Dell Force10 FTOS Command Line Reference Guide for the MXL 10/40GbE Switch IO Module

Publication Date: July 2012
1 About this Guide ................................................................. 9
   Objectives ........................................................................ 9
   Audience .......................................................................... 9
   Conventions ...................................................................... 9
   Information Symbols ........................................................ 10
   Related Documents .......................................................... 10

2 CLI Basics ................................................................. 11
   Accessing the Command Line ............................................ 11
   Multiple Configuration Users ............................................ 12
   Navigating the Command Line Interface ......................... 12
   Obtaining Help ................................................................ 13
   Using the Keyword no .................................................... 15
   Filtering show Commands ............................................... 15
   Displaying All Output .................................................... 16
   Filtering Command Output Multiple Times ..................... 16
   Command Modes .......................................................... 16
   EXEC Mode ..................................................................... 16
   EXEC Privilege Mode ..................................................... 17
   CONFIGURATION Mode .................................................. 17
   INTERFACE Mode ......................................................... 17
   LINE Mode ..................................................................... 18
   MAC ACCESS LIST Mode ............................................... 18
   IP ACCESS LIST Mode .................................................... 18
   ROUTE-MAP Mode ........................................................ 18
   PREFIX-LIST Mode ........................................................ 19
   SPANNING TREE Mode .................................................. 19
   Per-VLAN SPANNING TREE Plus Mode ......................... 19
   RAPID SPANNING TREE Mode ....................................... 19
   MULTIPLE SPANNING TREE Mode ............................... 20
   PROTOCOL GVRP Mode ............................................... 20
   ROUTER OSPF Mode ..................................................... 20
   ROUTER RIP Mode ........................................................ 20

3 File Management ..................................................... 21
   Overview ......................................................................... 21
   Basic File Management Commands ................................. 21

4 Control and Monitoring .............................................. 37
   Commands ........................................................................ 37

5 u-Boot ................................................................. 81
   Overview ......................................................................... 81
   Commands ....................................................................... 81
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Access Control Lists (ACL)</td>
<td>91</td>
</tr>
<tr>
<td>Overview</td>
<td>91</td>
</tr>
<tr>
<td>Commands Common to all ACL Types</td>
<td>91</td>
</tr>
<tr>
<td>Common IP ACL Commands</td>
<td>94</td>
</tr>
<tr>
<td>Standard IP ACL Commands</td>
<td>98</td>
</tr>
<tr>
<td>Extended IP ACL Commands</td>
<td>102</td>
</tr>
<tr>
<td>Common MAC Access List Commands</td>
<td>117</td>
</tr>
<tr>
<td>Standard MAC ACL Commands</td>
<td>120</td>
</tr>
<tr>
<td>Extended MAC ACL Commands</td>
<td>123</td>
</tr>
<tr>
<td>IP Prefix List Commands</td>
<td>127</td>
</tr>
<tr>
<td>Route Map Commands</td>
<td>132</td>
</tr>
<tr>
<td>7 Bare Metal Provisioning</td>
<td>143</td>
</tr>
<tr>
<td>Overview</td>
<td>143</td>
</tr>
<tr>
<td>Commands</td>
<td>143</td>
</tr>
<tr>
<td>8 Content Addressable Memory (CAM)</td>
<td>147</td>
</tr>
<tr>
<td>Overview</td>
<td>147</td>
</tr>
<tr>
<td>CAM Profile Commands</td>
<td>147</td>
</tr>
<tr>
<td>Important Points to Remember</td>
<td>147</td>
</tr>
<tr>
<td>9 Data Center Bridging</td>
<td>153</td>
</tr>
<tr>
<td>Overview</td>
<td>153</td>
</tr>
<tr>
<td>DCB Command</td>
<td>153</td>
</tr>
<tr>
<td>PFC Commands</td>
<td>153</td>
</tr>
<tr>
<td>ETS Commands</td>
<td>154</td>
</tr>
<tr>
<td>DCBX Commands</td>
<td>154</td>
</tr>
<tr>
<td>10 Dynamic Host Configuration Protocol (DHCP)</td>
<td>187</td>
</tr>
<tr>
<td>Overview</td>
<td>187</td>
</tr>
<tr>
<td>Commands to Configure the System to be a DHCP Server</td>
<td>187</td>
</tr>
<tr>
<td>Commands to Configure the System to be a DHCP Client</td>
<td>194</td>
</tr>
<tr>
<td>Other Commands supported by DHCP Client</td>
<td>195</td>
</tr>
<tr>
<td>Commands to Configure Secure DHCP</td>
<td>198</td>
</tr>
<tr>
<td>11 FIP Snooping</td>
<td>205</td>
</tr>
<tr>
<td>Overview</td>
<td>205</td>
</tr>
<tr>
<td>12 GARP VLAN Registration (GVRP)</td>
<td>217</td>
</tr>
<tr>
<td>Commands</td>
<td>217</td>
</tr>
<tr>
<td>Important Points to Remember</td>
<td>218</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>22</td>
<td>Port Monitoring</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
</tr>
<tr>
<td>23</td>
<td>Private VLAN (PVLAN)</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td></td>
<td>Private VLAN Concepts</td>
</tr>
<tr>
<td>24</td>
<td>Per-VLAN Spanning Tree Plus (PVST+)</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>25</td>
<td>Quality of Service (QoS)</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Global Configuration Commands</td>
</tr>
<tr>
<td></td>
<td>Per-Port QoS Commands</td>
</tr>
<tr>
<td></td>
<td>Policy-Based QoS Commands</td>
</tr>
<tr>
<td>26</td>
<td>Routing Information Protocol (RIP)</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>27</td>
<td>Remote Monitoring (RMON)</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>28</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>29</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td></td>
<td>AAA Accounting Commands</td>
</tr>
<tr>
<td></td>
<td>Authorization and Privilege Commands</td>
</tr>
<tr>
<td></td>
<td>Authentication and Password Commands</td>
</tr>
<tr>
<td></td>
<td>RADIUS Commands</td>
</tr>
<tr>
<td></td>
<td>TACACS+ Commands</td>
</tr>
<tr>
<td></td>
<td>SSH Server and SCP Commands</td>
</tr>
<tr>
<td></td>
<td>Secure DHCP Commands</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>30</td>
<td>sFlow</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>31</td>
<td>Simple Network Management Protocol (SNMP) and Syslog</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>SNMP Commands</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
</tr>
<tr>
<td></td>
<td>Syslog Commands</td>
</tr>
<tr>
<td>32</td>
<td>Storm Control</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
</tr>
<tr>
<td>33</td>
<td>Stacking Commands</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>34</td>
<td>Spanning Tree Protocol (STP)</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td>35</td>
<td>System Time and Date</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>36</td>
<td>Uplink Failure Detection (UFD)</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Commands</td>
</tr>
<tr>
<td>37</td>
<td>VLAN Stacking</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
</tr>
<tr>
<td>38</td>
<td>Virtual Router Redundancy Protocol (VRRP)</td>
</tr>
<tr>
<td></td>
<td>IPv4 VRRP Commands</td>
</tr>
<tr>
<td>39</td>
<td>Debugging and Diagnostics</td>
</tr>
<tr>
<td></td>
<td>Offline Diagnostic Commands</td>
</tr>
<tr>
<td></td>
<td>Important Points to Remember</td>
</tr>
</tbody>
</table>
Buffer Tuning Commands ................................................................. 677
Hardware Commands ................................................................. 682

40 Internet Control Message Protocol (ICMP) Message Types .......... 695
41 SNMP Traps ........................................................................ 697
42 Index ................................................................................. 701
43 Command Index ................................................................... 719
About this Guide

This book provides information about the Dell Force10 operating software (FTOS) command line interface (CLI). It includes some information about the protocols and features found in FTOS and on the Dell Force10 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 8.3.16.1
This chapter describes the command structure and command modes. The Dell Force10 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 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-&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-fo-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-po-1)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-fo-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-ma-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-range)#</td>
<td></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><code>access-list</code></td>
<td>Named access-list</td>
</tr>
<tr>
<td><code>control-plane</code></td>
<td>Control plane configuration</td>
</tr>
<tr>
<td><code>dhcp</code></td>
<td>DHCP configuration commands</td>
</tr>
<tr>
<td><code>domain-list</code></td>
<td>Domain name to complete unqualified host name</td>
</tr>
<tr>
<td><code>domain-lookup</code></td>
<td>Enable IP Domain Name System hostname translation</td>
</tr>
<tr>
<td><code>domain-name</code></td>
<td>Define the default domain name</td>
</tr>
<tr>
<td><code>ftp</code></td>
<td>FTP configuration commands</td>
</tr>
<tr>
<td><code>helper-address</code></td>
<td>DHCP relay agent configuration</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Add an entry to the ip hostname table</td>
</tr>
<tr>
<td><code>igmp</code></td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td><code>max-frag-count</code></td>
<td>Max. fragmented packets allowed in IP re-assembly</td>
</tr>
<tr>
<td><code>mroute</code></td>
<td>Multicast routes and counters</td>
</tr>
<tr>
<td><code>msdp</code></td>
<td>Multicast source discovery protocol</td>
</tr>
<tr>
<td><code>multicast-limit</code></td>
<td>Max entries in Multicast TIB</td>
</tr>
<tr>
<td><code>multicast-msdp</code></td>
<td>Enable IP multicast MSDP protocol</td>
</tr>
<tr>
<td><code>multicast-routing</code></td>
<td>Enable IP multicast forwarding</td>
</tr>
<tr>
<td><code>name-server</code></td>
<td>Specify address of name server to use</td>
</tr>
<tr>
<td><code>pim</code></td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td><code>prefix-list</code></td>
<td>Build a prefix list</td>
</tr>
<tr>
<td><code>route</code></td>
<td>Interface configuration for RADIUS</td>
</tr>
<tr>
<td><code>scp</code></td>
<td>SCP configuration commands</td>
</tr>
<tr>
<td><code>source-route</code></td>
<td>Process packets with source routing header options</td>
</tr>
<tr>
<td><code>ssh</code></td>
<td>SSH configuration commands</td>
</tr>
<tr>
<td><code>tacacs</code></td>
<td>Interface configuration for TACACS+</td>
</tr>
<tr>
<td><code>telnet</code></td>
<td>Specify telnet options</td>
</tr>
<tr>
<td><code>tftp</code></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` instead of `interface tengigabitethernet`.
- 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>
<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 (OSPFv2).

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 Force10 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**

```plaintext
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**

```plaintext
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**

```
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**

```
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**

```
cd
```

Changes the working directory.

### 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

**Figure 3-3. dir for the Internal Flash Command 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 drwx 720969768 Mar 05 2010 03:25:40 +00:00 6gb
  7 drwx 4260 Mar 03 2010 22:04:50 +00:00 prem-23-5-12
  8 drwx 31969685 Mar 05 2010 17:56:26 +00:00 FTOS-XL-8-3-16-148.bin
  9 drwx 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>Copies the current configuration to either the startup-configuration file or the terminal.</td>
</tr>
<tr>
<td>show file</td>
<td>Displays the contents of a text file in the local filesystem.</td>
</tr>
<tr>
<td>show file-systems</td>
<td>Displays information about the file systems on the system.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging coredump server</td>
<td>Designates a sever to upload kernel core-dumps.</td>
</tr>
</tbody>
</table>
logging coredump server

Designate a server to upload core dumps.

**Syntax**

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

**Parameters**

- *(ipv4-address)*: Enter the server IPv4 address (A.B.C.D)
- *name*: Enter a username to access the target server.
- *type*: Enter the password type:
  - Enter 0 to enter an unencrypted password.
  - Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.
- *password*: Enter a password to access the target server.

**Defaults**

Crash kernel files are uploaded to flash by default.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</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**

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**

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

**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

<table>
<thead>
<tr>
<th>url</th>
<th>Enter the following keywords and a filename:</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 the external Flash, enter usbflash:// followed by the filename.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `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**

```
FTOS#show file-systems

<table>
<thead>
<tr>
<th>Size(b)</th>
<th>Free(b)</th>
<th>Feature</th>
<th>Type</th>
<th>Flags</th>
<th>Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2143281152</td>
<td>2000936960</td>
<td>FAT32</td>
<td>USERFLASH</td>
<td>rw</td>
<td>flash:</td>
</tr>
<tr>
<td>15848660992</td>
<td>831594496</td>
<td>FAT32</td>
<td>USBFLASH</td>
<td>rw</td>
<td>usbflash:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>-</td>
<td>rw</td>
<td>ftp:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>-</td>
<td>rw</td>
<td>tftp:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>-</td>
<td>rw</td>
<td>scp:</td>
</tr>
</tbody>
</table>

FTOS#
```

**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>

**Related Commands**

- **format flash** Erases all existing files and reformats the filesystem in the internal flash memory.
- **show file** Displays the contents of a text file in the local filesystem.
- **show startup-config** Displays the current SFM status.

