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally
We are the root of the spanning tree
Current root has priority 32768 address 0001.e800.0a56
Topology change flag set, detected flag set
Number of topology changes 1 last change occurred 0:00:05 ago
from Tengigabitethernet 1/3
Timers: hold 1, topology change 35
hello 2, max age 20, forward delay 15
Times: hello 1, topology change 1, notification 0, aging 2

Port 26 (Tengigabitethernet 1/1) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.26
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.26, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 27 (Tengigabitethernet 1/2) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.27
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.27, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 28 (Tengigabitethernet 1/3) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.28
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.28, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:31, received 0
The port is not in the portfast mode

FTOS#

Table 49-1. show spanning-tree 0 Command Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Bridge Identifier...”</td>
<td>Lists the bridge priority and the MAC address for this STP bridge.</td>
</tr>
<tr>
<td>“Configured hello...”</td>
<td>Displays the settings for hello time, max age, and forward delay.</td>
</tr>
<tr>
<td>“Bpdu filter...”</td>
<td>States whether BPDU Filter is enabled/disabled globally.</td>
</tr>
<tr>
<td>“We are...”</td>
<td>States whether this bridge is the root bridge for the STG.</td>
</tr>
<tr>
<td>“Current root...”</td>
<td>Lists the bridge priority and MAC address for the root bridge.</td>
</tr>
<tr>
<td>“Topology flag...”</td>
<td>States whether the topology flag and the detected flag were set.</td>
</tr>
<tr>
<td>“Number of...”</td>
<td>Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.</td>
</tr>
<tr>
<td>“Timers”</td>
<td>Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.</td>
</tr>
</tbody>
</table>
Table 49-1. show spanning-tree 0 Command Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Times”</td>
<td>List the number of seconds since the last:</td>
</tr>
<tr>
<td></td>
<td>• hello time</td>
</tr>
<tr>
<td></td>
<td>• topology change</td>
</tr>
<tr>
<td></td>
<td>• notification</td>
</tr>
<tr>
<td></td>
<td>• aging</td>
</tr>
<tr>
<td>“Port 1...”</td>
<td>Displays the Interface type slot/port information and the status of the</td>
</tr>
<tr>
<td></td>
<td>interface (Disabled or Enabled).</td>
</tr>
<tr>
<td>“Port path...”</td>
<td>Displays the path cost, priority, and identifier for the interface.</td>
</tr>
<tr>
<td>“Designated root...”</td>
<td>Displays the priority and MAC address of the root bridge of</td>
</tr>
<tr>
<td></td>
<td>the STG that the interface belongs.</td>
</tr>
<tr>
<td>“Designated port...”</td>
<td>Displays the designated port ID</td>
</tr>
</tbody>
</table>

Figure 49-4. show spanning-tree 0 brief Command Example

```
FTOS#show span 0 brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768
Address 0001.e800.0a56
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768,
Address 0001.e800.0a56
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts</th>
<th>Cost</th>
<th>Bridge ID</th>
<th>PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tengig 1/1</td>
<td>8.26</td>
<td>8</td>
<td>4</td>
<td>FWD</td>
<td>0</td>
<td>32768 0001.e800.0a56</td>
<td>8.26</td>
</tr>
<tr>
<td>Tengig 1/2</td>
<td>8.27</td>
<td>8</td>
<td>4</td>
<td>FWD</td>
<td>0</td>
<td>32768 0001.e800.0a56</td>
<td>8.27</td>
</tr>
<tr>
<td>Tengig 1/3</td>
<td>8.28</td>
<td>8</td>
<td>4</td>
<td>FWD</td>
<td>0</td>
<td>32768 0001.e800.0a56</td>
<td>8.28</td>
</tr>
</tbody>
</table>
```

Figure 49-5. show spanning-tree 0 guard Command Example

```
FTOS#show spanning-tree 0 guard

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Instance</th>
<th>Sts</th>
<th>Guard type</th>
<th>Bpdu Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tengig 0/1</td>
<td>0</td>
<td>INCON(Root)</td>
<td>Rootguard</td>
<td>No</td>
</tr>
<tr>
<td>Tengig 0/2</td>
<td>0</td>
<td>LIS</td>
<td>Loopguard</td>
<td>No</td>
</tr>
<tr>
<td>Tengig 0/3</td>
<td>0</td>
<td>EDS (Shut)</td>
<td>Bpduguard</td>
<td>No</td>
</tr>
</tbody>
</table>
```

Table 49-2. show spanning-tree 0 guard Command Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>STP interface</td>
</tr>
<tr>
<td>Instance</td>
<td>STP 0 instance</td>
</tr>
<tr>
<td>Sts</td>
<td>Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut)</td>
</tr>
</tbody>
</table>
spanning-tree 0

Assigns a Layer 2 interface to STP instance 0 and configures a port cost or port priority, or enables loop guard, root guard, or the Portfast feature on the interface.

**Syntax**

```
spanning-tree stp-id {cost cost | {rootguard} | portfast [bpduguard [shutdown-on-violation] | bpdufilter] | priority priority}
```

To disable the spanning tree group on an interface, use the `no spanning-tree stp-id {cost cost | {rootguard} | portfast [bpduguard [shutdown-on-violation] | bpdufilter] | priority priority}` command.

**Parameters**

- **stp-id**
  Enter the STP instance ID. Range: 0

- **cost**
  Enter the keyword `cost` followed by a number as the cost.
  Range: 1 to 65535

  Defaults:
  - 40-Gigabit Ethernet interface = 1
  - 10-Gigabit Ethernet interface = 2
  - Port Channel interface with 40-Gigabit Ethernet = 1
  - Port Channel interface with 10-Gigabit Ethernet = 1

- **rootguard**
  Enter the keyword `rootguard` to enable STP root guard on a port or port-channel interface.

- **portfast [bpduguard [shutdown-on-violation] | bpdufilter]**
  Enter the keyword `portfast` to enable Portfast to move the interface into forwarding mode immediately after the root fails.

  Enter the optional keyword `bpduguard` to disable the port when it receives a BPDU.

  Enter the optional keyword `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

  Enter the keyword `bpdufilter` to enable on an interface; it should stop sending and receiving BPDUs on the port fast enabled ports.

- **priority**
  Enter keyword `priority` followed by a number as the priority.
  Range: zero (0) to 15

  Default: 8

**Defaults**

- `cost` = depends on the interface type; `priority` = 8

**Command Modes**

INTERFACE

**Command History**

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

**Usage Information**

If you enable `portfast bpduguard` on an interface and the interface receives a BPDU, the software disables the interface and sends a message stating that fact. The port is in ERR_DISABLE mode, yet appears in the `show interface` commands as enabled. If you do not enable the `shutdown-on-violation` command, BPDUs are still sent to the CPU.
STP root guard is supported on a port or port-channel enabled in any Spanning Tree mode: Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Per-VLAN Spanning Tree Plus (PVST+).

Root guard is supported on any STP-enabled port or port-channel except when used as a stacking port. When enabled on a port, root guard applies to all VLANs configured on the port.
System Time and Date

Overview

The commands in this chapter configure time values on the system, either using the Dell Networking operating software (FTOS), the hardware, or using the network time protocol (NTP). With NTP, the switch can act only as a client to an NTP clock host. For more information, refer to the “Network Time Protocol” section of the Management chapter in the FTOS Configuration Guide.

Commands

The NTP commands are:

- calendar set
- clock read-calendar
- clock set
- clock summer-time date
- clock summer-time recurring
- clock timezone
- clock update-calendar
- debug ntp
- ntp authenticate
- ntp authentication-key
- ntp broadcast client
- ntp disable
- ntp multicast client
- ntp server
- ntp source
- ntp trusted-key
- ntp update-calendar
- show calendar
- show clock
- show ntp associations
- show ntp status
calendar set

Set the time and date for the switch hardware clock.

Syntax

```
calendar set time month day year
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, for example, 17:15:00 is 5:15 pm.</td>
</tr>
<tr>
<td>month</td>
<td>Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to <em>time day month year</em>.</td>
</tr>
<tr>
<td>day</td>
<td>Enter the number of the day. Range: 1 to 31. You can enter the name of a month to change the order of the display to <em>time day month year</em>.</td>
</tr>
<tr>
<td>year</td>
<td>Enter a four-digit number as the year. Range: 1993 to 2035.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

```
Figure 50-1. calendar set Command Example

FTOS#calendar set 12:11:00 21 may 2012
FTOS#
```

Usage Information

You can change the order of the *month* and *day* parameters to enter the time and date as *time day month year*.

In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the FTOS automatically updates the software clock after system bootup. You cannot delete the hardware clock (calendar).

To manually update the software with the hardware clock, use the command *clock read-calendar*.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock read-calendar</td>
<td>Sets the software clock based on the hardware clock.</td>
</tr>
<tr>
<td>clock set</td>
<td>Sets the software clock.</td>
</tr>
<tr>
<td>clock update-calendar</td>
<td>Sets the hardware clock based on the software clock.</td>
</tr>
<tr>
<td>show clock</td>
<td>Displays the clock settings.</td>
</tr>
</tbody>
</table>

clock read-calendar

Set the software clock on the switch from the information set in hardware clock (calendar).

Syntax

```
clock read-calendar
```

Defaults

Not configured.
In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the FTOS automatically updates the software clock after system bootup.

You cannot delete this command (that is, there is not a “no” version of this command).

**clock set**

Set the software clock in the switch.

**Syntax**

```
clock set time month day year
```

**Parameters**

- **time**
  - Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.

- **month**
  - Enter the name of one of the 12 months, in English.
  - You can enter the number of a day and change the order of the display to `time day month year`.

- **day**
  - Enter the number of the day.
  - Range: 1 to 31.
  - You can enter the name of a month to change the order of the display to `time month day year`.

- **year**
  - Enter a four-digit number as the year.
  - Range: 1993 to 2035.

**Defaults**

Not configured

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**Usage Information**

- You can change the order of the `month` and `day` parameters to enter the time and date as `time day month year`. You cannot delete the software clock.

- The software clock runs only when the software is up. The clock restarts, based on the hardware clock, when the switch reboots.

- Dell Networking recommends using an outside time source, such as NTP, to ensure accurate time on the switch.

**Related Commands**

- `ntp update-calendar` — Sets the switch using the NTP settings.
clock summer-time date

Set a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

**Syntax**

```plaintext
clock summer-time time-zone date start-month start-day start-year start-time end-month end-day end-year end-time [offset]
```

To delete a daylight saving time zone configuration, use the no clock summer-time command.

**Parameters**

- **time-zone**
  - Enter the three-letter name for the time zone. This name is displayed in the `show clock` output.
- **start-month**
  - Enter the name of one of the 12 months in English.
  - You can enter the name of a day to change the order of the display to `time day month year`.
- **start-day**
  - Enter the number of the day.
  - Range: 1 to 31.
  - You can enter the name of a month to change the order of the display to `time day month year`.
- **start-year**
  - Enter a four-digit number as the year.
  - Range: 1993 to 2035.
- **start-time**
  - Enter the time in hours:minutes. For the hour variable, use the 24-hour format, example, 17:15 is 5:15 pm.
- **end-day**
  - Enter the number of the day.
  - Range: 1 to 31.
  - You can enter the name of a month to change the order of the display to `time day month year`.
- **end-month**
  - Enter the name of one of the 12 months in English.
  - You can enter the name of a day to change the order of the display to `time day month year`.
- **end-time**
  - Enter the time in hours:minutes. For the hour variable, use the 24-hour format, example, 17:15 is 5:15 pm.
- **end-year**
  - Enter a four-digit number as the year.
  - Range: 1993 to 2035.
- **offset**
  - (OPTIONAL) Enter the number of minutes to add during the summer-time period.
  - Range: 1 to 1440.
  - Default: 60 minutes

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- `calendar set` Sets the hardware clock.
- `clock summer-time recurring` Sets a date (and time zone) on which to convert the switch to daylight saving time each year.
- `show clock` Displays the current clock settings.
clock summer-time recurring

Set the software clock to convert to daylight saving time on a specific day each year.

**Syntax**

```
clock summer-time time-zone recurring [start-week start-day start-month start-time end-week end-month end-time [offset]]
```

To delete a daylight saving time zone configuration, use the no clock summer-time command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>time-zone</code></td>
<td>Enter the three-letter name for the time zone. This name is displayed in the <code>show clock</code> output. You can enter up to eight characters.</td>
</tr>
</tbody>
</table>
| `start-week` | (OPTIONAL) Enter one of the following as the week that daylight saving begins and then enter values for `start-day` through `end-time`:  
  - `week-number`: Enter a number from 1-4 as the number of the week in the month to start daylight saving time.  
  - `first`: Enter this keyword to start daylight saving time in the first week of the month.  
  - `last`: Enter this keyword to start daylight saving time in the last week of the month. |
| `start-day` | Enter the name of the day that you want daylight saving time to begin. Use English three letter abbreviations, for example, Sun, Sat, Mon etc.  
Range: Sun – Sat |
| `start-month` | Enter the name of one of the 12 months in English. |
| `start-time` | Enter the time in hours:minutes. For the hour variable, use the 24-hour format, example, 17:15 is 5:15 pm. |
| `end-week` | Enter the one of the following as the week that daylight saving ends:  
  - `week-number`: enter a number from 1-4 as the number of the week to end daylight saving time.  
  - `first`: enter the keyword first to end daylight saving time in the first week of the month.  
  - `last`: enter the keyword last to end daylight saving time in the last week of the month. |
| `end-day` | Enter the weekday name that you want daylight saving time to end. Enter the weekdays using the three letter abbreviations, for example Sun, Sat, Mon etc.  
Range: Sun to Sat |
| `end-month` | Enter the name of one of the 12 months in English. |
| `end-time` | Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm. |
| `offset` | (OPTIONAL) Enter the number of minutes to add during the summer-time period.  
Range: 1 to 1440.  
Default: 60 minutes. |

**Defaults**

Not configured.

**Command Modes**

`CONFIGURATION`

**Command History**

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>calendar set</code></td>
<td>Sets the hardware clock.</td>
</tr>
<tr>
<td><code>clock summer-time date</code></td>
<td>Sets a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.</td>
</tr>
<tr>
<td><code>show clock</code></td>
<td>Displays the current clock settings.</td>
</tr>
</tbody>
</table>
clock timezone

Configure a timezone for the switch.

Syntax

```
clock timezone timezone-name offset
```

To delete a timezone configuration, use the no clock timezone command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timezone-name</td>
<td>Enter the name of the timezone. You cannot use spaces.</td>
</tr>
</tbody>
</table>
| offset | Enter one of the following:  
  - a number from 1 to 23 as the number of hours in addition to UTC for the timezone.  
  - a minus sign (-) followed by a number from 1 to 23 as the number of hours |

Default

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Coordinated universal time (UTC) is the time standard based on the International Atomic Time standard, commonly known as Greenwich Mean time. When determining system time, you must include the differentiator between UTC and your local timezone. For example, San Jose, CA is the Pacific Timezone with a UTC offset of -8.

clock update-calendar

Set the switch hardware clock based on the software clock.

Syntax

```
clock update-calendar
```

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Use this command only if you are sure that the hardware clock is inaccurate and the software clock is correct.

You cannot delete this command (that is, there is not a “no” form of this command).

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>calendar set</td>
<td>Sets the hardware clock.</td>
</tr>
</tbody>
</table>
debug ntp

Display NTP transactions and protocol messages for troubleshooting.

Syntax

debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}

To disable debugging of NTP transactions, use the no debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjust</td>
<td>Enter the keyword adjust to display information on NTP clock adjustments.</td>
</tr>
<tr>
<td>all</td>
<td>Enter the keyword all to display information on all NTP transactions.</td>
</tr>
<tr>
<td>authentication</td>
<td>Enter the keyword authentication to display information on NTP authentication transactions.</td>
</tr>
<tr>
<td>events</td>
<td>Enter the keyword events to display information on NTP events.</td>
</tr>
<tr>
<td>loopfilter</td>
<td>Enter the keyword loopfilter to display information on NTP local clock frequency.</td>
</tr>
<tr>
<td>packets</td>
<td>Enter the keyword packets to display information on NTP packets.</td>
</tr>
<tr>
<td>select</td>
<td>Enter the keyword select to display information on the NTP clock selection.</td>
</tr>
<tr>
<td>sync</td>
<td>Enter the keyword sync to display information on the NTP clock synchronization.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

ntp authenticate

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

Syntax

ntp authenticate

To disable NTP authentication, use the no ntp authentication command.

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

You also must configure an authentication key for NTP traffic using the ntp authentication-key command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp authentication-key</td>
<td>Configures the authentication key for NTP traffic.</td>
</tr>
<tr>
<td>ntp trusted-key</td>
<td>Configures a key to authenticate.</td>
</tr>
</tbody>
</table>
ntp authentication-key

Specify a key for authenticating the NTP server.

Syntax

```
ntp authentication-key number md5 [0 | 7] key
```

Parameters

- **number**: Specify a number for the authentication key.
  - Range: 1 to 4294967295.
  - This number must be the same as the number parameter configured in the `ntp trusted-key` command.
- **md5**: Specify that the authentication key will be encrypted using MD5 encryption algorithm.
- **0**: Specify that authentication key will be entered in an unencrypted format (default).
- **7**: Specify that the authentication key will be entered in DES encrypted format.
- **key**: Enter the authentication key in the previously specified format.

Defaults

NTP authentication is not configured by default. If you do not specify the option [0 | 7], 0 is selected by default.

Command Modes

```
CONFIGURATION
```

Command History

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```

Usage Information

After configuring the `ntp authentication-key` command, to complete NTP authentication, configure the `ntp trusted-key` command.

FTOS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous FTOS versions; beginning in version 8.2.1.0, FTOS uses DES encryption to store the key in the startup-config when you enter the command `ntp authentication-key`. Therefore, if your system boots with a startup-configuration from an FTOS versions prior to 8.2.1.0 in which you have configured `ntp authentication-key`, the system cannot correctly decrypt the key, and cannot authenticate NTP packets. In this case you must re-enter this command and save the running-config to the startup-config.

Related Commands

```
ntp authenticate       Enables NTP authentication.
ntp trusted-key       Configures a trusted key.
```

ntp broadcast client

Set up the interface to receive NTP broadcasts from an NTP server.

Syntax

```
ntp broadcast client
```

To disable broadcast, use the no ntp broadcast client command.

Defaults

```
Disabled
```

Command Modes

```
INTERFACE
```

Command History

```
Version 8.3.16.1   Introduced on MXL 10/40GbE Switch IO Module
```
ntp disable

Prevent an interface from receiving NTP packets.

**Syntax**

```plaintext
ntp disable
```

To re-enable NTP on an interface, use the `no ntp disable` command.

**Default**

Disabled (that is, if an NTP host is configured, all interfaces receive NTP packets)

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**ntp multicast client**

Configure the switch to receive NTP information from the network via multicast.

**Syntax**

```plaintext
ntp multicast client [multicast-address]
```

To disable multicast reception, use the `no ntp multicast client [multicast-address]` command.

**Parameters**

- `multicast-address` (OPTIONAL) Enter a multicast address. Enter an IPv4 address in dotted decimal format. If you do not enter a multicast address, the address 224.0.1.1 is configured if the interface address is IPv4.

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**ntp server**

Configure an NTP time-serving host.

**Syntax**

```plaintext
ntp server {hostname | ipv4-address} [key keyid] [prefer] [version number]
```

**Parameters**

- `ipv4-address` Enter an IPv4 address (A.B.C.D).
- `hostname` Enter the hostname of the server.
- `key keyid` (OPTIONAL) Enter the keyword `key` and a number as the NTP peer key. Range: 1 to 4294967295
- `prefer` (OPTIONAL) Enter the keyword `prefer` to indicate that this peer has priority over other servers.
- `version number` (OPTIONAL) Enter the keyword `version` and a number to correspond to the NTP version used on the server. Range: 1 to 3

**Defaults**

Not configured.
You can configure multiple time serving hosts (up to 250). From these time serving hosts, the FTOS chooses one NTP host with which to synchronize. To determine which server was selected, use the `show ntp associations`.

Because a large number of polls to NTP hosts can impact network performance, Dell Networking recommends limiting the number of hosts configured.

You can configure multiple time serving hosts (up to 250). From these time serving hosts, the FTOS chooses one NTP host with which to synchronize. To determine which server was selected, use the `show ntp associations`.

Because a large number of polls to NTP hosts can impact network performance, Dell Networking recommends limiting the number of hosts configured.

### ntp source

Specify an interface’s IP address to be included in the NTP packets.

#### Syntax

```
ntp source interface
```

To delete the configuration, use the `no ntp source` command.

#### Parameters

- **interface**
  
  Enter the following keywords and slot/port or number information:
  
  - For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16383.
  
  - For a Port Channel interface, enter the keyword `lag` followed by a number:
    
    Range: 1-128
  
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  
  - For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

#### Defaults

Not configured.

### ntp trusted-key

Set a key to authenticate the system to which NTP will synchronize.

#### Syntax

```
ntp trusted-key number
```

To delete the key, use the `no ntp trusted-key number` command.

#### Parameters

- **number**
  
  Enter a number as the trusted key ID.
  
  Range: 1 to 4294967295.
The `number` parameter in the `ntp trusted-key` command must be the same number as the `number` parameter in the `ntp authentication-key` command. If you change the `ntp authentication-key` command, you must also change the `ntp trusted-key` command.

### ntp update-calendar

Configure the FTOS to update the calendar (the hardware clock) with the NTP-derived time.

**Syntax**

```
ntp update-calendar [minutes]
```

To return to default setting, use the `no ntp update-calendar` command.

**Parameters**

- `minutes`
  
  (OPTIONAL) Enter the number of minutes between updates from NTP to the hardware clock.
  
  Range: 1 to 1440.
  
  Default: 60 minutes.

**Defaults**

Not enabled.

**Command Modes**

- CONFIGURATION

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### show calendar

Display the current date and time based on the switch hardware clock.

**Syntax**

```
show calendar
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
show clock

Display the current clock settings.

Syntax

show clock [detail]

Parameters

detail (OPTIONAL) Enter the keyword detail to view the source information of the clock.

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 50-4. show clock Command Example

FTOS#show clock
12:30:04.402 pacific Tue May 22 2012
FTOS#

Figure 50-5. show clock detail Command Example

FTOS#show clock detail
12:30:26.892 pacific Tue May 22 2012
Time source is RTC hardware
Summer time starts 00:00:00 UTC Wed Mar 14 2012
Summer time ends 00:00:00 pacific Wed Nov 7 2012
FTOS#

clock summer-time recurring

Displays the time and date from the switch hardware clock.

show calendar

Displays the time and date from the switch hardware clock.

show ntp associations

Display the NTP master and peers.

Syntax

show ntp associations

Command Modes

EXEC
EXEC Privilege
**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 50-6.  show ntp associations Command Example**

```
FTOS#show ntp associations
remote ref clock st when poll reach delay offset disp
10.10.120.5 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16 377 -0.08 -1499.9 104.16
172.31.1.33 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
192.200.0.2 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
* master (synced), # master (unsynced), + selected, - candidate
FTOS#
```

**Table 50-1.  show ntp associations Command Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| (none)  | One or more of the following symbols could be displayed:  
  • * means synchronized to this peer  
  • # means almost synchronized to this peer  
  • + means the peer was selected for possible synchronization  
  • - means the peer is a candidate for selection  
  • ~ means the peer is statically configured |
| remote  | Displays the remote IP address of the NTP peer. |
| ref clock | Displays the IP address of the remote peer’s reference clock. |
| st      | Displays the peer’s stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source. |
| when    | Displays the last time the switch received an NTP packet. |
| poll    | Displays the polling interval (in seconds). |
| reach   | Displays the reachability to the peer (in octal bitstream). |
| delay   | Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds). |
| offset  | Displays the relative time of the NTP peer’s clock to the switch clock (in milliseconds). |
| disp    | Displays the dispersion. |

**Related Commands**

- `show ntp status` Displays current NTP status.

**show ntp status**

Display the current NTP status.

**Syntax**

`show ntp status`

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example

**Figure 50-7. show ntp status Command Example**

```
FTOS#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
frequency is 0.000 ppm, stability is 0.000 ppm, precision is 4294967279
reference time is 00000000.00000000 (6:28:16.000 UTC Thu Feb 7 2036)
clock offset is 0.000000 msec, root delay is 0.00000 sec
root dispersion is 0.000 sec, peer dispersion is 0.000 msec
peer mode is unspec
FTOS#
```

**Table 50-2. show ntp status Command Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Clock is...”</td>
<td>States whether or not the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.</td>
</tr>
<tr>
<td>“frequency is...”</td>
<td>Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.</td>
</tr>
<tr>
<td>“reference time is...”</td>
<td>Displays the reference time stamp.</td>
</tr>
<tr>
<td>“clock offset is...”</td>
<td>Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.</td>
</tr>
<tr>
<td>“root dispersion is...”</td>
<td>Displays the root and path dispersion.</td>
</tr>
<tr>
<td>“peer mode is...”</td>
<td>State what NTP mode the switch is. This should be client mode.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show ntp associations`: Displays information on the NTP Master and Peer configurations.
Tunneling Commands

The following commands have been added to support tunneling:

- tunnel destination
- tunnel dscp
- tunnel flow-label
- tunnel hop-limit
- tunnel mode
- tunnel source

**tunnel destination**

Set a destination endpoint for the tunnel.