**show os-version**

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

**Syntax**

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

**Parameters**

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

**Defaults**

- none

**Command Modes**

- EXEC Privilege
Example

**Figure 3-8. show os-version Command Example**

```bash
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
  - `boot` for the current boot configuration
  - `class-map` for the current class-map configuration
  - `fefd` for the current FEFD configuration
  - `ftp` for the current FTP configuration
  - `fvrp` for the current FVRP configuration
  - `host` for the current host configuration
  - `hardware-monitor` for hardware-monitor action-on-error settings
  - `igmp` for the current IGMP configuration
  - `interface` for the current interface configuration
  - `line` for the current line 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-route` for the current Management port forwarding configuration
  - `mroute` for the current Mroutes 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
  - `prefix-list` for the current prefix-list configuration
  - `privilege` for the current privilege configuration
  - `radius` for the current RADIUS configuration
  - `resolve` for the current DNS configuration
  - `rip` for the current RIP configuration
  - `route-map` for the current route map configuration
  - `snmp` for the current SNMP configuration
  - `spanning-tree` for the current spanning tree configuration
  - `static` for the current static route configuration
  - `tacacs+` for the current TACACS+ configuration
  - `tftp` for the current TFTP configuration
  - `users` for the current users configuration
  - `wred-profile` for the current wred-profile configuration
### Command Modes

**EXEC Privilege**

### Command History

**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
!
...```

**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

Figure 3-12. show version Command 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
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>
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 Application...</td>
<td>Software version</td>
</tr>
<tr>
<td>Copyright (c)...</td>
<td>Copyright information</td>
</tr>
<tr>
<td>Build Time...</td>
<td>Software build’s date stamp</td>
</tr>
<tr>
<td>Build Path...</td>
<td>Location of the software build files loaded on the system</td>
</tr>
<tr>
<td>Dell Force10 uptime is...</td>
<td>Amount of time the system has been up</td>
</tr>
<tr>
<td>System image...</td>
<td>Image file name</td>
</tr>
<tr>
<td>Chassis Type:</td>
<td>System type (MXL 10/40GbE)</td>
</tr>
<tr>
<td>Control Processor...</td>
<td>Control processor information and amount of memory on processor.</td>
</tr>
<tr>
<td>256M bytes...</td>
<td>Amount of boot flash memory on the system.</td>
</tr>
<tr>
<td>1 34-Port...</td>
<td>Hardware configuration of the system, including the number and type of physical interfaces available.</td>
</tr>
</tbody>
</table>

**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>Parameters</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 boot

**Syntax**

```
upgrade boot {all | bootflash-image | bootselector-image | stack-unit {0-5 | all} {A: | B:}}
```

**Parameters**

- `all`: Enter this keyword to upgrade the bootflash image and selector image.
- `bootflash-image`: Upgrade bootflash image.
- `bootselector-image`: Upgrade bootselector image.
- `stack-unit {0-5 | all} {A: | B:}`: Enter this keyword to upgrade only the mentioned stack-unit.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

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

**Usage Information**

You must reload FTOS after executing this command.

**Example**

**Figure 3-13. upgrade boot Command Example**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS#upgrade boot ? all</td>
<td>Upgrade both boot flash image and selector image</td>
</tr>
<tr>
<td>bootflash-image</td>
<td>Upgrade boot flash image</td>
</tr>
<tr>
<td>bootselector-image</td>
<td>Upgrade boot selector image</td>
</tr>
<tr>
<td>FTOS#</td>
<td></td>
</tr>
</tbody>
</table>

### upgrade system

**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**

none

**Command Modes**

EXEC Privilege

**Command History**

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

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

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

- **unit-id**: Enter the stack member unit identifier of the stack member to reset.
  - **Range**: 0 - 5
  - **all**: Enter `all` to reset all stack members.

- **queue size**: Enter the queue size of the stack member.
  - **Range**: 1 - 15

**Defaults**

Not configured.

**Command Modes**

- **CONFIGURATION**

**Command History**

- **Version 8.3.16.1** Introduced on 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**

- **c**: Enter the keywords `banner exec`, and then enter a character delineator, represented here by the letter `c`, and press ENTER.

- **line**: 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".

**Defaults**

No banner is displayed.

**Command Modes**

- **CONFIGURATION**

**Command History**

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

**Usage Information**

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

Figure 4-1. banner exec Command Example

Related Commands

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

- keyboard-interactive: Enter this keyword to require a carriage return (CR) to get the message banner prompt.
- c: Enter a delineator character to specify the limits of the text banner. In Figure 4-2, the % character is the delineator character.
- line: 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:
  - maximum of 50 lines
  - up to 255 characters per line

Defaults

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

Command Modes

CONFIGURATION

Command History

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

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

```
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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>banner exec</td>
<td>Sets a banner to be displayed when you enter EXEC Privilege mode.</td>
</tr>
<tr>
<td>banner motd</td>
<td>Sets a Message of the Day banner.</td>
</tr>
</tbody>
</table>

**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

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

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>banner exec</td>
<td>Sets a banner to be displayed when you enter the EXEC Privilege mode.</td>
</tr>
<tr>
<td>banner login</td>
<td>Sets a banner to be displayed after successful login to the system.</td>
</tr>
</tbody>
</table>
clear alarms

Clear alarms on the system.

Syntax

clear alarms

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on 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 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}

Parameters

<table>
<thead>
<tr>
<th>Parameter</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 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
configure

Enter CONFIGURATION mode from EXEC Privilege mode.

**Syntax**

```
configure [terminal]
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</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 8.3.16.1 Introduced on 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**

```
debug cpu-traffic-stats
```

**Defaults**

Disabled

**Command Modes**

EXEC Privilege

**Command History**

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

**Usage Information**

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 Force10 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**

```
debug ftpserver
```

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.16.1 Introduced on 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**

Version 8.3.16.1 Introduced on 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**

```
do command
```

**Parameters**

- `command` Enter an EXEC-level command.

**Defaults**

none

**Command Modes**

CONFIGURATION

INTERFACE

**Command History**

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

**Usage Information**

The following commands are **not** supported by the `do` command:

- enable
- disable
- exit
- config
### 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>level</code></td>
<td>(OPTIONAL) Enter a number for a privilege level of FTOS. Range: 0 to 15. Default: 15</td>
</tr>
</tbody>
</table>

**Defaults**

15

**Command Modes**

EXEC

**Command History**

Version 8.3.16.1 Introduced on 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**

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interval</code></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
end

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

Syntax

```
extend```

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 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 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>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.</td>
</tr>
<tr>
<td>seconds</td>
<td>(OPTIONAL) Enter the number of seconds. Range: 0 to 2147483. Default: 0 seconds</td>
</tr>
</tbody>
</table>

**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 MXL 10/40GbE Switch IO Module

**Usage Information**

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
ftp-server enable

Enable FTP server functions on the system.

**Syntax**

```
ftp-server enable
```

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Example**

```
Figure 4-6. Logging on to an FTP Server Example

morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 Dell Force10 (1.0) FTP server ready
Name (10.31.1.111:dch): dch
331 Password required
Password:  
230 User logged in
ftp> pwd
257 Current directory is "flash:"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size          date       time       name
--------       ------     ------    --------
 512    Jul-20-2004 18:15:00   tgtimg
 512    Jul-20-2004 18:15:00   diagnostic
 512    Jul-20-2004 18:15:00   other
 512    Jul-20-2004 18:15:00   tgt
226 Transfer complete
329 bytes received in 0.018 seconds (17.95 Kbytes/s)
ftp>
```

**Related Commands**

- `ftp-server topdir`  
  Sets the directory to be used for incoming FTP connections.

- `ftp-server username`  
  Sets a username and password for incoming FTP connections.

ftp-server topdir

Specify the top-level directory to be accessed when an incoming FTP connection request is made.

**Syntax**

```
ftp-server topdir directory
```

**Parameters**

- `directory`  
  Enter the directory path.

**Defaults**

The internal flash is the default directory.

**Command Modes**

CONFIGURATION
After you enable FTP server functions with the `ftp-server enable` command, Dell Force10 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.

### ftp-server username

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

**Syntax**

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

**Parameters**

- `username` Enter a text string up to 40 characters long as the user name.
- `password password` Enter the keyword `password` followed by a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.
- `encryption-type` (OPTIONAL) After the keyword `password` enter one of the following numbers:
  - 0 (zero) for an unencrypted (clear text) password
  - 7 (seven) for hidden text password.

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION

**Command History**

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

### hostname

Set the host name of the system.

**Syntax**

```plaintext
hostname name
```

**Parameters**

- `name` Enter a text string, up to 32 characters long.

**Defaults**

FTOS

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.16.1 Introduced on 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**
- `encryption-type` (OPTIONAL) Enter one of the following numbers:
  - 0 (zero) for an unencrypted (clear text) password
  - 7 (seven) for hidden text password
- `password` Enter a string up to 40 characters as the password.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

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

**Related Commands**

*copy* Copies files from and to the switch.

## ip ftp username

Assign a user name for outgoing FTP connection requests.

**Syntax**

```
ip ftp username username
```

**Parameters**

*username* Enter a text string as the user name up to 40 characters long.

**Defaults**

No user name is configured.

**Command Modes**

**CONFIGURATION**

**Command History**

Version 8.3.16.1 Introduced on 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
```

**Defaults**

Enabled

**Command Modes**

**CONFIGURATION**

**Command History**

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

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 MXL 10/40GbE Switch IO Module

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] [oif interface (ip src-ipv4-address) | interface]
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>(OPTIONAL) Enter the host name of the devices to which you are testing connectivity.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(OPTIONAL) Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format.</td>
</tr>
</tbody>
</table>
| count              | Enter the number of echo packets to be sent.  
  number: 1 - 2147483647  
  Continuous: transmit echo request continuously  
  Default: 5 |
| datagram size      | Enter the ICMP datagram size.  
  Range: 36 - 15360 bytes  
  Default: 100 |
| timeout            | Enter the interval to wait for an echo reply before timing out.  
  Range: 0 -3600 seconds  
  Default: 2 seconds |
| source             | Enter the IPv4 source ip address or the source interface.  
  • Enter the IP address in A.B.C.D format  
  • 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 interface, enter the keyword `vlan` followed by a number from 1 to 4094. |
| tos                | Enter the type of service required.  
  Range: 0-255  
  Default: 0 |
| df-bit             | Enter Y or N for the `don't fragment` bit in IPv4 header  
  • N: Do not set the `don't fragment` bit  
  • Y: Do set `don't fragment` bit  
  Default is No. |
| validate-reply     | Enter Y or N for reply validation.  
  • N: Do not validate reply data  
  • Y: Do validate reply data  
  Default is No. |
| pattern pattern    | Enter the IPv4 data pattern.  
  Range: 0-FFFF  
  Default: 0xABCD |
| sweep-min-size     | Enter the minimum size of datagram in sweep range.  
  Range: 52-15359 bytes |
| sweep-max-size     | Enter the maximum size of datagram in sweep range.  
  Range: 53-15359 bytes |
### 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 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 C.

**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 MXL 10/40GbE Switch IO Module
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

- `reset stack-unit` Resets any designated stack member except the management unit.

## send

Send messages to one or all terminal line users.

### Syntax

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

### Parameters

- `*` Enter the asterisk character * to send a message to all tty lines.
- `line` Send a message to a specific line.  
  Range: 0 to 11
- `console` Enter the keyword console to send a message to the Primary terminal line.
- `vty` Enter the keyword vty to send a message to the Virtual terminal

### Defaults

- none

### Command Modes

- EXEC

### Command History

- **Version 8.3.16.1** Introduced on 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

- `debug` (OPTIONAL) Enter the keyword debug to add timestamps to debug messages.
- `log` (OPTIONAL) Enter the keyword log to add timestamps to log messages with severity 0 to 6.
- `datetime` (OPTIONAL) Enter the keyword datetime to have the current time and date added to the message.
- `localtime` (OPTIONAL) Enter the keyword localtime to include the localtime in the timestamp.
- `msec` (OPTIONAL) Enter the keyword msec to include milliseconds in the timestamp.
- `show-timezone` (OPTIONAL) Enter the keyword show-timezone to include the time zone information in the timestamp.
- `uptime` (OPTIONAL) Enter the keyword uptime to have the timestamp based on time elapsed since system reboot.
show alarms

View alarms.

Syntax

show alarms

Command Modes

EXEC
EXEC Privilege

Command History

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

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 Mode

EXEC
EXEC Privilege

Command History

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

**Figure 4-9. show command-history Command Example**