**Syntax**

```
tunnel destination \{ip-address | ipv6-address\}
```

To delete a tunnel destination address, use the **no tunnel destination \{ip-address | ipv6-address\}** command.

**Parameters**

- **ip-address**
  
Enter the destination IPv4 address for the tunnel.

- **ipv6-address**
  
Enter the destination IPv6 address for the tunnel.

**Defaults**

none

**Command Modes**

INTERFACE TUNNEL (conf-if-tu)

**Command History**

- **Version 9.2(0.0)**
  
  Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

- The tunnel interface is inoperable without a valid reachable tunnel destination address of the appropriate address type for the configured tunnel mode.
- Use the destination address to establish a logical tunnel to the particular destination address by using a destination address of the outer tunnel header. If you configure a tunnel interface or source address, the tunnel destination must be compatible for this command to function.
tunnel dscp

Configure the method to set the DSCP in the outer tunnel header.

Syntax

```
tunnel dscp \{mapped | <value>\}
```

To use the default tunnel mapping behavior, use the `no tunnel dscp value` command.

Parameters

- **mapped**: Enter the keyword `mapped` to map original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.
- **value**: Enter a value to set the DSCP value in the tunnel header. The range is from 0 to 63. The default value of 0 denotes mapping of original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

Defaults

0 (Mapped)

Command Modes

```
INTERFACE TUNNEL (conf-if-tu)
```

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- This command configures the method used to set the high 6 bits (the differentiated services codepoint) of the IPv4 TOS or the IPv6 traffic class in the outer IP header.
- A value of 0 copies original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

---

tunnel flow-label

Configure the method to set the IPv6 flow label value in the outer tunnel header.

Syntax

```
tunnel flow-label \value\n```

To return to the default value of 0, use the `no tunnel flow-label value` command.

Parameters

- **value**: Enter a value to set the IPv6 flow label value in the tunnel header. The range is from 0 to 1048575. The default value is 0.

Defaults

0 (Mapped original packet flow-label value to tunnel header flow-label value)

Command Mode

```
INTERFACE TUNNEL (conf-if-tu)
```

Command History

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**Usage Information**
This command is only valid for tunnel interfaces with an IPv6 outer header.

---

### tunnel hop-limit

Configure the method to set the IPv4 time-to-live or the IPv6 hop limit value in the outer tunnel header.

**Syntax**
`tunnel hop-limit value`

To restore the default tunnel hop-limit, use the `no tunnel hop-limit` command.

**Parameters**
- **value**
  - Enter the hop limit (ipv6) or time-to-live (ipv4) to include in the tunnel header. The range is from 0 to 255. The default is 64.

**Defaults**
- 64 (Time-to-live for IPv4 outer tunnel header or hop limit for IPv6 outer tunnel header)

**Command Modes**
- INTERFACE TUNNEL (conf-if-tu)

**Command History**
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**
A value of 0 copies the inner packet hop limit (ipv6) or time-to-live (ipv4) in the encapsulated packet to the tunnel header hop limit (ipv6) or time-to-live (ipv4) value.

---

### tunnel mode

Enable a tunnel interface.

**Syntax**
`tunnel mode {ipip | ipv6 | ipv6ip}`

To disable an active tunnel interface, use the `no tunnel mode` command.

**Parameters**
- **ipip**
  - Enable tunnel in RFC 2003 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv4 tunnel.

- **ipv6**
  - Enable tunnel in RFC 2473 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv6 tunnel.

- **ipv6ip**
  - Enable tunnel in RFC 4213 mode and encapsulate IPv6 datagrams inside an IPv4 tunnel.

**Defaults**
- none

**Command Modes**
- INTERFACE TUNNEL (conf-if-tu)

**Command History**
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**
This command is required to enable a tunnel interface. You must define a tunnel mode for the tunnel to function. If you previously defined the tunnel destination or source address, the tunnel mode must be compatible for this command to function.
tunnel source

Set a source address for the tunnel.

**Syntax**

```
tunnel source {ip-address | ipv6-address | interface-type-number}
```

To delete the current tunnel source address, use the `no tunnel source` command.

**Parameters**

- **ip-address**
  - Enter the source IPv4 address in A.B.C.D format.

- **ipv6-address**
  - Enter the source IPv6 address in X::X::X::X format.

- **interface-type-number**
  - For a 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 1–Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel` then a number from 1 to 128.
  - For a 10–Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

```
none
```

**Command Modes**

```
INTERFACE TUNNEL (conf-if-tu)
```

**Command History**

```
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
```

**Usage Information**

- If you configure a tunnel interface or destination address, the tunnel source must be compatible for this command to function.
- If you configure a tunnel source address as an interface, the tunnel does not function until the compatible address is present on the particular interface.
u-Boot

Overview

All commands in this chapter are in u-Boot mode. These commands are supported on the Dell Networking MXL 10/40GbE Switch Module platform only.

To access this mode, press any key when the following line appears on the console during a system boot:

Hit any key to stop autoboot:

Enter u-Boot immediately, as indicated by the BOOT_USER# prompt.

⚠️ **Note:** This chapter describes only a few commands available in uBoot mode.

Commands

- boot change
- boot selection
- boot show net config retries
- boot write net config retries
- boot zero
- default gateway
- enable
- help
- ignore enable password
- ignore startup config
- interface management ethernet ip address
- no default-gateway
- no interface management ethernet ip address
- reload
- show boot blc
- show boot selection
- show bootflash
- show bootvar
- show default-gateway
- show interface management Ethernet
- show interface management port config
• syntax help

Note: You cannot use the Tab key to complete commands in this mode.

### boot change
Change the operating system boot parameters.

**Syntax**
```plaintext
boot change [primary | secondary | default]
```

**Command Modes**
- uBoot

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### boot selection
Change the ROM bootstrap bootflash partition.

**Syntax**
```plaintext
boot selection [a | b]
```

**Command Modes**
- uBoot

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### boot show net config retries
Show the number of retries for network boot configuration failure.

**Syntax**
```plaintext
boot show net config retries
```

**Command Modes**
- uBoot

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

**Figure 52-1. boot show net config retries Command Example**

```plaintext
BOOT_USER# boot show net config retries
Number of Network Boot Config Retries is : 0
BOOT_USER #
```
**boot write net config retries**

Set the number of retries for network boot configuration failure.

**Syntax**

```
boot write net config retries <int>
```

**Command Modes**
uBoot

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Example**

Figure 52-2. boot write net config retries Command Example

```
BOOT_USER # boot write net config retries 2
Updated number of Network Boot Config retries to 2.
BOOT_USER #
```

**boot zero**

Clears the primary, secondary, or default boot parameters.

**Syntax**

```
boot zero [primary | secondary | default]
```

**Command Modes**
uBoot

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**default gateway**

Set the default gateway IP address.

**Syntax**

```
default-gateway <ip-address>
```

**Command Modes**
uBoot

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**enable**

Change the access privilege level.

**Syntax**

```
enable [user | admin]
```

**Command Modes**
uBoot

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
help

Display help menu.

Syntax

```plaintext
help
```

Command Modes

uBoot

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

**Figure 52-3. help Command Example**

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (22 commands total):
  boot change [primary|secondary|default]
  change operating system boot parameters
  boot selection {a|b}
  change the rom bootstrap bootflash partition
  boot show net config retries
  show number of retries for network boot config failure
  boot write net config retries <int>
  write number of retries for network boot config failure
  boot zero [primary|secondary|default]
  zero operating system boot parameters
  default-gateway <ip-address>
  default-gateway - set the default gateway ip address
  enable [user|admin]
  change access privilege level
  help
  display help menu
-(36%)-Use <CR> to continue, q to stop:
BOOT_USER #
```
interface management ethernet ip address

Set the management port IP address and mask.

Syntax

```
interface management ethernet ip address <ip/mask>
```

Command Modes

uBoot

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

no default-gateway

Clear the default gateway IP address.

Syntax

```
no default-gateway
```

Command Modes

uBoot

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

no interface management ethernet ip address

Clear the management port IP address and mask.

Syntax

```
o no interface management ethernet ip address
```

Command Modes

uBoot

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

reload

Reload the MXL Switch.

Syntax

```
reload
```

Command Modes

uBoot

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
show boot blc

Show the boot loop counter value.

Syntax

show boot blc

Command Modes

uBoot

Command History

Version 8.3.16.1   Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 52-4.  show boot blc Command Example

BOOT_USER # show boot blc ?
Total 1 possible command found.
Possible command list:
  show boot blc
  show the boot loop counter value
BOOT_USER # show boot blc
Boot Loop Counter : 10
BOOT_USER #

show boot selection

Display ROM bootstrap bootflash partition.

Syntax

show boot selection

Command Modes

uBoot

Command History

Version 8.3.16.1   Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 52-5.  show boot selection Command Example

BOOT_USER # show boot selection
ROM BOOTSTRAP SELECTOR PARMETERS:
------------------------------------
Next ROM bootstrap set to occur from Bootflash partition A.
Last ROM bootstrap occurred from Bootflash partition B.
BOOT_USER #

show bootflash

Show summary of boot flash information.

Syntax

show bootflash

Command Modes

uBoot
show bootflash

Show summary of operating system boot parameters.

**Syntax**

`show bootflash`

**Command Modes**

- uBoot

---

**Command History**

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

---

**Example Figure 52-6. show bootflash Command Example**

```
BOOT_USER # show bootflash

GENERAL BOOTFLASH INFO
------------------------
Bootflash Partition A:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Bootflash Partition B:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Boot Selector Partition:
  Dell Force10 Networks System Boot
  Official IOM_XLOAD_LP_IMG_BOOT_SELECTOR, BSP Release 4.0.0.0bt1
  Created Tue May 1 10:56:34 2012 by build on login-sjc-01

BOOT_USER #
```
show default-gateway

Display the default gateway IP address.

Syntax

show default-gateway

Command Modes

uBoot

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 52-8. show default-gateway Command Example

BOOT_USER # show default-gateway
Gateway IP address: 15.0.0.1
BOOT_USER #

show interface management Ethernet

Show the management port IP address and mask.

Syntax

show interface management ethernet

Command Modes

uBoot
show interface management port config

Show the management port boot characteristics.

Syntax

```
show interface management port config
```

Command Modes

uBoot

Command History

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |

Example

Figure 52-9. show interface management ethernet Command Example

```
BOOT_USER # show interface management ethernet
Management ethernet IP address: 10.16.130.134/16

BOOT_USER #
```

Syntax help

Show syntax information.

Syntax

```
help
```

Command Modes

uBoot

Command History

| Version 8.3.16.1 | Introduced on MXL 10/40GbE Switch IO Module |
Example

**Figure 52-11. help Command Example**

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (22 commands total):
  boot change [primary|secondary|default]  
    change operating system boot parameters
  boot selection [a|b]  
    change the rom bootstrap bootflash partition
  boot show net config retries  
    show number of retries for network boot config failure
  boot write net config retries <int>  
    write number of retries for network boot config failure
  boot zero [primary|secondary|default]  
    zero operating system boot parameters
  default-gateway <ip-address>  
    set the default gateway ip address
  enable [user|admin]  
    change access privilege level
  help  
    display help menu
-(36%)=Use <CR> to continue, q to stop:
BOOT_USER #
```
Uplink Failure Detection (UFD)

Overview

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if used with network interface controller (NIC) teaming, automatic recovery from a failed link.

Commands

The UFD commands described in this chapter are:

- clear ufd-disable
- debug uplink-state-group
- description
- downstream
- downstream auto-recover
- downstream disable links
- enable
- show running-config uplink-state-group
- show uplink-state-group
- uplink-state-group
- upstream

**clear ufd-disable**

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-disabled error state so that an interface can send and receive traffic.

**Syntax**

```
clear ufd-disable {interface interface | uplink-state-group group-id}
```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>debug uplink-state-group</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface</td>
<td>Specifies one or more downstream interfaces. For interface, enter one of the following interface types: 10-Gigabit Ethernet: tengigabitethernet {slot/port</td>
<td>slot/port-range} 40-Gigabit Ethernet: fortygigabitethernet {slot/port</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Command Modes</td>
<td>Command Modes</td>
</tr>
<tr>
<td>EXEC Mode</td>
<td>Command History</td>
<td>Command History</td>
</tr>
<tr>
<td></td>
<td>Version 8.3.16.1</td>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
<tr>
<td>Command History</td>
<td>Related Commands</td>
<td>Related Commands</td>
</tr>
<tr>
<td></td>
<td>downstream</td>
<td>Assigns a port or port-channel to the uplink-state group as a downstream interface.</td>
</tr>
<tr>
<td></td>
<td>upstream</td>
<td>Assigns a port or port-channel to the uplink-state group as an upstream interface.</td>
</tr>
<tr>
<td></td>
<td>uplink-state-group</td>
<td>Creates an uplink-state group and enable the tracking of upstream links.</td>
</tr>
</tbody>
</table>

**debug uplink-state-group**

Enable debug messages for events related to a specified uplink-state group or all groups.

**Syntax**

double uplink-state-group [group-id]

To turn off debugging event messages, use the no debug uplink-state-group [group-id] command.

**Parameters**

group-id

Enables debugging on the specified uplink-state group. Valid group-id values are 1 to 16.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

clear ufd-disable

Re-enables downstream interfaces that are in a UFD-disabled error state.
### description

Enter a text description of an uplink-state group.

**Syntax**

```
description text
```

**Parameters**

- `text`  
  Text description of the uplink-state group.  
  Maximum length: 80 alphanumeric characters.

**Defaults**

none

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

- **Version 8.3.16.1**  
  Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- **uplink-state-group**  
  Creates an uplink-state group and enable the tracking of upstream links.

**Example**

**Figure 53-1. description Command Example**

```
FTOS(conf-uplink-state-group-3)#description Testing UFD feature
FTOS(conf-uplink-state-group-3)#show config
!
uplink-state-group 3
description Testing UFD feature
```

### downstream

Assign a port or port-channel to the uplink-state group as a downstream interface.

**Syntax**

```
downstream interface
```

**Parameters**

- `interface`  
  Enter one of the following interface types:
  - 10-Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
  - 40-Gigabit Ethernet: `fortygigabitethernet {slot/port | slot/port-range}`
  - Port channel: `port-channel {1-512 | port-channel-range}`
  
  Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example:
  - `tengigabitethernet 1/1-2,5,9,11-12`
  - `port-channel 1-3,5`
  
  A comma is required to separate each port and port-range entry.

**Defaults**

none

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

- **Version 8.3.16.1**  
  Introduced on MXL 10/40GbE Switch IO Module
You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. You must configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>downstream</td>
<td>Assigns a port or port-channel to the uplink-state group as a downstream interface.</td>
</tr>
<tr>
<td>upstream</td>
<td>Assigns a port or port-channel to the uplink-state group as an upstream interface.</td>
</tr>
<tr>
<td>uplink-state-group</td>
<td>Creates an uplink-state group and enable the tracking of upstream links.</td>
</tr>
</tbody>
</table>

**downstream auto-recover**

Enable auto-recovery so that UFD-disabled downstream ports in an uplink-state group automatically come up when a disabled upstream port in the group comes back up.

**Syntax**

downstream auto-recover

To disable auto-recovery on downstream links, use the no downstream auto-recover command.

**Defaults**

The auto-recovery of UFD-disabled downstream ports is enabled.

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>downstream</td>
<td>Assigns a port or port-channel to the uplink-state group as a downstream interface.</td>
</tr>
<tr>
<td>upstream</td>
<td>Assigns a port or port-channel to the uplink-state group as an upstream interface.</td>
</tr>
<tr>
<td>uplink-state-group</td>
<td>Creates an uplink-state group and enable the tracking of upstream links.</td>
</tr>
</tbody>
</table>

**downstream disable links**

Configure the number of downstream links in the uplink-state group that are disabled if one upstream link in an uplink-state group goes down.

**Syntax**

downstream disable links {number | all}

To revert to the default setting, use the no downstream disable links command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the number of downstream links to be brought down by UFD. Range: 1 to 1024.</td>
</tr>
<tr>
<td>all</td>
<td>Brings down all downstream links in the group.</td>
</tr>
</tbody>
</table>

**Defaults**

All

**Command Modes**

UPLINK-STATE-GROUP
Uplink Failure Detection (UFD)

When one upstream interface in an uplink-state group goes down, a user-configurable number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message.

If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.

**Related Commands**
- **downstream** Assigns a port or port-channel to the uplink-state group as a downstream interface.
- **upstream** Assigns a port or port-channel to the uplink-state group as an upstream interface.
- **uplink-state-group** Creates an uplink-state group and enable the tracking of upstream links.

**enable**

Re-enable upstream-link tracking for an uplink-state group after it has been disabled.

**Syntax**

```
enable
```

To disable upstream-link tracking without deleting the uplink-state group, use the no enable command.

**Parameters**

- **group-id** Enables debugging on the specified uplink-state group. Valid group-id values are 1 to 16.

**Defaults**

Upstream-link tracking is automatically enabled in an uplink-state group.

**Command Modes**

- UPLINK-STATE-GROUP

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Related Commands**

- **uplink-state-group** Creates an uplink-state group and enable the tracking of upstream links.

**show running-config uplink-state-group**

Display the current configuration of one or more uplink-state groups.

**Syntax**

```
show running-config uplink-state-group [group-id]
```

**Parameters**

- **group-id** Displays the current configuration of all uplink-state groups or a specified group. Valid group-id values are 1 to 16.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege
show uplink-state-group

Display status information on a specified uplink-state group or all groups.

Syntax

show uplink-state-group [group-id] [detail]

Parameters

group-id Displays status information on a specified uplink-state group or all groups. Valid group-id values are 1 to 16.

detail Displays additional status information on the upstream and downstream interfaces in each group.

Defaults

none

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
Example

Figure 53-3. show uplink-state-group Command Examples

<table>
<thead>
<tr>
<th>FTOS# show uplink-state-group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink State Group: 1 Status: Enabled, Up</td>
</tr>
<tr>
<td>Uplink State Group: 3 Status: Enabled, Up</td>
</tr>
<tr>
<td>Uplink State Group: 5 Status: Enabled, Down</td>
</tr>
<tr>
<td>Uplink State Group: 6 Status: Enabled, Up</td>
</tr>
<tr>
<td>Uplink State Group: 7 Status: Enabled, Up</td>
</tr>
<tr>
<td>Uplink State Group: 16 Status: Disabled, Up</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FTOS# show uplink-state-group 16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink State Group: 16 Status: Disabled, Up</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FTOS#show uplink-state-group detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Up): Interface up (Dwn): Interface down (Dis): Interface disabled</td>
</tr>
<tr>
<td>Uplink State Group : 1 Status: Enabled, Up</td>
</tr>
<tr>
<td>Upstream Interfaces :</td>
</tr>
<tr>
<td>Downstream Interfaces :</td>
</tr>
<tr>
<td>Uplink State Group : 3 Status: Enabled, Up</td>
</tr>
<tr>
<td>Upstream Interfaces : Te 0/46(Up) Te 0/47(Up)</td>
</tr>
<tr>
<td>Downstream Interfaces : Te 13/0(Up) Te 13/1(Up) Te 13/3(Up) Te 13/5(Up) Te 13/6(Up)</td>
</tr>
<tr>
<td>Uplink State Group : 5 Status: Enabled, Down</td>
</tr>
<tr>
<td>Upstream Interfaces : Te 0/0(Dwn) Te 0/3(Dwn) Te 0/5(Dwn)</td>
</tr>
<tr>
<td>Downstream Interfaces : Te 13/2(Dis) Te 13/4(Dis) Te 13/11(Dis) Te 13/12(Dis) Te 13/13(Dis) Te 13/14(Dis) Te 13/15(Dis)</td>
</tr>
<tr>
<td>Uplink State Group : 6 Status: Enabled, Up</td>
</tr>
<tr>
<td>Upstream Interfaces :</td>
</tr>
<tr>
<td>Downstream Interfaces :</td>
</tr>
<tr>
<td>Uplink State Group : 7 Status: Enabled, Up</td>
</tr>
<tr>
<td>Upstream Interfaces :</td>
</tr>
<tr>
<td>Downstream Interfaces :</td>
</tr>
<tr>
<td>Uplink State Group : 16 Status: Disabled, Up</td>
</tr>
<tr>
<td>Upstream Interfaces : Te 0/41(Dwn) Po 8(Dwn)</td>
</tr>
<tr>
<td>Downstream Interfaces : Te 0/40(Dwn)</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config uplink-state-group</td>
<td>Displays the current configuration of one or more uplink-state groups.</td>
</tr>
<tr>
<td>uplink-state-group</td>
<td>Creates an uplink-state group and enable the tracking of upstream links.</td>
</tr>
</tbody>
</table>

uplink-state-group

Create an uplink-state group and enable the tracking of upstream links on a switch/router.

Syntax

```
uplink-state-group group-id
```

To delete an uplink-state group, use the `no uplink-state-group group-id` command.

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command in Uplink-State-Group Configuration mode.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-id</td>
<td>Enter the ID number of an uplink-state group. Range: 1-16.</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

CONFIGURATION
After you enter the command, you enter Uplink-State-Group Configuration mode to assign upstream and downstream interfaces to the group.

An uplink-state group is considered to be operationally UP if at least one upstream interface in the group is in the Link-Up state.

An Uplink-State group is considered to be operationally DOWN if no upstream interfaces in the group are in the link-up state. No uplink-state tracking is performed when a group is disabled or in an operationally down state.

**Related Commands**
- `show running-config uplink-state-group`: Displays the current configuration of one or more uplink-state groups.
- `show uplink-state-group`: Displays status information on a specified uplink-state group or all groups.

**Example**

```
Figure 53-4. uplink-state-group Command Example

FTOS(conf)#uplink-state-group 16
FTOS(conf)#
02:23:17: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed uplink state group Admin state to up: Group 16
```

**upstream**

Assign a port or port-channel to the uplink-state group as an upstream interface.

**Syntax**

```
upstream interface
```

**Parameters**

- `interface` Enter one of the following interface types:
  - 10-Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
  - 40-Gigabit Ethernet: `fortygigabitethernet {slot/port | slot/port-range}`
  - Port channel: `port-channel {1-512 | port-channel-range}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example:
- `tengigabitethernet 1/1-2,5,9,11-12`
- `port-channel 1-3,5`
A comma is required to separate each port and port-range entry.

**Defaults**

`none`

**Command Modes**

- `UPLINK-STATE-GROUP`

**Usage Information**

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. You must configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.
You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>downstream</strong></td>
<td>Assigns a port or port-channel to the uplink-state group as a downstream interface.</td>
</tr>
<tr>
<td><strong>upstream</strong></td>
<td>Assigns a port or port-channel to the uplink-state group as an upstream interface.</td>
</tr>
<tr>
<td><strong>uplink-state-group</strong></td>
<td>Creates an uplink-state group and enable the tracking of upstream links.</td>
</tr>
</tbody>
</table>

**Example**

**Figure 53-5. upstream Command Example**