```
FTOS#show command-history
- Repeated 1 time.
[4/20 10:27:24]: CMD-(CLI): [line console 0] 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 0/5] by default from console
[4/20 16:38:14]: CMD-(CLI): [show vlan] by default from console
[5/4 9:12:9]: CMD-(TEL0): [show hosts] by admin from vty0 (10.11.68.14)
[5/4 9:13:52]: CMD-(TEL0): [show version] 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#
```

**Related Commands**

- `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**

- `count`: Display the command tree with a usage counter for each command.
- `no`: 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.

**Defaults**

None

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

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

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

```plaintext
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      command usage:1
    binding              option usage: 0
    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
    SLOT/PORT            option usage: 0
    port-channel         option usage: 0
    <1-128>              option usage: 0
    tengigabitethernet   option usage: 0
    SLOT/PORT            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
    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**

- **port number**  
  - (OPTIONAL) Enter the port number to display traffic statistics on that port only.
  - Range: 1 to 1568

- **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
Command History

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

Example

**Figure 4-11. show cpu-traffic-stats Command Example**

FTOS#show cpu-traffic-stats
Processor : CP
---------------
Received 100% traffic on TenGigabitEthernet 8/2 Total packets:100
LLC:0, SNAP:0, IP:100, ARP:0, other:0
Unicast:100, Multicast:0, Broadcast:0
FTOS#

Usage Information

Traffic statistics are sorted on a per-interface basis; the interface receiving the most traffic is displayed first. All CPU and port information is displayed unless a specific port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces. The traffic statistics are collected only after the debug cpu-traffic-stats command is executed; not from the system bootup.

**Note:** After debugging is complete, use the no debug cpu-traffic-stats command to shut off traffic statistics collection.

Related Commands

debug cpu-traffic-stats Enables CPU traffic statistics for debugging.

**show debugging**

View a list of all enabled debugging processes.

**Syntax**

show debugging

**Command Mode**

EXEC Privilege

**Command History**

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

**Example**

**Figure 4-12. show debugging Command Example**

FTOS#show debug
  (Access List: test)
  TenGigabitEthernet 0/16
  ICMP packet debugging is on for TenGigabitEthernet 0/16
  OSPF:1
  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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Enter the keyword <code>all</code> to view all components.</td>
</tr>
<tr>
<td><code>stack-unit unit-id</code></td>
<td>Enter the keyword <code>stack-unit</code> followed by the <code>unit-id</code> to display information on a specific stack member. Range: 0 to 5.</td>
</tr>
<tr>
<td><code>thermal sensor</code></td>
<td>Enter the keyword <code>thermal-sensor</code> to view all components.</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

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**

```plaintext
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#
```

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

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

```

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

```plaintext
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
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 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**

```plaintext
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**

```plaintext
FTOS#show inv media
Slot Port Type     Media                     Serial Number       F10Qualid
-------------------------------------------------------
 0  33  QSFP  40GBASE-CR4-1M      APF11490011J2Q    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              Media not present or accessible
 0  50              Media not present or accessible
 0  51              Media not present or accessible
 0  52              Media not present or accessible
 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

Version 8.3.16.1  Introduced on 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

```text
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.

Or, 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 MXL 10/40GbE Switch IO Module

### Example 1
**Figure 4-19. show processes cpu summary Command Example**

<table>
<thead>
<tr>
<th>CPU utilization</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit0</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>CPU utilization</td>
<td>5Sec</td>
<td>1Min</td>
<td>5Min</td>
</tr>
<tr>
<td>Unit1*</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Unit2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Unit3</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

* Mgmt Unit

### Example 2
**Figure 4-20. show processes cpu management-unit Command Example**

<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>0x00000000</td>
<td>4650</td>
<td>465</td>
<td>10000</td>
<td>4.43%</td>
<td>4.43%</td>
<td>4.43%</td>
<td>0</td>
</tr>
<tr>
<td>0x00000112</td>
<td>56372590</td>
<td>5637259</td>
<td>10000</td>
<td>1.58%</td>
<td>1.78%</td>
<td>1.89%</td>
<td>0</td>
</tr>
<tr>
<td>0x00000107</td>
<td>9630080</td>
<td>963008</td>
<td>10000</td>
<td>0.79%</td>
<td>0.28%</td>
<td>0.33%</td>
<td>0</td>
</tr>
<tr>
<td>0x00000172</td>
<td>1435540</td>
<td>143554</td>
<td>10000</td>
<td>0.00%</td>
<td>0.10%</td>
<td>0.05%</td>
<td>0</td>
</tr>
<tr>
<td>0x000001fc</td>
<td>1366570</td>
<td>136657</td>
<td>10000</td>
<td>0.00%</td>
<td>0.08%</td>
<td>0.05%</td>
<td>0</td>
</tr>
</tbody>
</table>

FTOS#
Example 3  

**Figure 4-21. show processes cpu stack-unit Command Example**

```
FTOS#show process cpu stack-unit 0
CPU utilization for five seconds: 4%/0%; one minute: 3%; five minutes: 2%

<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>96806080</td>
<td>10000</td>
<td>3.00%</td>
<td>3.25%</td>
<td>2.93%</td>
<td>0</td>
</tr>
<tr>
<td>0x76d5000</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>0x762af000</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>0x762f9000</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>0x7631d000</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>0x76348000</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>0x76367000</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>0x76350000</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>0x7629d000</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>0x763c7000</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x763e9000</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>0x77ee0000</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x77ee6000</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>0x77ef6000</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x77ee9000</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x7811a000</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x7811c000</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x7811e000</td>
<td>0</td>
<td>0</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x78365000</td>
<td>10</td>
<td>1</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>0x78367000</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>0x78369000</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>0x7836e000</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>0x785bb000</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

```
FTOS#show processes memory
Memory Statistics Of Stack Unit 0 (bytes)
Total:  2147483648, MaxUsed:   378417152, CurrentUsed:  378417152, CurrentFree: 1769066496

TaskName      TotalAllocated       TotalFreed       MaxHeld    CurrentHolding
f10appioserv          225280              0             0          208896
                    573440              0             0          8716288
ospf          225280              0             0          208896
f10appioserv          225280              0             0          8716288
              548864              0             0         1310720
fcoectrl          262144              0             0         7917568
            548864              0             0         1310720
f10appioserv          225280              0             0          208896
             618496              0             0         7512064
ndpm          225280              0             0          208896
vrrp          335872              0             0         8048640
f10appioserv          225280              0             0          208896
                      180224              0             0         7512064
frrp          225280              0             0          208896
f10appioserv          225280              0             0          208896
xstp          2740224              0             0         9801728
f10appioserv          225280              0             0          208896
                 1007616              0             0         7757824
pim          225280              0             0          208896
f10appioserv          225280              0             0          208896
                    401408              0             0         7639040
lqm           225280              0             0          208896
f10appioserv          225280              0             0          208896
                5496832              0             0        11124736
mrtm         225280              0             0          208896
f10appioserv          225280              0             0          208896
             1036288              0             0         16134144
l2mgr          225280              0             0          208896
f10appioserv          225280              0             0          208896
                   172032              0             0         7483392
l2pm          225280              0             0          208896
arpm          192512              0             0         7057408
FTOS#
```

Example 5  Figure 4-23.  show processes memory stack-unit Command Example

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

TaskName      TotalAllocated       TotalFreed       MaxHeld    CurrentHolding
f10appioserv          225280              0             0          208896
                    573440              0             0          8716288
ospf          225280              0             0          208896
f10appioserv          225280              0             0          8716288
              548864              0             0         1310720
fcoectrl          262144              0             0         7917568
            548864              0             0         1310720
f10appioserv          225280              0             0          208896
             618496              0             0         7512064
ndpm          225280              0             0          208896
vrrp          335872              0             0         8048640
f10appioserv          225280              0             0          208896
                      180224              0             0         7512064
frrp          225280              0             0          208896
f10appioserv          225280              0             0          208896
xstp          2740224              0             0         9801728
f10appioserv          225280              0             0          208896
                 1007616              0             0         7757824
pim          225280              0             0          208896
f10appioserv          225280              0             0          208896
                    401408              0             0         7639040
lqm           225280              0             0          208896
f10appioserv          225280              0             0          208896
                5496832              0             0        11124736
mrtm         225280              0             0          208896
f10appioserv          225280              0             0          208896
             1036288              0             0         16134144
l2mgr          225280              0             0          208896
f10appioserv          225280              0             0          208896
                   172032              0             0         7483392
l2pm          225280              0             0          208896
arpm          192512              0             0         7057408
FTOS#
```

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

- **cp** (OPTIONAL) Enter the keyword cp to view the Control Processor’s SWPQ statistics.

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

```
FTOS#show processes ipc flow-control
Q Statistics on CP Processor
TxProcess RxProcess Cur Len High Mark Out ies Sent Rcvd Retra Retra
ACL0        RTM0        0        0        0        0        0       0     10     10
ACL0        DIFSERV0    0        0        0        0        0       0     10     10
ACL0        IGMP0       0        0        0        0        0       0     10     10
ACL0        PIM0        0        0        0        0        0       0     10     10
ARPMGR0     MRTM0       0        0        0        0        0       0 100   100
LACP0       IFMGR0      0        0        0        0        0       0    25    25
RTM0        OTM0        0        0        0        0        0       0    60    60
RTM0        OTM0        0        0        0        0        0       0    60    60
FTOS#
```

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 queue 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**

```plaintext
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 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>

### Example Figure 4-26. show processes memory management-unit Command Example

```
FTOS#show processes memory management-unit
Total : 2147483648, MaxUsed : 378470400 [05/23/2012 09:49:39]
CurrentUsed: 378470400, CurrentFree: 1769013248
SharedUsed : 18533952, SharedFree : 2437592
```

<table>
<thead>
<tr>
<th>PID</th>
<th>Process</th>
<th>ResSize</th>
<th>Size</th>
<th>Allocs</th>
<th>Frees</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>472</td>
<td>ospf</td>
<td>8716288</td>
<td>573440</td>
<td>94952</td>
<td>0</td>
<td>94952</td>
</tr>
<tr>
<td>94952</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>529</td>
<td>fcoecntrl</td>
<td>7917568</td>
<td>262144</td>
<td>916736</td>
<td>844764</td>
<td>187920</td>
</tr>
<tr>
<td>71972</td>
<td>dhclient</td>
<td>1310720</td>
<td>548864</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>360</td>
<td>ndpm</td>
<td>7512064</td>
<td>618496</td>
<td>4848</td>
<td>0</td>
<td>4848</td>
</tr>
<tr>
<td>4848</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>160</td>
<td>vrrp</td>
<td>8048640</td>
<td>335872</td>
<td>83700</td>
<td>0</td>
<td>83700</td>
</tr>
<tr>
<td>83700</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>508</td>
<td>frpp</td>
<td>7512064</td>
<td>180224</td>
<td>1445898</td>
<td>1341684</td>
<td>137342</td>
</tr>
<tr>
<td>104214</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>186</td>
<td>xstp</td>
<td>9801728</td>
<td>2740224</td>
<td>54986</td>
<td>16564</td>
<td>38422</td>
</tr>
<tr>
<td>38422</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>374</td>
<td>pim</td>
<td>7757824</td>
<td>1007616</td>
<td>111860</td>
<td>0</td>
<td>111860</td>
</tr>
<tr>
<td>111860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

--More--

Table 4-2 defines the fields that appear in the `show processes memory` output.