```
FTOS(conf-uplink-state-group-16)# upstream tengigabitethernet 1/10-15
FTOS(conf-uplink-state-group-16)#
```
VLAN Stacking

Overview

With the virtual local area network (VLAN)-stacking feature (also called stackable VLANs and QinQ), you can “stack” VLANs into one tunnel and switch them through the network transparently.

The VLAN stacking commands described in this chapter are:

- `dei enable`
- `dei honor`
- `dei mark`
- `member`
- `show interface dei-honor`
- `show interface dei-mark`
- `vlan-stack access`
- `vlan-stack compatible`
- `vlan-stack dot1p-mapping`
- `vlan-stack protocol-type`
- `vlan-stack trunk`

For information about basic VLAN commands, refer to Virtual LAN (VLAN) Commands in the Layer 2 chapter.

Important Points to Remember

- If the spanning tree protocol (STP) is not enabled across the stackable VLAN network, STP bridge protocol data units (BPDUs) from the customer’s networks are tunneled across the stackable VLAN network.
- If STP is enabled across the stackable VLAN network, STP BPDUs from the customer’s networks are consumed and not tunneled across the stackable VLAN network unless you enable the tunneling protocol.
- Layer 3 protocols are not supported on a stackable VLAN network.
- Assigning an IP address to a stackable VLAN is supported when all the members are only stackable VLAN trunk ports. IP addresses on a stackable VLAN-enabled VLAN is not supported if the VLAN contains stackable VLAN access ports. This facility is provided for the simple network management protocol (SNMP) over a stackable VLAN-enabled VLAN containing only stackable VLAN trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
Dell Networking recommends not using the same MAC address, on different customer VLANs, on the same stackable VLAN.

- Interfaces configured using stackable VLAN access or stackable VLAN trunk commands do not switch traffic for the default VLAN. These interfaces switch traffic only when they are added to a non-default VLAN.

dei enable

Make packets eligible for dropping based on their drop eligible indicator (DEI) value.

**Syntax**

dei enable

**Defaults**

Packets are colored green; no packets are dropped.

**Command Mode**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

dei honor

Honor the incoming DEI value by mapping it to an FTOS drop precedence. You can enter the command once for 0 and once for 1.

**Syntax**

dei honor \{0 | 1\} \{green | red | yellow\}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>green</td>
<td>red</td>
</tr>
<tr>
<td>Green</td>
<td>Red</td>
</tr>
<tr>
<td>High priority packets that are the least preferred to be dropped.</td>
<td></td>
</tr>
<tr>
<td>Lowest priority packets that are always dropped (regardless of congestion status).</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

Disabled; packets with an unmapped DEI value are colored green.

**Command Mode**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must first enable DEI for this configuration to take effect.

**Related Commands**

dei enable Enables DEI.
**dei mark**

Set the DEI value on egress according to the color currently assigned to the packet.

**Syntax**

dei mark \{green \| yellow\} \{0 \| 1\}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{green | yellow}</td>
<td>Choose a color:</td>
</tr>
<tr>
<td>0 | 1</td>
<td>Enter the bit value you want to map to a color.</td>
</tr>
</tbody>
</table>

**Defaults**

All the packets on egress are marked with DEI 0.

**Command Mode**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must first enable DEI for this configuration to take effect.

**Related Commands**

- **dei enable** Enables DEI.

---

**member**

Assign a Stackable VLAN access or trunk port to a VLAN. The VLAN must contain the `vlan-stack compatible` command in its configuration.

**Syntax**

member interface

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number: Range: 1 to 128</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Mode**

conf-if-vl-<vlan-id>-stack

**Command History**

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

**Usage Information**

You must enable stackable VLAN (using the `vlan-stack compatible` command) on the VLAN prior to adding a member to the VLAN.
show interface dei-honor

Display the dei honor configuration.

Syntax

show interface dei-honor [interface slot/port]

Parameters

interface slot/port Enter the interface type followed by the slot and port number.

Command Mode

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 54-1. show interface dei-honor Command Example

FTOS#show interface dei-honor
Default Drop precedence: Green
Interface CFI/DEI Drop precedence
-----------------------------------------------
Te 0/1              0                       Green
Te 0/1              1                       Yellow
Te 8/9              1                       Red
Te 8/40             0                       Yellow

dei honor Honors the incoming DEI value.

show interface dei-mark

Display the dei mark configuration.

Syntax

show interface dei-mark [interface slot/port]

Parameters

interface slot/port Enter the interface type followed by the slot and port number.

Command Mode

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 54-2. show interface dei-mark Command Example

FTOS#show interface dei-mark
Default CFI/DEI Marking: 0
Interface Drop precedence CFI/DEI
-----------------------------------------------
Te 0/1              Green 0
Te 0/1              Yellow 1
Te 8/9              Yellow 0
Te 8/40             Yellow 0
vlan-stack access

Specify a Layer 2 port or port channel as an access port to the Stackable VLAN network.

Syntax

```
vlan-stack access
```

To remove access port designation, use the `no vlan-stack access` command.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```

Usage Information

Prior to enabling this command, to place the interface in Layer 2 mode, you must enter the `switchport` command.

To remove the access port designation, the port must be removed (use the `no member interface` command) from all stackable VLAN-enabled VLANs.

vlan-stack compatible

Enable the Stackable VLAN feature on a VLAN.

Syntax

```
vlan-stack compatible
```

To disable the stackable VLAN feature on a VLAN, use the `no vlan-stack compatible` command.

Defaults

Not configured.

Command Modes

CONF-IF-VLAN

Command History

```
Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
```

Usage Information

You must remove the members prior to disabling the stackable VLAN feature.

To view the stackable VLANs, use the `show vlan` command in EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.
vlan-stack dot1p-mapping

Map C-Tag dot1p values to a S-Tag dot1p value. C-Tag values may be separated by commas and dashed ranges are permitted. Dynamic Mode CoS overrides any Layer 2 QoS configuration in case of conflicts.

Syntax

```
vlan-stack dot1p-mapping c-tag-dot1p values sp-tag-dot1p value
```

Parameters

- `c-tag-dot1p value` Enter the keyword followed by the customer dot1p value that will be mapped to a service provider dot1p value.
  
  Range: 0 to 5

- `sp-tag-dot1p value` Enter the keyword followed by the service provider dot1p value.
  
  Range: 0 to 5

Defaults

none

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

vlan-stack protocol-type

Define the Stackable VLAN tag protocol identifier (TPID) for the outer VLAN tag (also called the VMAN tag). If you do not configure this command, FTOS assigns the value 0x9100.

Syntax

```
vlan-stack protocol-type number
```

Parameters

- `number` Enter the hexadecimal number as the Stackable VLAN tag.
  You may specify both bytes of the 2-byte S-Tag TPID.
  Range: 0 to FFFF
  Default: 9100

Defaults

0x9100
vlan-stack trunk

Specify a Layer 2 port or port channel as a trunk port to the stackable VLAN network.

Syntax

```plaintext
vlan-stack trunk
```

To remove a trunk port designation from the selected interface, use the `no vlan-stack trunk` command.

Defaults

Not configured.

Command Modes

- **CONFIGURATION**
- **INTERFACE**

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Usage Information

Prior to using this command, to place the interface in Layer 2 mode, you must execute the `switchport` command.

To remove the trunk port designation, the port must first be removed (using the `no member interface` command) from all stackable VLAN-enabled VLANs.

A VLAN-Stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the VLAN-Stack trunk port is also a member of an untagged VLAN, the port should be in hybrid mode. For more information, refer to `portmode hybrid`.

In **Figure 54-4**, a VLAN-Stack trunk port is configured and then also made part of a single-tagged VLAN.

In **Figure 54-5**, the tag protocol identifier (TPID) is set to 8848. The “Tengig 3/10” port is configured to act as a VLAN-stack access port, while the “Tengig 8/0” port acts as a VLAN-Stack trunk port, switching stackable VLAN traffic for VLAN 10, while also switching untagged traffic for VLAN 30 and tagged traffic for VLAN 40. (To allow VLAN 30 traffic, the native VLAN feature is required, by using the `portmode hybrid` command. For more information, refer to `portmode hybrid` in the Interfaces chapter.

**Related Commands**

- `portmode hybrid` Sets a port (physical ports only) to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.
- `vlan-stack trunk` Specifies a Layer 2 port or port channel as a trunk port to the stackable VLAN network.
### Example 1

**Figure 54-4.  Adding a Stackable VLAN Trunk Port to a Tagged VLAN**

```
FTOS(conf-if-te-0/42)#switchport
FTOS(conf-if-te-0/42)#vlan-stack trunk
FTOS(conf-if-te-0/42)#show config
!
interface Tenigigabitethernet 0/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
FTOS(conf-if-te-0/42)#interface vlan 100
FTOS(conf-if-vl-100)#vlan-stack compatible
FTOS(conf-if-vl-100-stack)#member Tenigigabitethernet 0/42
FTOS(conf-if-vl-100-stack)#show config
!
interface Vlan 100
  no ip address
  vlan-stack compatible
  member Tenigigabitethernet 0/42
  shutdown
FTOS(conf-if-vl-100-stack)#interface vlan 20
FTOS(conf-if-vl-20)#tagged Tenigigabitethernet 0/42
FTOS(conf-if-vl-20)#show config
!
interface Vlan 20
  no ip address
  tagged Tenigigabitethernet 0/42
  shutdown
FTOS(conf-if-vl-20)#do show vlan

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
x - Dot1x untagged, X - Dot1x tagged
G - GVRP tagged, M - Vlan-stack

<table>
<thead>
<tr>
<th>NUM</th>
<th>Status</th>
<th>Description</th>
<th>Q Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Inactive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Active</td>
<td></td>
<td>T Te 0/42</td>
</tr>
<tr>
<td>100</td>
<td>Active</td>
<td></td>
<td>M Te 0/42</td>
</tr>
</tbody>
</table>
```

### Example 2

**Figure 54-5.  Adding a Stackable VLAN Trunk Port to Tagged and Untagged VLANs**

```
Virtual Link Trunking (VLT)

Overview

Virtual link trunking (VLT) allows physical links between two chassis to appear as a single virtual link to the network core. VLT eliminates the requirement for Spanning Tree protocols by allowing LAG terminations on two separate distribution or core switches, and by supporting a loop free topology. VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

Prerequisites: Before you configure VLT, make sure that both VLT peer switches are running the same FTOS version and are configured for RSTP as described in the Virtual Link Trunking (VLT) chapter in the FTOS Configuration Guide.

Commands

- back-up destination
- clear ip mroute
- clear ip pim tib
- lacp ungroup member-independent vlt
- multicast peer-routing timeout
- peer-link port-channel
- peer-routing
- peer-routing-timeout
- primary-priority
- show ip mroute
- show vlt backup-link
- show vlt brief
- show vlt detail
- show vlt inconsistency
- show vlt mismatch
- show vlt role
- show vlt statistics
- system-mac
- unit-id
- vlt domain
- vlt-peer-lag port-channel
**back-up destination**

Configure the IP address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

**Note:**

**Syntax**

```
back-up destination ip-address [interval seconds]
```

**Parameters**

- `ip-address` Enter the IPv4 or IPv6 address of the management interface.
- `interval seconds` Enter the keyword `interval` to specify the time interval used to send hello messages. The range is from 1 to 5 seconds. The default value is 1 second.

**Defaults**

Not configured.

**Command Modes**

VLT DOMAIN

**Usage Information**

Either IPv4 or IPv6 only can be enabled.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

**clear ip mroute**

Clear learned multicast routes on the multicast forwarding table. To clear the protocol-independent multicast (PIM) tree information base, use the `clear ip pim tib` command.

**Syntax**

```
clear ip mroute {group-address [source-address] | * | snooping}
```

**Parameters**

- `group-address [source-address]` Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
- `*` Enter * to clear all multicast routes.
- `snooping` Enter the keyword `snooping` to delete multicast snooping route table entries.

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the MXL 10/40GbE Switch IO Module.</td>
</tr>
</tbody>
</table>

**clear ip pim tib**

Clear PIM tree information from the PIM database.

**Syntax**

```
clear ip pim tib [group]
```

**Parameters**

- `group` (OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).
Virtual Link Trunking (VLT)

### lacp ungroup member-independent vlt

Prevent possible loop during the bootup of a VLT peer switch or a device that accesses the VLT domain.

**Syntax**

```
lacp ungroup member-independent vlt
```

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Usage Information**

LACP on VLT ports (on a VLT switch or access device), which are members of the virtual link trunk, is not brought up until the VLT domain is recognized on the access device.

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

### multicast peer-routing timeout

Configure the time for a VLT node to retain synced multicast routes or synced multicast OIF after VLT peer node failure.

**Syntax**

```
multicast peer-routing timeout value
```

To restore the default value, use the no multicast peer-routing timeout command.

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Enter the timeout value in seconds. The range is from 1 to 1200. The default is 150.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

VLT DOMAIN

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

Syntax

peer-link port-channel id-number

Parameters

- **id-number**: Enter the port-channel number that will act as the interconnect trunk. The range is from 1 to 128.

Defaults

Not configured.

Command Modes

VLT DOMAIN

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

peer-routing

Enable L3 VLT peer-routing.

Syntax

peer-routing

To disable L3 VLT peer-routing, use the no peer-routing command.

Command Modes

VLT DOMAIN

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

peer-routing-timeout

Configure the timeout for the software to wait before connecting to a VLT peer with a “down” status.

Syntax

peer-routing-timeout value

To restore the default value, use the no peer-routing-timeout command.

Parameters

- **value**: Enter the timeout value in seconds. The range is from 1 to 65535. The default value is 0 (no timeout).

Command Modes

VLT DOMAIN

Usage Information

When the timer expires, the software checks to see if the VLT peer is now available. If the VLT peer is not available, peer-routing is disabled on that peer.

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
**primary-priority**
Reconfigure the primary role of VLT peer switches.