### 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]
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clients</td>
<td>Enter the keyword clients to display IFM client information.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword summary to display brief information about IFM clients.</td>
</tr>
<tr>
<td>ifagt number</td>
<td>Enter the keyword ifagt followed by the number of an interface agent to display software pipe and IPC statistics.</td>
</tr>
<tr>
<td>ifcb interface</td>
<td>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:</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>• For a 10G Ethernet interface, enter the keyword TenGigabitEthernet.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE.</td>
</tr>
<tr>
<td>stack-unit unit-ID</td>
<td>Enter the keyword stack-unit followed by the stack member number to display IFM information for that unit.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-5</td>
</tr>
<tr>
<td>trace-flags</td>
<td>Enter the keyword trace-flags to display IFM information for internal trace flags.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Mode**

EXEC

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Process ID</td>
</tr>
<tr>
<td>Process</td>
<td>Process Name</td>
</tr>
<tr>
<td>ResSize</td>
<td>Actual resident size of the process in memory</td>
</tr>
<tr>
<td>Size</td>
<td>Process test, stack, and data size</td>
</tr>
<tr>
<td>Allocs</td>
<td>Total dynamic memory allocated</td>
</tr>
<tr>
<td>Frees</td>
<td>Total dynamic memory freed</td>
</tr>
<tr>
<td>Max</td>
<td>Maximum dynamic memory allocated</td>
</tr>
<tr>
<td>Current</td>
<td>Current dynamic memory in use</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>PID</td>
<td>Process ID</td>
</tr>
<tr>
<td>Process</td>
<td>Process Name</td>
</tr>
<tr>
<td>ResSize</td>
<td>Actual resident size of the process in memory</td>
</tr>
<tr>
<td>Size</td>
<td>Process test, stack, and data size</td>
</tr>
<tr>
<td>Allocs</td>
<td>Total dynamic memory allocated</td>
</tr>
<tr>
<td>Frees</td>
<td>Total dynamic memory freed</td>
</tr>
<tr>
<td>Max</td>
<td>Maximum dynamic memory allocated</td>
</tr>
<tr>
<td>Current</td>
<td>Current dynamic memory in use</td>
</tr>
</tbody>
</table>
## 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 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 4-27. show software ifm clients summary Command Example**

```
FTOS#show software ifm clients summary
ClntType Inst svcMask subSvcMask tlvSvcMask tlvSubSvc swp
IPM 0 0x00000000 0x00000000 0x90ff71f3 0xb98784a1 22
RIP 0 0x00000000 0x00000000 0x800010ff 0x0064c798 56
ISIS 0 0x00000002 0x00000000 0x803330f3 0x0013c480 38
L2PM 0 0x00000000 0x00000000 0x87ff79f3 0xd80b0c50 64
ACL 0 0x00000000 0x00000000 0x867f50c3 0x0103c018 21
OSPF 0 0x000000dfa 0x00100338 0x00000000 0x00000000 0
PIM 0 0x000e00f3 0x00000000 0x00000000 0x00000000 0
SNMP 0 0x00000000 0x00000000 0x80000000 0x80000000 0
EVDTERM 0 0x00000000 0x00000000 0x80000020 0x0003c000 20
HRTM 0 0x00000000 0x00000000 0x8f710f3f 0x0c600000 30
DSM 0 0x00000000 0x00000000 0x80771033 0x00000000 58
Mirror 0 0x00000000 0x00000000 0x80770003 0x00000000 25
LACP 0 0x00000000 0x00000000 0x8000383f 0x01000000 33
SFL CP 0 0x00000000 0x00000000 0x807739ff 0x00000000 24
V6RAD 0 0x000000433 0x00000000 0x80000000 0x80000000 0
Unidentified Client0 0x006e0002 0x00000000 0x00000000 0x00000000 0
Unidentified Client0 0x6066003f 0x00000000 0x6066003f 0x00000000 95
LLDP 0 0x000f2433 0x0408c000 0x000f2433 0x0408c000 60
--More--
```
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
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
SM 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

FTOS#
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Force10 technical support to perform troubleshooting on MXL switches.

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit</td>
<td>(OPTIONAL) Enter the keyword stack-unit to view CPU memory usage for the stack member designated by unit-id. Range: 0 to 5</td>
</tr>
<tr>
<td>page</td>
<td>(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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>save</td>
<td>Enter the save keyword to save the command output.</td>
</tr>
<tr>
<td>flash</td>
<td>Save to local flash drive (flash://filename (max 20 chars))</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on 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
|                Pipe through a command
<cr>
FTOS#show tech-support stack-unit 1 ?
page            Page through output
|                Pipe through a command
<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 startup-config
8 -rwx 4 Feb 19 2012 07:05:02 +01:00 dhcpBindConflict
9 -rwx 12829 Feb 18 2012 02:24:14 +01:00 startup-config.backup
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
---------------------------
1       39      41

----------------------------- 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: 43908 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>show version</td>
<td>Displays the FTOS version.</td>
</tr>
<tr>
<td>show system</td>
<td>Displays the current switch status.</td>
</tr>
<tr>
<td>show environment</td>
<td>Displays system component status.</td>
</tr>
<tr>
<td>show processes memory</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>host</td>
<td>Enter the name of a server.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Enter the IPv4 address in dotted decimal format of the server.</td>
</tr>
<tr>
<td>source-interface</td>
<td>(OPTIONAL) Enter the keywords /source-interface 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 loopback followed by a number from zero (0) to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For the Null interface, enter the keyword null followed by 0.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number: 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></td>
<td>• For a VLAN interface, enter the keyword vlan followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>
### terminal length

Configure the number of lines displayed on the terminal screen.

**Syntax**

```plaintext
terminal length screen-length
```

To return to the default values, use the `terminal no length` command.

**Parameters**

- `screen-length` Enter a number of lines. Entering zero will cause the terminal to display without pausing.
  - Range: 0 to 512.
  - Default: 24 lines.

**Defaults**

24 lines

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

---

### terminal xml

Enable XML mode in Telnet and SSH client sessions.

**Syntax**

```plaintext
terminal xml
```

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

**Defaults**

Disabled

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

---
This command enables XML input mode where you can either cut and paste XML requests or enter the XML requests line-by-line. For more information about using the XML feature, refer to the XML chapter in the FTOS Configuration Guide.

**traceroute**

View the packet path to a specific device.

**Syntax**

```
traceroute {host | ip-address}
```

**Parameters**

- **host**
  - Enter the name of device.

- **ip-address**
  - Enter the IP address of the device in dotted decimal format.

**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 MXL 10/40GbE Switch IO Module

When you enter the `traceroute` command without specifying an IP address (Extended Traceroute), 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**

Figure 4-32. `traceroute` (IPv4) Command Example

```
FTOS#traceroute 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
```

**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 M40G-ON

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 M40G-ON

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.
Command Modes

EXEC Privilege

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

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.
u-Boot

Overview

All commands in this chapter are in u-Boot mode. These commands are supported on the Dell Force10 MXL 10/40GbE Switch Module platform only.

To access this mode, hit any key when the following line appears on the console during a system boot:

Hit any key to stop autoboot:

You 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
boot change

Change the operating system boot parameters.

Syntax boot change [primary | secondary | default]

Command Modes uBoot

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>

boot selection

Change the ROM bootstrap bootflash partition.

Syntax boot selection [a | b]

Command Modes uBoot

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>

Example Figure 5-1. boot show net config retries Command Example

```
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**

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

**Example**

Figure 5-2.  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**

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

default gateway
Set the default gateway IP address.

**Syntax**

```
default-gateway <ip-address>
```

**Command Modes**

uBoot

**Command History**

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

enable
Change the access privilege level.

**Syntax**

```
enable [user | admin]
```

**Command Modes**

uBoot

**Command History**

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

Display help menu.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>uBoot</td>
</tr>
</tbody>
</table>

**Example**

**Figure 5-3. help Command Example**

```bash
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 #
```

## ignore enable password

Ignore the enabled password.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>ignore enable-password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>uBoot</td>
</tr>
</tbody>
</table>

**Command History**

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

## ignore startup config

Ignore system startup configuration.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>ignore startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>uBoot</td>
</tr>
</tbody>
</table>
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
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

Example Figure 5-4. show boot blc Command Example

show boot selection
Display ROM bootstrap bootflash partition.

Syntax show boot selection

Command Modes uBoot

Command History

Example Figure 5-5. show boot selection Command Example

show bootflash
Show summary of boot flash information.

Syntax show bootflash

Command Modes uBoot
Example

Figure 5-6.  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 bootvar

Display the boot variables.

Syntax

show bootvar

Command Modes

uBoot

Example

Figure 5-7. show bootvar Command Example

```
BOOT_USER # show bootvar
PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
------------------------------------------
boot device                             : tftp
file name                              : premnath
Management Ethernet IP address         : 10.16.130.134/16
Server IP address                      : 10.16.127.35
Default Gateway IP address             : 15.0.0.1
Management Ethernet MAC address        : 00:01:E8:43:DE:DF
SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
------------------------------------------
No Operating System boot parameters specified!
DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
------------------------------------------
boot device                             : tftp
file name                              : FTOS-XL-8-3-16-99.bin
Management Ethernet IP address         : 10.16.130.134/16
Server IP address                      : 10.16.127.35
Default Gateway IP address             : 15.0.0.1
Management Ethernet MAC address        : 00:01:E8:43:DE:DF
BOOT_USER #
```

show default-gateway

Display the default gateway IP address.

Syntax

show default-gateway

Command History

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

Example

Figure 5-8. 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

**Example**

**Figure 5-10. show interface management port config Command Example**

```
BOOT_USER # show interface management port config
Management ethernet Port Configuration: no Auto Negotiate
Management ethernet Port Configuration: 100M
Management ethernet Port Configuration: full duplex
BOOT_USER #
```
**Example**

**Figure 5-11. help Command Example**

```plaintext
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 #
```
Access Control Lists (ACL)

Overview

The Dell Force10 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.
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.

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)#
```
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

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 of a new sequence number to entries of an existing access-list.

Related Commands

resequence prefix-list ipv4 Resequences a prefix list

resequence prefix-list ipv4

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

Syntax

resequence prefix-list ipv4 \{prefix-list-name StartingSeqNum Step-to-increment\}

Parameters

prefix-list-name Enter the name of configured prefix list, up to 140 characters long.

StartingSeqNum Enter the starting sequence number to resequence.
Range: 0 to 65535

Step-to-Increment Enter the step to increment the sequence number.
Range: 1 to 65535

Defaults

none

Command Modes

EXEC
EXEC Privilege
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

**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**
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**

<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>

clear counters ip access-group

Erase all counters maintained for access lists.

**Syntax**
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**

<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>

ip access-group

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

**Syntax**

```
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.
- **implicit-permit**: (OPTIONAL) Enter the keyword implicit-permit to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
- **vlan vlan-id**: (OPTIONAL) Enter the keyword vlan followed by the ID numbers of the VLANs.

**Defaults**
Not enabled.

**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>
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list standard</td>
<td>Configures a standard ACL.</td>
</tr>
<tr>
<td>ip access-list extended</td>
<td>Configures an extended ACL.</td>
</tr>
</tbody>
</table>

### 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 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**

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

**Parameters**

- `access-list-name` Enter the name of the ACL to be displayed.
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**

<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**

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**

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

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

<table>
<thead>
<tr>
<th>Parameters</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.</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>
</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). |

| 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            | deny Assign an IP ACL filter to deny IP packets.  
                             | ip access-list standard Create a standard ACL. |

**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**

| sequence-number             | Enter a number from 0 to 4294967290.  
                             | Range: 0 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. |
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

deny Configures a filter to drop packets.
permit Configures a filter to forward packets.
seq Assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.
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 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

<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>destination</td>
<td>Enter the IP address of the network or host to which the packets are sent.</td>
</tr>
<tr>
<td>dscp</td>
<td>Enter this keyword to deny a packet based on DSCP value.</td>
</tr>
</tbody>
</table>

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 icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} command.
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 6-2. ICMP Message Type Keywords

<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-redirect</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} [dscp] [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.

---

**Table 6-2. ICMP Message Type Keywords**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>ICMP Message Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>mask-reply</td>
<td>Mask replies</td>
</tr>
<tr>
<td>mask-request</td>
<td>Mask requests</td>
</tr>
<tr>
<td>mobile-redirect</td>
<td>Mobile host redirect</td>
</tr>
<tr>
<td>net-redirect</td>
<td>Network redirect</td>
</tr>
<tr>
<td>net-tos-redirect</td>
<td>Network redirect for TOS</td>
</tr>
<tr>
<td>net-tos-unreachable</td>
<td>Network unreachable for TOS</td>
</tr>
<tr>
<td>net-unreachable</td>
<td>Network unreachable</td>
</tr>
<tr>
<td>network-unknown</td>
<td>Network unknown</td>
</tr>
<tr>
<td>no-room-for-option</td>
<td>Parameter required but no room</td>
</tr>
<tr>
<td>option-missing</td>
<td>Parameter required but not present</td>
</tr>
<tr>
<td>packet-too-big</td>
<td>Fragmentation needed and DF set</td>
</tr>
<tr>
<td>parameter-problem</td>
<td>All parameter problems</td>
</tr>
<tr>
<td>port-unreachable</td>
<td>Port unreachable</td>
</tr>
<tr>
<td>precedence-unreachable</td>
<td>Precedence cutoff</td>
</tr>
<tr>
<td>protocol-unreachable</td>
<td>Protocol unreachable</td>
</tr>
<tr>
<td>reassembly-timeout</td>
<td>Reassembly timeout</td>
</tr>
<tr>
<td>redirect</td>
<td>All redirects</td>
</tr>
<tr>
<td>router-advertisement</td>
<td>Router discovery advertisements</td>
</tr>
<tr>
<td>router-solicitation</td>
<td>Router discovery solicitations</td>
</tr>
<tr>
<td>source-quench</td>
<td>Source quenches</td>
</tr>
<tr>
<td>source-route-failed</td>
<td>Source route failed</td>
</tr>
<tr>
<td>time-exceeded</td>
<td>All time exceeded</td>
</tr>
<tr>
<td>timestamp-reply</td>
<td>Timestamp replies</td>
</tr>
<tr>
<td>timestamp-request</td>
<td>Timestamp requests</td>
</tr>
<tr>
<td>traceroute</td>
<td>Traceroute</td>
</tr>
<tr>
<td>ttl-exceeded</td>
<td>TTL exceeded</td>
</tr>
<tr>
<td>unreachable</td>
<td>All unreachables</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>source</strong></td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td><strong>mask</strong></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><strong>any</strong></td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td><strong>host ip-address</strong></td>
<td>Enter the keyword host followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td><strong>dscp</strong></td>
<td>Enter this keyword to deny a packet based on DSCP value. Range: 0-63</td>
</tr>
<tr>
<td><strong>bit</strong></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><strong>operator</strong></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><strong>port</strong></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><strong>destination</strong></td>
<td>Enter the IP address of the network or host to which the packets are sent.</td>
</tr>
<tr>
<td><strong>mask</strong></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><strong>count</strong></td>
<td>(OPTIONAL) Enter the keyword count to count packets processed by the filter.</td>
</tr>
<tr>
<td><strong>byte</strong></td>
<td>(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.</td>
</tr>
<tr>
<td><strong>order</strong></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><strong>fragments</strong></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
Access Control Lists (ACL) | 107

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 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>0000111111010000</td>
<td>1111111111100000</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>1111100000000000</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000</td>
<td>1111111000000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111000000000</td>
<td>1111111100000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000</td>
<td>1111111111000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111110000000</td>
<td>1111111111111111</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

Denied

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]

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 udp {source mask | any | host ip-address} {destination mask | any | host ip-address} command.

Parameters

<table>
<thead>
<tr>
<th>Source</th>
<th>Enter the IP address of the network or host from which the packets were sent.</th>
</tr>
</thead>
<tbody>
<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</td>
<td>1111111111100000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111100000</td>
<td>1111111111100000</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>1111111000000000</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000</td>
<td>1111111100000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111000000000</td>
<td>1111111100000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000</td>
<td>1111111111000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111110000000</td>
<td>1111111111111111</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>1111100000000000</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>deny</td>
<td>Assigns a deny filter for IP traffic.</td>
</tr>
<tr>
<td>deny tcp</td>
<td>Assigns a deny filter for TCP traffic.</td>
</tr>
</tbody>
</table>

**ip access-list extended**

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

**Syntax**

```plaintext
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

**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**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list standard</td>
<td>Configures a standard IP access list.</td>
</tr>
<tr>
<td>resequence access-list</td>
<td>Displays the current configuration.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Parameters</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. 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 <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

```
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.*
### 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.

<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.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-63</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 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.</td>
</tr>
<tr>
<td></td>
<td>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>0000111110000000</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>1111111000000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111000000000</td>
<td>1111111100000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000</td>
<td>1111111110000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111101000000</td>
<td>1111111111000000</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
ip access-list extended  Creates an extended ACL.
permit  Assigns a permit filter for IP packets.
permit udp  Assigns a permit filter for UDP packets.
**permit udp**

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

**Syntax**

```plaintext
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**

- **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.
- **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 (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.
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</td>
<td>1111111111010000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111010000</td>
<td>1111111111010000</td>
<td>4032</td>
<td>4095</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000</td>
<td>1111111111000000</td>
<td>4096</td>
<td>6143</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0001110000000000</td>
<td>1111111111010000</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000</td>
<td>1111111111010000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001110000000000</td>
<td>1111111111010000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001110000000000</td>
<td>1111111111010000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001110000000000</td>
<td>1111111111111111</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>1111111100000000</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.
<table>
<thead>
<tr>
<th>Command</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>tcp</td>
<td>Enter the keyword <code>tcp</code> to configure a TCP access list filter.</td>
</tr>
<tr>
<td>udp</td>
<td>Enter the keyword <code>udp</code> to configure a UDP access list filter.</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>operator</td>
<td>(OPTIONAL) Enter one of the following logical operands:</td>
</tr>
<tr>
<td></td>
<td>• <code>eq</code> = equal to</td>
</tr>
<tr>
<td></td>
<td>• <code>neq</code> = not equal to</td>
</tr>
<tr>
<td></td>
<td>• <code>gt</code> = greater than</td>
</tr>
<tr>
<td></td>
<td>• <code>lt</code> = less than</td>
</tr>
<tr>
<td></td>
<td>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter.)</td>
</tr>
<tr>
<td>port port</td>
<td>(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the <code>range</code> 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>message-type</td>
<td>(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</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 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 <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
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.

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>
</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><strong>mac-list-name</strong> (OPTIONAL) Enter the name of a configured MAC access list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>EXEC Privilege</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>
**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 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 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</td>
<td>Enter the keyword interface followed by the 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 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>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

Figure 6-6. show mac accounting access-list Command 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 (393143077 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all traffic is subject to the filter.</td>
</tr>
<tr>
<td>mac-source-address-mask</td>
<td>(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).</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>

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**

```plaintext
mac access-list standard mac-list-name
```

**Parameters**

- `mac-list-name` 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**

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**

```plaintext
permit {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 permit {any | mac-source-address mac-source-address-mask}` command.

**Parameters**

- `any` Enter the keyword `any` to forward all packets received with a MAC address.
- `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).
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 any to drop all packets.</td>
</tr>
<tr>
<td>host mac-address</td>
<td>Enter the keyword host 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

Example Figure 6-8. mac access-list extended Command Example

```plaintext
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)#remark 15 ARP
FTOS(conf-ext-macl)#seq 20 permit any any ev2 eq 806 count bytes
FTOS(conf-ext-macl)#seq 30 permit any any ev2 eq 86dd count bytes
FTOS(conf-ext-macl)#perm 40 permit any any count bytes
FTOS(conf-ext-macl)#exit
FTOS(conf)#do show mac accounting access-list snickers interface tengig0/47

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>mac access-list standard</td>
<td>Configures a standard MAC access list.</td>
</tr>
<tr>
<td>show mac accounting access-list</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

```plaintext
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Enter the keyword any to forward all packets.</td>
</tr>
<tr>
<td>host</td>
<td>Enter the keyword host followed by a MAC address to forward 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 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.</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 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.</td>
</tr>
</tbody>
</table>
**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-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.
IP Prefix List Commands

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

- **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.

Defaults

Not configured.

Command Modes

- **PREFIX-LIST**

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**: Configures 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

- **prefix-name**: Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.

Command Modes

- **CONFIGURATION**

Command History

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

Related Commands

- **ip prefix-list**: Configures a prefix list.
Usage Information
Prefix lists redistribute OSPF and RIP routes meeting specific criteria. For related RIP commands, refer to Chapter 26, Routing Information Protocol (RIP). For related OSPF commands supported, refer to FTOS Command Line Reference Guide Chapter 21, Open Shortest Path First (OSPFv2).

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip route list</td>
<td>Displays IP routes in an IP prefix list.</td>
</tr>
<tr>
<td>show ip prefix-list summary</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

<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>

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>deny</td>
<td>Configures a filter to drop packets.</td>
</tr>
<tr>
<td>seq</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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence-number</td>
<td>Enter a number. Range: 1 to 4294967294.</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 condition.</td>
</tr>
<tr>
<td>any</td>
<td>(OPTIONAL) Enter the keyword any to match any packets.</td>
</tr>
<tr>
<td>ip-prefix /nn</td>
<td>(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.</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
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

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

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
### 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 6-10. show ip prefix-list detail Command Example

```bash
FTOS#show ip prefix-list detail
Prefix-list with the last deletion/insertion: filter_ospf
ip prefix-list filter_in:
  count: 3, range entries: 3, sequences: 5 - 10
    seq 5 deny 1.102.0.0/16 le 32 (hit count: 0)
    seq 6 deny 2.1.0.0/16 ge 23 (hit count: 0)
    seq 10 permit 0.0.0.0/0 le 32 (hit count: 0)
ip prefix-list filter_ospf:
  count: 4, range entries: 1, sequences: 5 - 10
    seq 5 deny 100.100.1.0/24 (hit count: 5)
    seq 6 deny 200.200.1.0/24 (hit count: 1)
    seq 7 deny 200.200.2.0/24 (hit count: 1)
    seq 10 permit 0.0.0.0/0 le 32 (hit count: 132)
FTOS#
```

### 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

<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 6-11. show ip prefix-list summary Command Example

```bash
FTOS#show ip prefix summary
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
  count: 3, range entries: 3, sequences: 5 - 10
  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.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Range: 1 - 65535</td>
<td>Default: no sequence number</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

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.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>set metric</td>
</tr>
<tr>
<td>set automatic-tag</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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</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**

route-map Enables a route map.
match interface

Configure a filter to match routes whose next hop is on the interface specified.

**Syntax**

```plaintext
match interface interface
```

To remove a match, use the `no match interface interface` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</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 the 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: Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• For a Ten 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>

**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` 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.
- `match tag` Redistributes routes that match a specific tag.

match ip address

Configure a filter to match routes based on IP addresses specified in an access list.

**Syntax**

```plaintext
match ip address prefix-list-name
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>prefix-list-name</code></td>
<td>Enter 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

**Related Commands**

- `match interface` Redistributes routes that match the next-hop interface.
- `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 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}

Parameters

access-list-name
Enter the name of a configured IP access list, up to 140 characters.

prefix-list prefix-list-name
Enter the keywords prefix-list followed by the name of configured prefix list.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

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

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}

Parameters

access-list-name
Enter the name of a configured IP access list, up to 140 characters.

prefix-list prefix-list-name
Enter the keywords prefix-list followed by 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
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

---

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  (OPTIONAL) Enter the keyword deny to set the route map default as deny.

sequence-number  (OPTIONAL) 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
```

To delete a setting, use the `no set metric` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>(OPTIONAL) Enter + to add a metric-value to the redistributed routes.</td>
</tr>
<tr>
<td>-</td>
<td>(OPTIONAL) Enter - to subtract a metric-value from the redistributed routes.</td>
</tr>
<tr>
<td>metric-value</td>
<td>Enter a number as the new metric value.</td>
</tr>
<tr>
<td>Range:</td>
<td>zero (0) to 4294967295</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**

- `set automatic-tag`: Computes the tag value of the route.
- `set metric-type`: Specifies the route type assigned to redistributed routes.
- `set tag`: Specifies the tag assigned to redistributed routes.