**Syntax**
```
primary-priority value
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>To configure the primary role on a VLT peer, enter a lower value than the priority value of the remote peer. The range is from 1 to 65535.</td>
</tr>
</tbody>
</table>

**Default**
32768

**Command Modes**
VLT DOMAIN

**Usage Information**
After you configure the VLT domain on each peer switch on both sides of the interconnect trunk, by default, the FTOS software elects a primary and secondary VLT peer device. Use the `priority` command to reconfigure the primary role of VLT peer switches.

**Command History**
- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**show ip mroute**
View the multicast routing table.

**Syntax**
```
show ip mroute [static | group-address [source-address] | count | snooping [vlan vlan-id] [group-address [source-address]] | summary | vlt [group-address | count]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static</code></td>
<td>(OPTIONAL) Enter the keyword static to view static multicast routes.</td>
</tr>
<tr>
<td><code>group-address [source-address]</code></td>
<td>(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.</td>
</tr>
<tr>
<td><code>count</code></td>
<td>(OPTIONAL) Enter the keyword count to view the number of multicast routes and packets.</td>
</tr>
<tr>
<td><code>snooping [vlan vlan-id] [group-address [source-address]]</code></td>
<td>(OPTIONAL) only: Enter the keyword snooping to display information on the multicast routes PIM-SM snooping discovers. Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. the valid VLAN ID range is from 1 to 4094. Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(OPTIONAL) Enter the keyword summary to view routes in a tabular format.</td>
</tr>
<tr>
<td><code>vlt</code></td>
<td>(OPTIONAL) Enter the keyword vlt to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group. Enter the keyword count to display VLT route and packet data.</td>
</tr>
</tbody>
</table>
Command Modes

```text
EXEC

EXEC Privilege
```

Command History

```
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
```

Examples

### Figure 55-1.  show vlt mroute static Command Output

```
FTOS#show ip mroute static
Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change: 00:00:23
```

### Figure 55-2.  show vlt mroute snooping Command Output

```
FTOS#show ip mroute snooping
IPv4 Multicast Snooping Table (*, 224.0.0.0), uptime 17:46:23
Incoming vlan: Vlan 2
Outgoing interface list:
GigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
Incoming vlan: Vlan 2
Outgoing interface list:
GigabitEthernet 4/11
GigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
Incoming vlan: Vlan 2
Outgoing interface list:
GigabitEthernet 4/11
GigabitEthernet 4/13
GigabitEthernet 4/20
GigabitEthernet 4/13
GigabitEthernet 4/20
```

### Figure 55-3.  show vlt detail Command Output

```
FTOS#show ip mroute
IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
Incoming interface: GigabitEthernet 3/12
Outgoing interface list:
GigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
Incoming interface: GigabitEthernet 3/4
Outgoing interface list:
GigabitEthernet 3/12
GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
Incoming interface: GigabitEthernet 3/12
Outgoing interface list:
GigabitEthernet 3/4
outgoing interface 1
GigabitEthernet 3/4
```

---

**Virtual Link Trunking (VLT)**
Usage Information

The following describes the `show ip mroute` command shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the forwarding entry in the multicast route table.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the multicast forwarding table.</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Lists the interfaces that meet one of the following:</td>
</tr>
</tbody>
</table>
|                | • a directly connected member of the Group
|                | • statically configured member of the Group
|                | • received a (*,G) or (S,G) Join message

**show vlt backup-link**

Display information on backup link operation

**Syntax**

`show vlt backup-link`

**Defaults**

Not configured.

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

Figure 55-4.  `show vlt backup-link` Command Output on VLT peer switches

```
FTOS# show vlt backup-link
VLT Backup Link
--------------------
Destination: 10.11.198.130
Peer HeartBeat status: Up
HeartBeat Timer Interval: 1
HeartBeat Timeout: 3
UDP Port: 34998
HeartBeat Messages Sent: 634
HeartBeat Messages Received: 473
```

**show vlt brief**

Display brief status information about VLT domains currently configured on the switch.

**Syntax**

`show vlt brief`

**Defaults**

Not configured.
show vlt detail

Display detail status information about VLT domains currently configured on the switch.

Syntax
show vlt detail

Defaults
Not configured.

Command Modes
EXEC

Command History
Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Examples

Figure 55-6. show vlt detail Command Output

<table>
<thead>
<tr>
<th>Local LAG Id</th>
<th>Peer LAG Id</th>
<th>Local Status</th>
<th>Peer Status</th>
<th>Active VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>128</td>
<td>UP</td>
<td>UP</td>
<td>1000</td>
</tr>
</tbody>
</table>

FTOS#
show vlt inconsistency

Display deviations in VLT multicast traffic.

Syntax

show vlt inconsistency ip mroute

Command Modes

EXEC

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 55-7. show vlt inconsistency Command Output on VLT peer switches

FTOS#show vlt inconsistency ip mroute
Spanned Multicast routing IIF inconsistency:
Multicast Route                              Local IIF      Peer IIF
(22.22.22.200, 225.1.1.2)                    Vlan 5         Vlan6
(*, 225.1.1.2)                                Vlan 15        te 0/5
FTOS#

show vlt mismatch

Configure the time for a VLT node to retain synced multicast routes or synced multicast OIF after VLT peer node failure.

Syntax

show vlt mismatch

Command Modes

EXEC

Command History

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

Example

Figure 55-8. show vlt mismatch Command Output on VLT peer switches

FTOS#show vlt mismatch
Domain
Parameters              Local         Peer
----------------------- -----------   ---------
System-Mac             00:00:00:0a:0a:0a  00:00:00:00:00:00
Vlan-config
----------------------- -----------   ---------
Vlan-ID     Local Mode Peer Mode
-----------   -----------   -----------
2000        --          L2
3000        L3           --
FTOS#
show vlt role

Display the VLT peer status, role of the local VLT switch, VLT system MAC address and system priority, and the MAC address and priority of the locally-attached VLT device.

**Syntax**

```text
show vlt role
```

**Defaults**

Not configured.

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
FTOS#show vlt role
VLT Role
--------
VLT Role:                     Primary
System MAC address:           00:00:00:0a:0a:0a
Primary Role Priority:         700
Local System MAC address:     00:01:e8:d7:3f:bd
Local System Role Priority:   700
Local Unit Id:                0
Local Role Priority:          700
FTOS#
```

show vlt statistics

Display statistics on VLT operation.

**Syntax**

```text
show vlt statistics
```

**Defaults**

Not configured.

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Example

**Figure 55-10. show vlt statistics Command Output on VLT peer switches**

```
FTOS#show vlt statistics
VLT Domain Statistics
------------------------
HeartBeat Messages Sent: 646
HeartBeat Messages Received: 484
ICL Hello's Sent: 162
ICL Hello's Received: 162
Domain Mismatch Errors: 0
Version Mismatch Errors: 0
Config Mismatch Errors: 14

VLT MAC Statistics
-------------------
L2 Info Pkts sent:65, L2 Mac-sync Pkts Sent:88
L2 Info Pkts Rcvd:82, L2 Mac-sync Pkts Rcvd:61
L2 Reg Request sent:17
L2 Reg Request rcdv:15
L2 Reg Response sent:12
L2 Reg Response rcdv:11

VLT Igmp-Snooping Not Enabled

VLT ARP Statistics
-------------------
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP Tunnel Pkts sent Non Vlt:0
ARP Tunnel Pkts Rcvd Non Vlt:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:18
ARP Reg Request rcdv:16

VLT NDP Statistics
-------------------
NDP NA VLT Tunnel Pkts sent:0
NDP NA VLT Tunnel Pkts Rcvd:0
NDP NA Non-VLT Tunnel Pkts sent:0
NDP NA Non-VLT Tunnel Pkts Rcvd:0
Ndp-sync Pkts Sent:0
Ndp-sync Pkts Rcvd:0
Ndp Reg Request sent:17
Ndp Reg Request rcdv:15

VLT Multicast Statistics
------------------------
Info Pkts Sent: 0
Info Pkts Rcvd: 0
Reg Request Sent: 0
Reg Request Rcvd: 0
Reg Response Sent: 0
Reg Response Rcvd: 0
Route updates sent to Peer: 0
Route updates rcvd from Peer: 0
Route update pkts sent to Peer: 0
Route update pkts rcvd from Peer: 0
```
system-mac

Explicitly configure the MAC address for the VLT domain on a VLT peer switch.

**Syntax**

```
system-mac mac-address
```

**Parameters**

- `mac-address` Enter a MAC address in the format aaaa.bbbb.cccc.

**Defaults**

Automatically assigned based on the primary priority and MAC address of each VLT peer.

**Command Modes**

VLT DOMAIN

**Usage Information**

When you create a VLT domain on a switch, the FTOS software automatically creates a VLT-system MAC address used for internal system operations. Use the `system-mac` command to explicitly define the MAC address for the domain. You must also reconfigure the same MAC address on the VLT peer switch.

Use this command to minimize the time required for the VLT system to synchronize the default MAC address of the VLT domain on both peer switches when one peer switch reboots.

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

unit-id

Explicitly configure the default unit ID of a VLT peer switch.

**Syntax**

```
unit-id id
```

**Parameters**

- `id` Enter the system unit ID for VLT. The range is from 0 to 1.

**Defaults**

Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.

**Command Modes**

VLT DOMAIN

**Usage Information**

When you create a VLT domain on a switch, the FTOS software automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. Use the `unit-id` command to explicitly configure the unit ID of a VLT peer. You must configure a different unit ID (0 or 1) on each peer switch.

Use this command to minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots.

**Command History**

- **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

vlt domain

Enable VLT on a switch, configures a VLT domain, and enters VLT-domain configuration mode.

**Syntax**

```
vlt domain domain-id
```

**vlt-peer-lag port-channel**

Associate the port channel to the corresponding port channel in the VLT peer for the VLT connection to an attached device.

**Syntax**

```plaintext
vlt-peer-lag port-channel id-number
```

**Parameters**

- `id-number` Enter the port-channel number that will connect to another port channel in the VLT peer. The range is from 1 to 128.

**Defaults**

Not configured.

**Command Modes**

- INTERFACE PORT-CHANNEL

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.

---

**domain-id**

Enter the domain ID number. You must configure the same domain ID on the peer switch. VLT uses the domain ID to automatically create a VLT MAC address for the domain. The range is from 1 to 1000.

**Command Modes**

- CONFIGURATION

**Command History**

- Version 9.2(0.0) Introduced on the MXL 10/40GbE Switch IO Module.
Virtual Router Redundancy Protocol (VRRP)

IPv4 VRRP Commands

The virtual router redundancy protocol (VRRP) chapter describes the commands:

- advertise-interval
- authentication-type
- clear counters vrrp
- debug vrrp
- description
- disable
- hold-time
- preempt
- priority
- show config
- show vrrp
- track
- virtual-address
- vrrp delay minimum
- vrrp delay reload
- vrrp-group

The VRRP chapter describes the following VRRP for IPv6 commands:

- clear counters vrrp ipv6
- debug vrrp ipv6
- show vrrp ipv6
- vrrp-ipv6-group

The following commands apply to IPv4 and IPv6:

- advertise-interval
- description
- disable
- hold-time
- preempt
- priority
- show config
- track
- virtual-address
advertise-interval

Set the time interval between VRRP advertisements.

Syntax

advertise-interval seconds

To return to the default settings, use the no advertise-interval command.

Parameters

seconds Enter a number of seconds.
Range: 1 to 255.
Default: 1 second.

Defaults

1 second.

Command Modes

INTERFACE-VRRP

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Dell Networking recommends keeping the default setting for this command. If you do change the time interval between VRRP advertisements on one router, you must change it on all routers.

authentication-type

Enable authentication of VRRP data exchanges.

Syntax

authentication-type simple [encryption-type] password

To delete an authentication type and password, use the no authentication-type command.

Parameters

simple Enter the keyword simple to specify simple authentication.
encryption-type (OPTIONAL) Enter one of the following numbers:
• 0 (zero) for an un-encrypted (clear text) password
• 7 (seven) for hidden text password.
password Enter a character string up to 8 characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.

Defaults

Not configured.

Command Modes

VRRP

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The password is displayed in the show config output if the encryption-type is unencrypted or clear text. If you choose to encrypt the password, the show config displays an encrypted text string.

clear counters vrrp

Clear the counters maintained on VRRP operations.
Syntax: `clear counters vrrp [vrrp-id]`

Parameters:

- `vrrp-id` (OPTIONAL) Enter the number of the VRRP group ID.
  
  Range: 1 to 255

Command Modes: EXEC Privilege

Command History:

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
**debug vrrp**

Allows you to enable debugging of VRRP.

**Syntax**