---

### 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**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>Enter the keyword <code>internal</code> to assign the Interior Gateway Protocol metric of the next hop as the route’s BGP MULTI_EXIT_DES (MED) value.</td>
</tr>
<tr>
<td>external</td>
<td>Enter the keyword <code>external</code> to assign the IS-IS external metric.</td>
</tr>
<tr>
<td>type-1</td>
<td>Enter the keyword <code>type-1</code> to assign the OSPF Type 1 metric.</td>
</tr>
<tr>
<td>type-2</td>
<td>Enter the keyword <code>type-2</code> to assign the OSPF Type 2 metric.</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**

- `set automatic-tag`: Computes the tag value of the route.
- `set metric`: Specifies the metric value assigned to redistributed routes.
- `set tag`: Specifies the tag assigned to redistributed routes.
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

!
route-map hopper permit 10
FTOS(conf-route-map)#
```

show route-map

Display the current route map configurations.

**Syntax**

```
show route-map [map-name]
```

**Parameters**

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

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

`route-map` Configures a route map.
Bare Metal Provisioning

Overview

Bare metal provisioning (BMP) or jumpstarting improves accessibility to the MXL 10/40GbE Switch IO Module. Bare metal provisioning performs auto configuration using a configuration file and an approved version of the Dell Force10 operating system (FTOS) from a network source. Bare metal provisioning not only allows you to configure a stack with a minimum of effort, but it is also useful for quick configuration of a stand alone system.

Bare metal provisioning eases configuration in the following key areas:

- Obtaining an IP address, running the configuration, and boot image information from a dynamic host configuration protocol (DHCP) server.
- Allowing access to the system through an Ethernet management port and data ports with or without DHCP-based dynamic IP address configuration of the user device. This does not stop BMP.
- Booting up in Layer 3 mode with interfaces already in No Shutdown mode. Only the management mode will be in No Shutdown mode and have `ip address dhcp` enabled. Front end ports are in the Shut mode. You can configure the username root password if the configuration file is not received.

Note: The MXL 10/40GbE Switch IO Module supports BMP on the management ports and front end ports. BMP is supported on the 10GbE, 40GbE, and management interfaces.

Commands

- `reload-type`
- `show reload-type`
- `show boot jumpstart`
**reload-type**

Reload the system using the specified start-up mode.

**Syntax**

```
reload-type [normal | jump-start auto-save [enable | disable] dhcp-timeout {minutes}
config-download [enable | disable]]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>Enable the normal reload type. The system retrieves the FTOS image and</td>
</tr>
<tr>
<td></td>
<td>start-up configuration files from the flash.</td>
</tr>
<tr>
<td>jump-start</td>
<td>Enable the BMP reload type. The system acts as a DHCP client and</td>
</tr>
<tr>
<td></td>
<td>downloads the FTOS image and configuration and boot files from a</td>
</tr>
<tr>
<td></td>
<td>specified DHCP server.</td>
</tr>
<tr>
<td>dhcp-timeout</td>
<td>Set the amount of time the system waits for a DHCP server response before</td>
</tr>
<tr>
<td></td>
<td>reverting to normal reload type.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 1-50 minutes</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> infinity</td>
</tr>
<tr>
<td></td>
<td>The default time is infinity; if no time is set, the system continues to</td>
</tr>
<tr>
<td></td>
<td>wait unless the stop jump-start command is given.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Dell Force10 recommends setting the value to 2 or higher.</td>
</tr>
<tr>
<td>config-download</td>
<td>Specify if the system should download a configuration file from the DHCP</td>
</tr>
<tr>
<td></td>
<td>server or use the start-up configuration files from the flash.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable:</strong> Download the configuration files from the server.</td>
</tr>
<tr>
<td></td>
<td><strong>Disable:</strong> Use the local start-up configuration files.</td>
</tr>
<tr>
<td>auto-save</td>
<td>Configure the auto save option for the downloaded configuration file.</td>
</tr>
</tbody>
</table>

**Defaults**
jump-start

**Command Modes**
EXEC Privilege

**Command History**

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

---

**show reload-type**

Display the reload type currently configured on the system.

**Syntax**

```
show reload-type
```

**Command Modes**
EXEC Privilege

**Command History**

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

---

**show boot jumpstart**

Display the jumpstart status at any instant.

**Syntax**

```
show boot jumpstart
```

**Command Modes**
EXEC Privilege
stop jump-start

Cancel the jump-start reload process.

Syntax

stop jump-start

Command Modes
EXEC Privilege

Command History

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

Usage Information
This command stops the jump-start process while the reload is in progress. However, if the system is downloading an FTOS image or configuration file, the process is stopped AFTER the DHCP release is sent.
Content Addressable Memory (CAM)

Overview

⚠️ **Warning:** If you are using these features for the first time, contact Dell Force10 Technical Assistance Center (TAC) for guidance. For information on contacting Dell Force10 TAC, visit the Dell Force10 website at [www.force10networks.com/support](http://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 Force10 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`
- `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

- 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 ipv4acl range is 1 to 4.
  - The ipv6acl 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

- Version 8.3.16.1 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

- 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 than 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

- Introduced on MXL 10/40GbE Switch IO Module

Usage Information

The display reflects the settings implemented with the cam-acl command.
Figure 8-1. 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 8-2. 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 8-3. 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#
```
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 Force10 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}

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.

```
dcb-enable
```

Enable DCB.

**Syntax**

```
dcb enable
```

To disable DCB, use the `no dcb enable` command.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

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

**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**

```
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>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-name</code></td>
<td>Maximum: 32 alphanumeric characters.</td>
<td>none</td>
</tr>
</tbody>
</table>

**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**

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**

```
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>
<tbody>
<tr>
<td><code>policy-name</code></td>
<td>Enter the DCB output policy name.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 32 alphanumeric characters.</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>
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dcb-policy output</code></td>
<td>Apply the output policy.</td>
</tr>
</tbody>
</table>

**dcb-policy input**

Apply the input policy with the PFC configuration to an ingress interface.

**Syntax**

```
dcb-policy input policy-name
```

**Parameters**

- `policy-name` Enter the input policy name with the PFC configuration to an ingress interface.

**Defaults**

- none

**Command Modes**

- INTERFACE

**Command History**

- 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dcb-input</code></td>
<td>Create a DCB input policy.</td>
</tr>
</tbody>
</table>
**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 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 stack-unit-id` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>stack-unit-id</code></td>
<td>Enter the stack unit identification.</td>
</tr>
<tr>
<td><code>dcb-input-policy-name</code></td>
<td>Enter the policy name for the DCB input policy.</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**

The `dcb-policy input stack-unit all` command overwrites any previous `dcb-policy input stack-unit stack-unit-id` configurations. Similarly, a `dcb-policy input stack-unit 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 policy-name
```

To delete the output policy, use the `no dcb-policy output policy-name` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-name</code></td>
<td>Enter the output policy name.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

INTERFACE

**Command History**

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

**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><code>dcb-output</code></td>
<td>Create a DCB output policy.</td>
</tr>
</tbody>
</table>

**dcb-policy output stack-unit stack-ports all**

Apply the specified DCB output policy on all ports of the switch stack or a single stacked switch.

**Syntax**

```
dcb-policy output stack-unit {all | stack-unit-id} stack-ports all dcb-output-policy-name
```

**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**

- **Version 8.3.16.1** 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><code>dcb-policy input stack-unit stack-ports all</code></td>
<td>Apply the specified DCB input policy.</td>
</tr>
</tbody>
</table>

**dcb stack-unit all pfc-buffering pfc-port-count pfc-queues**

Configure the PFC buffer for all switches in the stack.

**Syntax**

```
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.
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.

---

**Related Commands**

`dcb stack-unit all pfc-buffering pfc-port-count pfc-queues`

Configure the PFC buffer for all switches in the stack.

---

### dcbx 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 form 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto, cee, cin, ieee-v2.5</td>
<td>Enter the DCBX version type used on the interface, where:</td>
</tr>
<tr>
<td>auto</td>
<td>configures the port to operate using the DCBX version received from a peer.</td>
</tr>
<tr>
<td>cee</td>
<td>configures the port to use CDD (Intel 1.01).</td>
</tr>
<tr>
<td>cin</td>
<td>configures the port to use Cisco-Intel-Nuova (DCBX 1.0).</td>
</tr>
<tr>
<td>ieee-v2</td>
<td>configures the port to use IEEE 802.1az (Draft 2.5).</td>
</tr>
</tbody>
</table>

**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**

```
debug 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all, auto-detect-timer, config-exchng, fail, mgmt, resource, sem, tlv</td>
<td>Enter the type of debugging, where:</td>
</tr>
<tr>
<td>all</td>
<td>enables all DCBX debugging operations.</td>
</tr>
<tr>
<td>auto-detect-timer</td>
<td>enables traces for DCBX auto-detect timers.</td>
</tr>
<tr>
<td>config-exchng</td>
<td>enables traces for DCBX configuration exchanges.</td>
</tr>
<tr>
<td>fail</td>
<td>enables traces for DCBX failures.</td>
</tr>
<tr>
<td>mgmt</td>
<td>enables traces for DCBX management frames.</td>
</tr>
<tr>
<td>resource</td>
<td>enables traces for DCBX system resource frames.</td>
</tr>
<tr>
<td>sem</td>
<td>enables traces for the DCBX state machine.</td>
</tr>
<tr>
<td>tlv</td>
<td>enables traces for DCBX TLVs.</td>
</tr>
</tbody>
</table>

**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

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.
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>

**fcoe priority-bits**

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

**Syntax**

```
fcoe priority-bits priority-bitmap
```

To remove the configured FCoE priority, use the `no fcoe priority-bits` command.

**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
```

To remove the configured iSCSI priority, use the `no iscsi priority-bits` command.

**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 9-1 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.
Defaults

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>DCB INPUT POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Usage Information</td>
<td></td>
</tr>
</tbody>
</table>

you can enable any number of 802.1p priorities 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcb-input</td>
<td>Create a DCB input policy.</td>
</tr>
</tbody>
</table>

**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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-name</td>
<td>Enter the name of the ETS priority group. Maximum: 32 characters.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Usage Information</td>
<td></td>
</tr>
</tbody>
</table>

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.
## 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

- **group-name**
  - Enter the group name of the 802.1p priority group.
  - Maximum: 32 characters.

- **ets-policy-name**
  - Enter the ETS policy name.

### 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

- `dcb-output` Create a DCB output policy.
- `dcb-policy output` Apply the output policy.

## 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

- **value**
  - 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.

### Defaults

none

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>priority-list</code></td>
<td>Configure the 802.1p priorities for an ETS output policy.</td>
</tr>
<tr>
<td><code>set-pgid</code></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**

```plaintext
qos-policy-output policy-name ets
```

To remove the QoS output policy, use the `no qos-policy-output ets` command.

**Parameters**

- `policy-name` Enter the policy name.
  Maximum: 32 characters.

**Command Modes**

CONFIGURATION

**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

- `scheduler` Schedule priority traffic in port queues.
- `bandwidth-percentage` Bandwidth percentage allocated to priority traffic in port queues.

### scheduler

Configure the method used to schedule priority traffic in port queues.

**Syntax**

```plaintext
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

**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 9-1. 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 9-2 lists the show interface dcbx detail field descriptions.

**Table 9-2. 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>
To clear DCBX frame counters, use the `clear dcbx counters interface stack-unit/port` command.

<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 Operational 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 Operational 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>
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} |
|--------|--------------------------------------------------------|

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-type slot/port ets</td>
<td>Enter the port-type slot and port ETS information.</td>
</tr>
<tr>
<td>{summary</td>
<td>detail}</td>
</tr>
</tbody>
</table>

| Command Mode | CONFIGURATION |

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

### Figure 9-3. 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
<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>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
</tbody>
</table>

Priority# | Bandwidth | TSA |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>1</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>2</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>3</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>4</td>
<td>12%</td>
<td>ETS</td>
</tr>
<tr>
<td>5</td>
<td>12%</td>
<td>ETS</td>
</tr>
<tr>
<td>6</td>
<td>12%</td>
<td>ETS</td>
</tr>
<tr>
<td>7</td>
<td>12%</td>
<td>ETS</td>
</tr>
</tbody>
</table>

Remote Parameters:
-------------------
Remote is disabled

Local Parameters :
------------------
Local 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>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0%</td>
<td>ETS</td>
<td></td>
</tr>
</tbody>
</table>

Priority# | Bandwidth | TSA |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>1</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>2</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>3</td>
<td>13%</td>
<td>ETS</td>
</tr>
<tr>
<td>4</td>
<td>12%</td>
<td>ETS</td>
</tr>
<tr>
<td>5</td>
<td>12%</td>
<td>ETS</td>
</tr>
<tr>
<td>6</td>
<td>12%</td>
<td>ETS</td>
</tr>
<tr>
<td>7</td>
<td>12%</td>
<td>ETS</td>
</tr>
</tbody>
</table>

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 9-3 lists the show interface ets detail field descriptions.

**Table 9-3. 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 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 9-4 lists the show interface pfc summary field descriptions.

<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 Admin is enabled</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 and received 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>
Table 9-4. show interfaces pfc summary Command Example Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote is enabled, Priority list</td>
<td>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.</td>
</tr>
<tr>
<td>Remote Willing Status is enabled</td>
<td></td>
</tr>
<tr>
<td>Local is enabled</td>
<td>DCBX operational status (enabled or disabled) with a list of the configured PFC priorities.</td>
</tr>
<tr>
<td>Operational status (local port)</td>
<td>Port state for current operational PFC configuration:</td>
</tr>
<tr>
<td></td>
<td>• Init: Local PFC configuration parameters were exchanged with the peer.</td>
</tr>
<tr>
<td></td>
<td>• Recommend: Remote PFC configuration parameters were received from the peer.</td>
</tr>
<tr>
<td></td>
<td>• Internally propagated: PFC configuration parameters were received from the configuration source.</td>
</tr>
<tr>
<td>PFC DCBX Oper status</td>
<td>Operational status for the exchange of the PFC configuration on the local port: match (up) or mismatch (down).</td>
</tr>
<tr>
<td>State Machine Type</td>
<td>Type of state machine used for DCBX exchanges of the PFC parameters:</td>
</tr>
<tr>
<td></td>
<td>Feature - for legacy DCBX versions; Symmetric - for an IEEE version.</td>
</tr>
<tr>
<td>TLV Tx Status</td>
<td>Status of the PFC TLV advertisements: enabled or disabled.</td>
</tr>
<tr>
<td>PFC Link Delay</td>
<td>Link delay (in quanta) used to pause specified priority traffic.</td>
</tr>
<tr>
<td>Application Priority TLV: FCOE TLV Tx Status</td>
<td>Status of FCoE advertisements in application priority TLVs from the local DCBX port: enabled or disabled.</td>
</tr>
<tr>
<td>Application Priority TLV: SCSI TLV Tx Status</td>
<td>Status of iSCSI advertisements in application priority TLVs from the local DCBX port: enabled or disabled.</td>
</tr>
<tr>
<td>Application Priority TLV: Local FCOE Priority Map</td>
<td>Priority bitmap used by the local DCBX port in FCoE advertisements in application priority TLVs.</td>
</tr>
<tr>
<td>Application Priority TLV: Local ISCSI Priority Map</td>
<td>Priority bitmap used by the local DCBX port in iSCSI advertisements in application priority TLVs.</td>
</tr>
<tr>
<td>Application Priority TLV: Remote FCOE Priority Map</td>
<td>Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.</td>
</tr>
<tr>
<td>Application Priority TLV: Remote ISCSI Priority Map</td>
<td>Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.</td>
</tr>
<tr>
<td>PFC TLV Statistics: Input TLV pkts</td>
<td>Number of PFC TLVs received.</td>
</tr>
<tr>
<td>PFC TLV Statistics: Output TLV pkts</td>
<td>Number of PFC TLVs transmitted.</td>
</tr>
<tr>
<td>PFC TLV Statistics: Error pkts</td>
<td>Number of PFC error packets received.</td>
</tr>
<tr>
<td>PFC TLV Statistics: Pause Tx pkts</td>
<td>Number of PFC pause frames transmitted.</td>
</tr>
<tr>
<td>PFC TLV Statistics: Pause Rx pkts</td>
<td>Number of PFC pause frames received.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-type</td>
<td>Enter the port type.</td>
</tr>
<tr>
<td>slot/port</td>
<td>Enter the slot/port number.</td>
</tr>
</tbody>
</table>

**Command Mode**

INTERFACE

**Command History**

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

**Example**

```
Figure 9-5. show interfaces pfc statistics Command Example

Force10#show interfaces te 0/0 pfc statistics
Interface TenGigabitEthernet 0/0
Priority Received PFC Frames Transmitted PFC Frames
-------- ------------------- ----------------------
 0       0                 0
 1       0                 0
 2       0                 0
 3       0                 0
 4       0                 0
 5       0                 0
 6       0                 0
 7       0                 0
```

show qos dcb-input

Displays the PFC configuration in a DCB input policy.

**Syntax**

```
show qos dcb-input [pfc-profile]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pfc-profile]</td>
<td>Enter the PFC profile.</td>
</tr>
</tbody>
</table>

**Command Mode**

CONFIGURATION

**Command History**

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

**Example**

```
Figure 9-6. 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

Display 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**

```
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

Display 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**

```
Force10# show qos priority-groups
priority-group ipc
  priority-list 4
  set-pgid 2
```

show stack-unit stack-ports ets detail

Display 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 9-9. 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
TC-grp  Priority#  Bandwidth  TSA
---------  --------  --------  -----
0         0,1,2,3,4,5,6,7  100%  ETS
1          -          -      -
2          -          -      -
3          -          -      -
4          -          -      -
5          -          -      -
6          -          -      -
7          -          -      -
8          -          -      -

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
TC-grp  Priority#  Bandwidth  TSA
---------  --------  --------  -----
0         0,1,2,3,4,5,6,7  100%  ETS
1          -          -      -
2          -          -      -
3          -          -      -
4          -          -      -
5          -          -      -
6          -          -      -
7          -          -      -
8          -          -      -
```
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**

- `stack-unit` Enter the stack unit.
- `port-number` Enter the port number.

**Command Mode**

CONFIGURATION

**Command History**

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

**Example**

```
Figure 9-10. 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
```
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.

ddebug ip dhcp server
Display FTOS debugging messages for DHCP.

Syntax
ddebug ip dhcp server [events | packets]

Parameters

- **events**: Enter this keyword to display DHCP state changes.
- **packet**: Enter this keyword to display packet transmission/reception.

Command Mode
EXEC Privilege

Default
none

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

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
```

**dns-server**

Assign a DNS server to clients based on address pool.

```
Syntax:  dns-server address [address2...address8]
Parameters:  
  address  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.
Command Mode:  DHCP <POOL>
Default:  none
```

**domain-name**

Assign a domain to clients based on address pool.

```
Syntax:  domain-name name
Parameters:  
  name  Give a name to the group of addresses in a pool.
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
- **address**: Enter a single address to be excluded from the pool.
- **low-address**: Enter the lowest address in a range of addresses to be excluded from the pool.
- **high-address**: Enter the highest address in a range of addresses to be excluded from the pool.

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
- **address**: Enter the hardware address of the client.

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
- **address/mask**: Enter the host IP address and subnet mask.

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>days</td>
<td>Enter the number of days of the lease. Range: 0-31</td>
</tr>
<tr>
<td>hours</td>
<td>Enter the number of hours of the lease. Range: 0-23</td>
</tr>
<tr>
<td>minutes</td>
<td>Enter the number of minutes of the lease. Range: 0-59</td>
</tr>
<tr>
<td>infinite</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>address</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 Force10 recommends specifying clients as hybrid.

Syntax

```
 netbios-node-type type
```

Dynamic Host Configuration Protocol (DHCP) | 191
**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| type       | Enter the NETBIOS node type.  
Broadcast: Enter the keyword b-node.  
Hybrid: Enter the keyword h-node.  
Mixed: Enter the keyword m-node.  
Peer-to-peer: Enter the keyword p-node. |

**Command Mode**

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>DHCP &lt;POOL&gt;</th>
</tr>
</thead>
</table>

**Default**

Hybrid

**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>

## network

Specify the range of addresses in an address pool.

**Syntax**

network network/prefix-length

**Parameters**

<table>
<thead>
<tr>
<th>network/</th>
<th>prefix-length</th>
</tr>
</thead>
</table>
| Specify a range of addresses.  
Prefix-length Range: 17-31 |

**Command Mode**

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>DHCP &lt;POOL&gt;</th>
</tr>
</thead>
</table>

**Default**

none

**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>

## show ip dhcp binding

Display the DHCP binding table.

**Syntax**

show ip dhcp binding

**Command Mode**

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>EXEC Privilege</th>
</tr>
</thead>
</table>

**Default**

none

**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>

## show ip dhcp configuration

Display the DHCP configuration.

**Syntax**

show ip dhcp configuration [global | pool name]
### show ip dhcp conflict

Display the address conflict log.

**Syntax**

```
show ip dhcp conflict address
```

**Parameters**

- **address**: Display a particular conflict log entry.

**Command Mode**

EXEC Privilege

**Default**

none

**Command History**

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

### 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**
- all: Clear DHCP client statistics on all DHCP client-enabled interfaces on the switch.
- 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**
debug ip dhcp client events [interface type slot/port]

**Parameters**
- 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.
debug ip dhcp clients packets

Enable the display of log messages for all DHCP packets sent and received on DHCP client interfaces.

Syntax

```
debug ip dhcp clients packets [interface type slot/port]
```

Parameters

```
interface type slot/port
```

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`.

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

```
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`.

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

<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>
</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 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

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display DHCP client statistics on all DHCP client-enabled interfaces on the switch.</td>
</tr>
<tr>
<td>interface type</td>
<td>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.</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

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]
Commands to Configure Secure DHCP

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`

**arp inspection**

Enable dynamic ARP inspection (DAI) on a VLAN.

**Syntax**

```
arp inspection
```

**Command Modes**

```
INTERFACE VLAN
```

**Default**

Disabled

**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>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping vlan</td>
<td>Enables DHCP snooping on one or more VLANs.</td>
</tr>
</tbody>
</table>

### 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

- 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 mac-address vlan-id vlan-id ip ip-address interface type slot/port lease time 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 (Not available on E-Series).

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**

```
[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.

**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]
```

202 | Dynamic Host Configuration Protocol (DHCP)
Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding</td>
<td>Display the binding table.</td>
</tr>
<tr>
<td>source-address-validation</td>
<td>Display the interfaces configured with IP Source Guard.</td>
</tr>
</tbody>
</table>

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.

**ip dhcp snooping verify mac-address**
Validate a DHCP packet’s source hardware address against the client hardware address field (CHADDR) in the payload.

Syntax

```
[no] ip dhcp snooping verify mac-address
```

Command Modes

- CONFIGURATION

Default

- Disabled

Command History

```
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module
```
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>Parameters</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

Command History

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc-map-value</td>
<td>Enter the FC-MAP value used by FIP snooping.</td>
</tr>
<tr>
<td></td>
<td>The valid values are from 0EFC00 to 0EFCFF.</td>
</tr>
</tbody>
</table>

Defaults
0xEFC00

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

Example

Figure 11-1. 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

Example

Figure 11-2. 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
```
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**

<table>
<thead>
<tr>
<th>fcf-mac-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the MAC address of the FCF to be displayed.</td>
</tr>
</tbody>
</table>

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

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

**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 11-2 lists the show fip-snooping fcf command field descriptions.

**Table 11-2. 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**

```
FTOS#show fip-snooping sessions
Enode MAC    Enode Intf   FCF MAC       FCF Intf   VLAN
aa:bb:cc:00:00:00  Te 0/42  aa:bb:cd:00:00:00  Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42  aa:bb:cd:00:00:00  Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42  aa:bb:cd:00:00:00  Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42  aa:bb:cd:00:00:00  Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42  aa:bb:cd:00:00:00  Te 0/43  100
aa:bb:cc:00:00:00  Te 0/42  aa:bb:cd:00:00:00  Te 0/43  100

FCoE MAC       FC-ID       Port WWPN       Port WWNN
0e:fc:00:01:00:01  01:00:01  31:00:0e:fc:00:00:00:00  21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:02  01:00:02  41:00:0e:fc:00:00:00:00  21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:03  01:00:03  41:00:0e:fc:00:00:00:00  21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:04  01:00:04  41:00:0e:fc:00:00:00:00  21:00:0e:fc:00:00:00:00
0e:fc:00:01:00:05  01:00:05  41:00:0e:fc:00:00:00:00  21:00:0e:fc:00:00:00:00
```

Table 11-2. show fip-snooping fcf Command Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of ENodes</td>
<td>Number of ENodes connected to the FCF</td>
</tr>
<tr>
<td>FC-ID</td>
<td>Fibre Channel session ID assigned by the FCF.</td>
</tr>
</tbody>
</table>

Table 11-3 lists the `show fip-snooping sessions` command field descriptions.