```
debug vrrp interface [vrrp-id] {all | packets | state | timer}
```

To disable debugging, use the `no debug vrrp interface [vrrp-id] {all | packets | state | timer}` command.

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  - For Port Channel interface types, enter the keyword `port-channel` followed by the number:
    - Range: 1 to 128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN interface, enter the keyword `vlan` followed by the VLAN ID. The VLAN ID range is from 1 to 4094.
- `vrrp-id` (OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
- `all` Enter the keyword `all` to enable debugging of all VRRP groups.
- `bfd` Enter the keyword `bfd` to enable debugging of all VFFP BFD interactions.
- `packets` Enter the keyword `packets` to enable debugging of VRRP control packets.
- `state` Enter the keyword `state` to enable debugging of VRRP state changes.
- `timer` Enter the keyword `timer` to enable debugging of the VRRP timer.

**Command Modes**

EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If no options are specified, debug is active on all interfaces and all VRRP groups.

**description**

Configure a short text string describing the VRRP group.

**Syntax**

```
description text
```

To delete a VRRP group description, use the `no description` command.

**Parameters**

- `text` Enter a text string up to 80 characters long.

**Defaults**

Not enabled.

**Command Modes**

VRRP

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
disable

Disable a VRRP group.

Syntax
disable

To re-enable a disabled VRRP group, use the no disable command.

Defaults
VRRP is enabled.

Command Modes
VRRP

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
To enable VRRP traffic, assign an IP address to the VRRP group using the virtual-address command and enter no disable.

Related Commands
virtual-address Specifies the IP address of the virtual router.

hold-time

Specify a delay (in seconds) before a switch becomes the MASTER virtual router. By delaying the initialization of the VRRP MASTER, the new switch can stabilize its routing tables.

Syntax
hold-time seconds

To return to the default value, use the no hold-time command.

Parameters

seconds Enter a number of seconds.
Range: 0 to 65535.
Default: zero (0) seconds.

Defaults
zero (0) seconds

Command Modes
VRRP

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
If a switch is a MASTER and you change the hold timer, you must disable and re-enable VRRP for the new hold timer value to take effect.

Related Commands
disable Disables a VRRP group.
**preempt**

Permit a BACKUP router with a higher priority value to preempt or become the MASTER router.

**Syntax**

```
preempt
```

To prohibit preemption, use the `no preempt` command.

**Defaults**

Enabled (that is, a BACKUP router can preempt the MASTER router).

**Command Modes**

VRRP

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**priority**

Specify a VRRP priority value for the VRRP group. This value is used by the VRRP protocol during the MASTER election process.

**Syntax**

```
priority priority
```

To return to the default value, use the `no priority` command.

**Parameters**

- `priority` Enter a number as the priority. Enter 255 only if the router’s virtual address is the same as the interface’s primary IP address (that is, the router is the OWNER).
  
  Range: 1 to 255
  
  Default: 100

**Defaults**

100

**Command Modes**

VRRP

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

To guarantee that a VRRP group becomes MASTER, configure the VRRP group’s virtual address with same IP address as the interface’s primary IP address and change the `priority` of the VRRP group to 255.

If you set the `priority` to 255 and the `virtual-address` is not equal to the interface’s primary IP address, an error message appears.

---

**Note:** Configuring VRRP priority 255 on an interface on which DHCP Client is enabled is not supported.
show config

View the non-default VRRP configuration.

**Syntax**

show config [verbose]

**Parameters**

| verbose  | (OPTIONAL) Enter the keyword verbose to view all VRRP group configuration information, including defaults. |

**Command Modes**

VRRP

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

Figure 56-1. show config Command Example

```
FTOS(conf-if-vrid-4)#show conf
vrrp-group 4
  virtual-address 119.192.182.124
```

show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the FTOS returns “No Active VRRP group.”

**Syntax**

show vrrp [vrrp-id] [interface] [brief]

**Parameters**

| vrrp-id  | (OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. Range: 1 to 255. |
| interface | (OPTIONAL) Enter the following keywords and slot/port or number information: |
|           | • For Port Channel interface types, enter the keyword port-channel followed by the number: Range: 1 to 128 |
|           | • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information. |
|           | • For a VLAN interface, enter the keyword vlan followed by the VLAN ID. The VLAN ID range is from 1 to 4094. |
| brief     | (OPTIONAL) Enter the keyword brief to view a table of information on the VRRP groups. |

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Example  Figure 56-2.  show vrrp brief Command Example

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp</th>
<th>Pri</th>
<th>Pre</th>
<th>State</th>
<th>Master addr</th>
<th>Virtual addr(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGig 10/37</td>
<td>1</td>
<td>100</td>
<td>Y</td>
<td>NA/IF</td>
<td>200.200.200.200</td>
<td>200.200.200.201</td>
</tr>
<tr>
<td>TenGig 10/37</td>
<td>3</td>
<td>100</td>
<td>Y</td>
<td>MASTER</td>
<td>1.1.1.1</td>
<td>1.1.1.2</td>
</tr>
</tbody>
</table>

Table 56-1.  show vrrp brief Command Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Lists the interface type, slot and port on which the VRRP group is configured.</td>
</tr>
<tr>
<td>Grp</td>
<td>Displays the VRRP group ID.</td>
</tr>
<tr>
<td>Pri</td>
<td>Displays the priority value assigned to the interface. If the track command is configured to track that interface and the interface is disabled, the cost is subtracted from the priority value assigned to the interface.</td>
</tr>
<tr>
<td>Pre</td>
<td>States whether preempt is enabled on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Y = Preempt is enabled.</td>
</tr>
<tr>
<td></td>
<td>• N = Preempt is not enabled.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the operational state of the interface by using one of the following:</td>
</tr>
<tr>
<td></td>
<td>• NA/IF (the interface is not available).</td>
</tr>
<tr>
<td></td>
<td>• MASTER (the interface associated with the MASTER router).</td>
</tr>
<tr>
<td></td>
<td>• BACKUP (the interface associated with the BACKUP router).</td>
</tr>
<tr>
<td>Master addr</td>
<td>Displays the IP address of the MASTER router.</td>
</tr>
<tr>
<td>Virtual addr(s)</td>
<td>Displays the virtual IP addresses of the VRRP routers associated with the interface.</td>
</tr>
</tbody>
</table>
### Figure 56-3. show vrrp Command Example

FTOS>show vrrp
------------------
TenGigabitEthernet 12/3, VRID: 1, Net: 10.1.1.253
State: Master, Priority: 105, Master: 10.1.1.253 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address: 00:00:5e:00:01:01
Virtual IP address: 10.1.1.252
Authentication: (none)
Tracking states for 1 interfaces:
  Up  Tengigabitethernet 12/17 priority-cost 10
------------------
Tengigabitethernet 12/4, VRID: 2, Net: 10.1.2.253
State: Master, Priority: 110, Master: 10.1.2.253 (local)
Hold Down: 10 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address: 00:00:5e:00:01:02
Virtual IP address: 10.1.2.252
Authentication: (none)
Tracking states for 2 interfaces:
  Up  Tengigabitethernet 2/1 priority-cost 10
  Up  Tengigabitethernet 12/17 priority-cost 10
FTOS>

### Table 56-2. show vrrp Command Description

<table>
<thead>
<tr>
<th>Line Beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tengigabitethernet 12/3...</td>
<td>Displays the Interface, the VRRP group ID, and the network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network address.</td>
</tr>
<tr>
<td>State: master...</td>
<td>Displays the interface’s state:</td>
</tr>
<tr>
<td></td>
<td>• Na/If (not available),</td>
</tr>
<tr>
<td></td>
<td>• master (MASTER virtual router)</td>
</tr>
<tr>
<td></td>
<td>• backup (BACKUP virtual router)</td>
</tr>
<tr>
<td></td>
<td>the interface’s priority and the IP address of the MASTER.</td>
</tr>
<tr>
<td>Hold Down:...</td>
<td>This line displays additional VRRP configuration information:</td>
</tr>
<tr>
<td></td>
<td>• Hold Down displays the hold down timer interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>• Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.</td>
</tr>
<tr>
<td></td>
<td>• AdvInt displays the Advertise Interval in seconds.</td>
</tr>
<tr>
<td>Adv rcvd:...</td>
<td>This line displays counters for the following:</td>
</tr>
<tr>
<td></td>
<td>• Adv rcvd displays the number of VRRP advertisements received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Adv sent displays the number of VRRP advertisements sent on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Gratuitous ARP sent displays the number of gratuitous ARPs sent.</td>
</tr>
<tr>
<td>Virtual MAC address</td>
<td>Displays the virtual MAC address of the VRRP group.</td>
</tr>
<tr>
<td>Virtual IP address</td>
<td>Displays the virtual IP address of the VRRP router to which the interface is connected.</td>
</tr>
</tbody>
</table>
Table 56-2. show vrrp Command Description

<table>
<thead>
<tr>
<th>Authentication:...</th>
<th>States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking states...</td>
<td>This line is displayed if the track command is configured on an interface. Below this line, the following information on the tracked interface is displayed:</td>
</tr>
<tr>
<td></td>
<td>• Dn or Up states whether the interface is down or up.</td>
</tr>
<tr>
<td></td>
<td>• the interface type slot/port information</td>
</tr>
</tbody>
</table>

**track**

Monitor an interface and lower the priority value of the VRRP group on that interface if it is disabled.

**Syntax**

```
track interface [priority-cost cost]
```

To disable monitoring, use the no track interface command.

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383.
    - For Port Channel interface types, enter the keyword **port-channel** followed by the number: Range: 1-128
    - For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
    - For a VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

- **cost**
  - (OPTIONAL) Enter a number as the amount to be subtracted from the priority value.
  - Range: 1 to 254.
  - Default: 10.

**Defaults**

- cost = 10

**Command Modes**

VRRP

**Command History**

- Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If you disable the interface, the cost value is subtracted from the priority value and forces a new MASTER election if the priority value is lower than the priority value in the BACKUP virtual routers.
**virtual-address**

Configure up to 12 IP addresses of virtual routers in the VRRP group. You must set at least one virtual address for the VRRP group to start sending VRRP packets.

**Syntax**

```
virtual-address ip-address1 [... ip-address12]
```

To delete one or more virtual IP addresses, use the `no virtual-address ip-address1 [... ip-address12]` command.

**Parameters**

- `ip-address1` Enter an IP address of the virtual router in dotted decimal format. The IP address must be on the same subnet as the interface’s primary IP address.

- `... ip-address12` (OPTIONAL) Enter up to 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space. The IP addresses must be on the same subnet as the interface’s primary IP address.

**Defaults**

Not configured.

**Command Modes**

VRRP

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

A system message appears after you enter or delete the `virtual-address` command.

To guarantee that a VRRP group becomes MASTER, configure the VRRP group’s virtual address with the same IP address as the interface’s primary IP address and change the `priority` of the VRRP group to 255.

You can ping the virtual addresses configured in all VRRP groups.

---

**vrrp delay minimum**

Set the delay time for VRRP initialization after an interface comes up.

**Syntax**

```
vrrp delay minimum seconds
```

**Parameters**

- `seconds` Enter the number of seconds for the delay for VRRP initialization after an interface becomes operational. Range: 0 to 900 (0 indicates no delay)

**Defaults**

0

**Command Modes**

INTERFACE

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information

This command applies to a single interface. When used in conjunction with the `vrrp delay reload` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for vrrp.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Related Commands

- `vrrp delay reload` Sets the delay time for VRRP initialization after a system reboot.

vrrp delay reload

Set the delay time for VRRP initialization after a system reboot.

Syntax

```
vrrp delay minimum seconds
```

Parameters

- `seconds` Enter the number of seconds for the delay.

  Range: 0 to 900 (0 indicates no delay)

Defaults

0

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

This command applies to all the VRRP configured interfaces on a system. When used in conjunction with the `vrrp delay minimum` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for vrrp.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

You must save the configuration and reload the system for the delay timers to take affect.

Related Commands

- `vrrp delay minimum` Sets the delay time for VRRP initialization after a line card reboot.
vrrp-group

Assign a VRRP ID to an interface. You can configure up to 12 VRRP groups per interface.

Syntax

vrrp-group vrrp-id

Parameters

vrrp-id

Enter a number as the group ID.
Range: 1 to 255.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

Related Commands

- virtual-address Assigns up to 12 virtual IP addresses per VRRP group.

VRRP for IPv6 Commands

clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

Syntax

clear counters vrrp ipv6 [vrid | vrf instance]

Parameters

vrid

(Optional) Enter a number of an IPv6 VRRP group.
Range: 1 to 255.

vrf instance

(Optional) E-Series only: Enter the name of a VRF instance (32 characters maximum) to clear the counters of all IPv6 VRRP groups in the specified VRF.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

debug vrrp ipv6

Allows you to enable debugging of VRRP.
**debug vrrp ipv6 interface [vrid] {all | packets | state | timer}**

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a Port Channel interface, enter the keywords port-channel then a number.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
    - For a VLAN interface, enter the keyword vlan then the VLAN ID. The VLAN ID range is from 1 to 4094.

- **vrid**
  - (OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.

- **all**
  - Enter the keyword all to enable debugging of all VRRP groups.

- **bfd**
  - Enter the keyword bfd to enable debugging of all VRRP BFD interactions.

- **database**
  - Enter the keyword database to display changes related to group, prefix, and interface entries in the VRRP table.

- **packets**
  - Enter the keyword packets to enable debugging of VRRP control packets.

- **state**
  - Enter the keyword state to enable debugging of VRRP state changes.

- **timer**
  - Enter the keyword timer to enable debugging of the VRRP timer.

**Command Modes**

- EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If no options are specified, debug is active on all interfaces and all VRRP groups.

---

**show vrrp ipv6**

View the IPv6 VRRP groups that are active. If no VRRP groups are active, the FTOS returns No Active VRRP group.

**Syntax**

`show vrrp ipv6 [vrid] [interface] [brief]`

**Parameters**

- **vrid**
  - (OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is from 1 to 255.

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a Port Channel interface, enter the keywords port-channel then a number. The range is from 1 to 128.
    - For SONET interfaces, enter the keyword sonet then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
    - For a VLAN interface, enter the keyword vlan then the VLAN ID. The VLAN ID range is from 1 to 4009.

- **brief**
  - (OPTIONAL) Enter the keyword brief to view a table of information on the VRRP groups.
The following describes the show vrrp ipv6 command shown in the following example.

<table>
<thead>
<tr>
<th>Line Beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet...</td>
<td>Displays the Interface, the VRRP group ID, and the network address. If the interface is no sending VRRP packets, 0.0.0.0 appears as the network address.</td>
</tr>
<tr>
<td>VRF</td>
<td>VRF instance to which the interface (on which the VRRP group is configured) belongs.</td>
</tr>
<tr>
<td>State: master...</td>
<td>Displays the interface’s state:</td>
</tr>
<tr>
<td></td>
<td>• Na/If (not available).</td>
</tr>
<tr>
<td></td>
<td>• master (MASTER virtual router).</td>
</tr>
<tr>
<td></td>
<td>• backup (BACKUP virtual router).</td>
</tr>
<tr>
<td></td>
<td>the interface’s priority and the IP address of the MASTER.</td>
</tr>
<tr>
<td>Hold Down:..</td>
<td>This line displays additional VRRP configuration information:</td>
</tr>
<tr>
<td></td>
<td>• Hold Down displays the hold down timer interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>• Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.</td>
</tr>
<tr>
<td></td>
<td>• AdvInt displays the Advertise Interval in seconds.</td>
</tr>
<tr>
<td>Adv rcvd:..</td>
<td>This line displays counters for the following:</td>
</tr>
<tr>
<td></td>
<td>• Adv rcvd displays the number of VRRP advertisements received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Adv sent displays the number of VRRP advertisements sent on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Bad pkts rcvd displays the number of invalid packets received on the interface.</td>
</tr>
<tr>
<td>Virtual MAC address</td>
<td>Displays the virtual MAC address of the VRRP group.</td>
</tr>
<tr>
<td>Virtual IP address</td>
<td>Displays the virtual IP address of the VRRP router to which the interface is connected.</td>
</tr>
<tr>
<td>Tracking states...</td>
<td>Displays information on the tracked interfaces or objects configured for a VRRP group (track command), including:</td>
</tr>
<tr>
<td></td>
<td>• UP or DOWN state of the tracked interface or object (Up or Dn).</td>
</tr>
<tr>
<td></td>
<td>• Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object.</td>
</tr>
<tr>
<td></td>
<td>• Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.</td>
</tr>
</tbody>
</table>
vrrp-ipv6-group

Assign an interface to a VRRP group.

Syntax
vrrp-ipv6-group vrid

Parameters
vrid  Enter the virtual-router ID number of the VRRP group. The VRID range is from 1 to 255.

Defaults
Not configured

Command Modes
INTERFACE

Command History
Version 8.3.16.1 Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information
The VRRP group only becomes active and sends VRRP packets when a link-local virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

- When VRF microcode is not loaded in CAM, the VRID for a VRRP group is the same as the VRID number configured with the vrp-group or vrp-ipv6-group command.
- When VRF microcode is loaded in CAM, the VRID for a VRRP group is equal to 16 times the vrp-group or vrp-ipv6-group vrid number plus the ip vrf vrf-id number. For example, if VRF microcode is loaded and VRRP group 10 is configured in VRF 2, the VRID used for the VRRP group is (16 x 10) + 2, or 162. This VRID value is used in the lowest byte of the virtual MAC address of the VRRP group and is also used for VRF routing.

Note: Configure the same VRID on neighboring routers (Dell Networking or non-Dell Networking) in the same VRRP group in order for all routers to interoperate.
Internet Control Message Protocol (ICMP) Message Types

This chapter lists and describes the possible internet control message protocol (ICMP) Message Types resulting from a ping. The first three columns list the possible symbol or type/code. For example, you would receive a ! or 03 as an echo reply from your ping.

Table 57-1. ICMP Messages and Their Definitions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
<th>Query</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td></td>
<td>0</td>
<td>Timeout (no reply)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>!</td>
<td>0</td>
<td>3</td>
<td>echo reply</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>U</td>
<td>3</td>
<td></td>
<td>destination unreachable:</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td>network unreachable</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>host unreachable</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>protocol unreachable</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>port unreachable</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>fragmentation needed but don’t fragment bit set</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>source route failed</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>destination network unknown</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>destination host unknown</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>source host isolated (obsolete)</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td>destination network administratively prohibited</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>destination host administratively prohibited</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>network unreachable for TOS</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>host unreachable for TOS</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td>communication administratively prohibited by filtering</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td>host precedence violation</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td>precedence cutoff in effect</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>4</td>
<td>0</td>
<td>source quench</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>redirect</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
<td>redirect for network</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>redirect for host</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>redirect for type-of-service and network</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>redirect for type-of-service and host</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td></td>
<td>echo request</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>
Table 57-1. ICMP Messages and Their Definitions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
<th>Query</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>0</td>
<td></td>
<td>router advertisement</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td></td>
<td>router solicitation</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>&amp; 11</td>
<td></td>
<td></td>
<td>time exceeded:</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>0</td>
<td>time-to-live equals 0 during transit</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>time-to-live equals 0 during reassembly</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td></td>
<td>parameter problem:</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td></td>
<td>IP header bad (catchall error)</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>required option missing</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td></td>
<td>timestamp request</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td></td>
<td>timestamp reply</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td></td>
<td>information request (obsolete)</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td></td>
<td>information reply (obsolete)</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td>address mask request</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td>address mask reply</td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>
SNMP Traps

This chapter lists the traps sent by FTOS. Each trap is listed by the fields Message ID, Trap Type, and Trap Option, and the next is the message(s) associated with the trap.

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Trap Type</th>
<th>Trap Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLD_START</td>
<td>SNMP</td>
<td>COLDSTART</td>
<td>%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.</td>
</tr>
<tr>
<td>WARM_START</td>
<td>SNMP</td>
<td>WARMSTART</td>
<td></td>
</tr>
<tr>
<td>COPY_CONFIG_COMPLETE</td>
<td>SNMP</td>
<td>NONE</td>
<td>SNMP Copy Config Command Completed</td>
</tr>
<tr>
<td>LINK_DOWN</td>
<td>SNMP</td>
<td>LINKDOWN</td>
<td>%IFA-1-PORT_LINKDN: changed interface state to down:%d</td>
</tr>
<tr>
<td>LINK_UP</td>
<td>SNMP</td>
<td>LINKUP</td>
<td>%IFA-1-PORT_LINKUP: changed interface state to up:%d</td>
</tr>
<tr>
<td>AUTHENTICATION_FAIL</td>
<td>SNMP</td>
<td>AUTH</td>
<td>%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed. Request with invalid community string.</td>
</tr>
<tr>
<td>EGP_NEIGHBOR_LOSS</td>
<td>SNMP</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>OSTATE_DOWN</td>
<td>SNMP</td>
<td>LINKDOWN</td>
<td>%IFM-1-OSTATE_DN: changed interface state to down:%s</td>
</tr>
<tr>
<td>OSTATE_UP</td>
<td>SNMP</td>
<td>LINKUP</td>
<td>%IFM-1-OSTATE_UP: changed interface state to up:%s</td>
</tr>
<tr>
<td>RMON_RISING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID &lt;oid&gt;</td>
</tr>
<tr>
<td>RMON_FALLING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID &lt;oid&gt;</td>
</tr>
<tr>
<td>RMON_HC_RISING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID &lt;oid&gt;</td>
</tr>
<tr>
<td>RMON_HC_FALLING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID &lt;oid&gt;</td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>RESV</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_MIN_ALRM_TEMP</td>
<td>ENVMON</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_MIN_ALRM_TEMP_CLR</td>
<td>ENVMON</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMRG-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_MAJ_ALRM_TEMP</td>
<td>ENVMON</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_MAJ_ALRM_TEMP_CLR</td>
<td>ENVMON</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%TME_TASK_SUSPEND</td>
<td>ENVMON</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%TME_TASK_TERM</td>
<td>ENVMON</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_CPU_THRESHOLD</td>
<td>ENVMON</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_CPU_THRESHOLD_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_MEM_THRESHOLD</td>
<td>ENVMON</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHM_MEM_THRESHOLD_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%MACMGR_STN_MOVE</td>
<td>ENVMON</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%VRRP_BAUTH</td>
<td>PROTO</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on TenGig 11/12 rcvd pkt with authentication type mismatch.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on TenGig 11/12 rcvd pkt with authentication failure.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%VRRP_GO_MASTER</td>
<td>PROTO</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%VRRP_PROTOCOL_ERROR</td>
<td>PROTO</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>VRRP_PROTOERR: VRRP protocol error on %S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%BGP4_ESTABLISHED</td>
<td>PROTO</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%TRAP-5-Peer_ESTABLISHED: Neighbor %a, state %s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%BGP4_BACKW_XSITION</td>
<td>PROTO</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>%ETS_TRAP_TYPE_MODULE_STATUS_CHANGE</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>ETS_TRAP_TYPE_ADMIN_MODE_CHANGE</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to on for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to off for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>ETS_TRAP_TYPE_OPER_STATE_CHANGE</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to init for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to off for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to recommended for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to rxConfigSrc for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>ETS_TRAP_TYPE_PEER_STATE_CHANGE</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to enabled for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to disabled for port %s</td>
<td>ETS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>PFC_TRAP_TYPE_MODULE_STATUS_CHANGE</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to enabled</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to disabled</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>PFC_TRAP_TYPE_ADMIN_MODE_CHANGE</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to on for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to off for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>PFC_TRAP_TYPE_OPER_STATE_CHANGE</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to init for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to off for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to recommended for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to rxConfigSrc for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>PFC_TRAP_TYPE_PEER_STATE_CHANGE</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE : PFC Peer state changed to enabled for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE : PFC Peer state changed to disabled for port %s</td>
<td>PFC</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>FIPS_MAX_FCF_LIMIT_RCH</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%FCOE-5-MAX_FCF_LIMIT_RCH: Number of FCFs reached maximum allowed limit in VLAN %d</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>FIPS_MAX_ENODE_LIMIT_RCH</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%FCOE-5-MAX_ENODE_LIMIT_RCH: Number of ENodes reached maximum allowed limit in the system</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>FIPS_MAX_SESSION_LIMIT_RCH</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%FCOE-5-MAX_SESSION_LIMIT_RCH: Number of sessions reached maximum allowed limit in the system</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>FIPS_FCF_DROP</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%FCOE-5-FCF_DROP: New FCF(%d,%s) discovered in Vlan %d is dropped as max-FCF-limit per VLAN is reached</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>FIPS_ENODE_DROP</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%FCOE-5-ENODE_DROP: New ENode(%d,%s) discovered in interface %s dropped as max-ENode-limit in system reached</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>FIPS_SESSION_DROP</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%FCOE-5-SESSION_DROP: New session(%,%) request in interface %s dropped as max-session-limit in system reached</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIPS_ACL_INSTALL_FAIL</td>
<td>FIPS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>%FCOE-5-ACL_INSTALL_FAIL: problem in installing ACL entries due to no space or hardware failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHMGR_ENT_LAST_CHANGE_TIME</td>
<td>ENTITY</td>
<td>NONE</td>
<td></td>
</tr>
</tbody>
</table>

No error messages. Time, at which there is a change in a physical entity, is logged.