Table 11-3. 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 11-5. show fip-snooping statistics Command Example

FTOS# show fip-snooping statistics interface vlan 100
Number of Vlan Requests :0
Number of Vlan Notifications :0
Number of Multicast Discovery Solicits :2
Number of Unicast Discovery Solicits :0
Number of FLOGI :2
Number of FDISC :16
Number of FLOGO :0
Number of Enode Keep Alive :9021
Number of VN Port Keep Alive :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts :2
Number of FLOGI Rejects :0
Number of FDISC Accepts :16
Number of FDISC Rejects :0
Number of FLOGO Accepts :0
Number of FLOGO Rejects :0
Number of CVL :0
Number of FCF Discovery Timeouts :0
Number of VN Port Session Timeouts :0
Number of Session failures due to Hardware Config :0
FTOS(conf)#

FTOS# show fip-snooping statistics int tengigabitethernet 0/11
Number of Vlan Requests :1
Number of Vlan Notifications :0
Number of Multicast Discovery Solicits :1
Number of Unicast Discovery Solicits :0
Number of FLOGI :1
Number of FDISC :16
Number of FLOGO :0
Number of Enode Keep Alive :4416
Number of VN Port Keep Alive :3136
Number of Multicast Discovery Advertisement :0
Number of Unicast Discovery Advertisement :0
Number of FLOGI Accepts :0
Number of FLOGI Rejects :0
Number of FDISC Accepts :0
Number of FDISC Rejects :0
Number of FLOGO Accepts :0
Number of FLOGO Rejects :0
Number of CVL :0
Number of FCF Discovery Timeouts :0
Number of VN Port Session Timeouts :0
Number of Session failures due to Hardware Config :0
Figure 11-6.  show fip-snooping statistics (port channel) Command Example

FTOS# show fip-snooping statistics interface port-channel 22
Number of Vlan Requests :0
Number of Vlan Notifications :2
Number of Multicast Discovery Solicits :0
Number of Unicast Discovery Solicits :0
Number of FLOGI :0
Number of FDISC :0
Number of FLOGO :0
Number of ENode Keep Alive :0
Number of VN Port Keep Alive :0
Number of Multicast Discovery Advertisement :4451
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts :2
Number of FLOGI Rejects :0
Number of FDISC Accepts :16
Number of FDISC Rejects :0
Number of FLOGO Accepts :0
Number of FLOGO Rejects :0
Number of CVL :0
Number of FCF Discovery Timeouts :0
Number of VN Port Session Timeouts :0
Number of Session failures due to Hardware Config :0

Table 11-4 lists the show fip-snooping statistics command field descriptions.

Table 11-4.  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 FDISC</td>
<td>Number of FIP-snooped FDISC request frames received on the interface</td>
</tr>
<tr>
<td>Number of FLOGO</td>
<td>Number of FIP-snooped FLOGO 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>
Table 11-4. show fip-snooping statistics Command Fields Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of FLOGI Accepts</td>
<td>Number of FIP FLOGI accept frames received on the interface</td>
</tr>
<tr>
<td>Number of FLOGI Rejects</td>
<td>Number of FIP FLOGI reject frames received on the interface</td>
</tr>
<tr>
<td>Number of FDISC Accepts</td>
<td>Number of FIP FDISC accept frames received on the interface</td>
</tr>
<tr>
<td>Number of FDISC Rejects</td>
<td>Number of FIP FDISC reject frames received on the interface</td>
</tr>
<tr>
<td>Number of FLOGO Accepts</td>
<td>Number of FIP FLOGO accept frames received on the interface</td>
</tr>
<tr>
<td>Number of FLOGO Rejects</td>
<td>Number of FIP FLOGO reject frames received on the interface</td>
</tr>
<tr>
<td>Number of CVLs</td>
<td>Number of FIP clear virtual link frames received on the interface</td>
</tr>
<tr>
<td>Number of FCF Discovery Timeouts</td>
<td>Number of FCF discovery timeouts that occurred on the interface</td>
</tr>
<tr>
<td>Number of VN Port Session Timeouts</td>
<td>Number of VN port session timeouts that occurred on the interface</td>
</tr>
<tr>
<td>Number of Session failures due to Hardware Config</td>
<td>Number of session failures due to hardware configuration that occurred 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

```
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 11-8. show fip-snooping vlan Command Example

    FTOS# show fip-snooping vlan
    * = Default VLAN
       VLAN    FC-MAP          FCFs    Enodes  Sessions
       ----    ------          ----    ------  --------
          *1      -               -       -       -
          100     0X0EFC00        1       2       17
```
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

```
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
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show gvrp statistics</td>
<td>Displays the GVRP statistics</td>
</tr>
</tbody>
</table>

**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>config</td>
<td>Enter the keyword <code>config</code> to enable debugging on the GVRP configuration.</td>
</tr>
<tr>
<td>event</td>
<td>Enter the keyword <code>event</code> to enable debugging on the JOIN/LEAVE events.</td>
</tr>
<tr>
<td>pdu</td>
<td>Enter the keyword <code>pdu</code> followed one of the following Interface 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: 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>
</tbody>
</table>

**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**

<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>
**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>join</strong></td>
<td>Enter the keyword <code>join</code> followed by the number of milliseconds to configure the join time. Range: 100 to 147483647 milliseconds Default: 200 milliseconds</td>
</tr>
<tr>
<td><strong>leave</strong></td>
<td>Enter the keyword <code>leave</code> followed by the number of milliseconds to configure the leave time. Range: 100 to 2147483647 milliseconds Default: 600 milliseconds</td>
</tr>
<tr>
<td><strong>leave-all</strong></td>
<td>Enter the keyword <code>leave-all</code> followed by the number of milliseconds to configure the leave-all time. Range: 100 to 2147483647 milliseconds Default: 1000 milliseconds</td>
</tr>
</tbody>
</table>

**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 reregistration 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**

- `fixed`
  - Enter the keyword `fixed` followed by the VLAN range in a comma separated VLAN ID set.

- `normal`
  - Enter the keyword `normal` followed by the VLAN range in a comma separated VLAN ID set.
  - This is the default

- `forbidden`
  - Enter the keyword `forbidden` followed by the VLAN range in a comma separated VLAN ID set.

**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.
**protocol gvrp**

Access GVRP protocol — (config-gvrp)#.

**Syntax**

```
protocol gvrp
```

**Defaults**

Disabled

**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>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>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**

<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>

**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**

<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>
**Example**

**Figure 12-1. show garp timers Command Example**

<table>
<thead>
<tr>
<th>FTOS#show garp timers</th>
</tr>
</thead>
<tbody>
<tr>
<td>GARP Timers Value (milliseconds)</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Join Timer 200</td>
</tr>
<tr>
<td>Leave Timer 600</td>
</tr>
<tr>
<td>LeaveAll Timer 10000</td>
</tr>
<tr>
<td>FTOS#</td>
</tr>
</tbody>
</table>

**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. |

<table>
<thead>
<tr>
<th>interface</th>
<th>(OPTIONAL) Enter the following keywords and slot/port or number information:</th>
</tr>
</thead>
<tbody>
<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>
</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**

**Figure 12-2. show gvrp brief Command Example**

```
R3#show gvrp brief
GVRP Feature is currently enabled.

Port GVRP Status Edge-Port
--- --------------- ----
Te 3/0 Disabled No
Te 3/1 Disabled No
Te 3/2 Enabled No
Te 3/3 Disabled No
Te 3/4 Disabled No
Te 3/5 Disabled No
Te 3/6 Disabled No
Te 3/7 Disabled No
Te 3/8 Disabled No
R3#show gvrp brief
```

**Usage Information**

If no ports are GVRP participants, the message output changes from:

GVRP Participants running on `<port_list>`
GARP VLAN Registration (GVRP)

Related Commands

- show gvrp statistics: Displays the GVRP statistics.

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

```
Figure 12-3. show gvrp statistics Command Example

FTOS#show gvrp statistics int tengig 1/0
Join Empty Received: 0
Join In Received: 0
Empty Received: 0
LeaveIn 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

show vlan

Command Modes

- EXEC
- EXEC Privilege

Command History

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

Example

Figure 12-4.  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 Active
G 10 Active
learned vlan
FTOS#
Internet Group Management Protocol (IGMP)

IGMP Snooping Commands

The Dell Force10 operating software (FTOS) supports internet group management protocol (IGMP) snooping version 2 and 3 on all Dell Force10 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**

```plaintext
ip igmp access-group access-list
```

To remove the feature, use the `no ip igmp access-group access-list` command.

**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**

```plaintext
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**

```
ip igmp querier-timeout seconds
```

To return to the default value, enter `no ip igmp querier-timeout`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Enter the number of seconds the router must wait to become the new querier.</td>
</tr>
<tr>
<td></td>
<td>Default: 125 seconds</td>
</tr>
<tr>
<td></td>
<td>Range: 60 to 300</td>
</tr>
</tbody>
</table>

**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**

```
ip igmp query-interval seconds
```

To return to the default values, enter `no ip igmp query-interval`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Enter the number of seconds between queries sent out.</td>
</tr>
<tr>
<td></td>
<td>Default: 60 seconds</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 18000</td>
</tr>
</tbody>
</table>

**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**

```
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
```

To disable IGMP snooping, enter no ip igmp snooping enable command.

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.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no shutdown</td>
<td>Activates an interface.</td>
</tr>
</tbody>
</table>

## ip igmp snooping fast-leave

Enable IGMP snooping fast leave for this VLAN.

**Syntax**

```plaintext
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**

```plaintext
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 ip 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-n)

**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 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-)

**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 13-1. 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
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.

- **vrf instance** (Optional): Enter the keyword `vrf instance` 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 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 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**

```
Example Figure 14-2. 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}
```
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:

**Figure 14-3. 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.
```

For details on using XFP ports with CX4 cables, refer to your MXL Switch hardware guide.

**Figure 14-4** shows a successful CX4 cable length configuration.

**Figure 14-4. Example of CX4 Cable Length Configuration**

```
FTOS(config)#interface tengigabitethernet 0/52
FTOS(conf-if-0/52)#cx4-cable-length long
FTOS(conf-if-0/52)#show config
!
interface TenGigabitEthernet 0/51
  no ip address
  cx4-cable-length long
  shutdown
FTOS(conf-if-0/52)#exit
```

**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` command syntax.

---

**Example**

```
FTOS(config)#interface tengigabitethernet 0/52
FTOS(conf-if-0/52)#cx4-cable-length long
FTOS(conf-if-0/52)#show config
!
interface TenGigabitEthernet 0/51
  no ip address
  cx4-cable-length long
  shutdown
FTOS(conf-if-0/52)#exit
```
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.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>half-life</code></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><code>reuse-threshold</code></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><code>suppress-threshold</code></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><code>max-suppress-time</code></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

INTERFACEx (conf-if-)

### Command History

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

### Example

**Figure 14-5. dampening Command Example**

```
FTOS(config-if-tengig-3/2)#dampening 20 800 4500 120
FTOS(config-if-tengig-3/2)#
```

### Related Commands

- `clear dampening` Clears the dampening counters on all the interfaces or just the specified interface.
- `show interfaces dampening` Displays interface dampening information.
### 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.

**Defaults**

No description is defined.

**Command Modes**

`INTERFACE`

**Command History**

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

**Usage Information**

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>speed (for 1000/10000/auto interfaces)</td>
<td>Sets the speed on the Base-T Ethernet interface.</td>
</tr>
<tr>
<td>negotiation auto</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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx on</td>
<td>Enter the keywords <code>rx on</code> to process the received flow control frames on this port. This is the default value for the receive side.</td>
</tr>
<tr>
<td>rx off</td>
<td>Enter the keywords <code>rx off</code> to ignore the received flow control frames on this port.</td>
</tr>
<tr>
<td>tx on</td>
<td>Enter the keywords <code>tx on</code> 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.</td>
</tr>
<tr>
<td>tx off</td>
<td>Enter the keywords <code>tx off</code> so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.</td>
</tr>
</tbody>
</table>

Defaults

```
rx off tx off
```

Command Modes

```
INTERFACE
```

Command History

Version 8.3.16.1 Introduced on 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

- Do not enable `tx` pause when buffer carving is enabled. Consult Dell Force10 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 14-6. 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 14-1 lists how FTOS negotiates the flow control values between two Dell Force10 chassis connected back-to-back using 10G copper ports.

<table>
<thead>
<tr>
<th>Configured LocRxConf</th>
<th>Configured LocTxConf</th>
<th>Configured RemoteRxConf</th>
<th>Configured RemoteTxConf</th>
<th>Negotiated LocNegRx</th>
<th>Negotiated LocNegTx</th>
<th>Negotiated RemNegRx</th>
<th>Negotiated RemNegTx</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>off</td>
<td>off</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>off</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
</tbody>
</table>

Table 14-1. Negotiated Flow Control Values
interfaces

interface

Configure a physical interface on the switch.

**Syntax**

```plaintext
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 MXL 10/40GbE Switch IO Module

**Example**

```plaintext
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 MXL 10/40GbE Switch IO Module

Example

Figure 14-8. 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 MXL 10/40GbE Switch IO Module

Example

Figure 14-9. 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><code>management route</code></td>
<td>Configure a static route that points to the Management interface or a forwarding router.</td>
</tr>
<tr>
<td><code>duplex (1000/10000 Interfaces)</code></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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter zero (0) as the Null interface number.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured; `number = 0`

**Command Modes**

CONFIGURATION

**Command History**

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

**Example**

```plaintext
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Configures a physical interface.</td>
</tr>
<tr>
<td><code>interface loopback</code></td>
<td>Configures a Loopback 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>ip unreachables</code></td>
<td>Enables generation of ICMP unreachable messages.</td>
</tr>
</tbody>
</table>

### 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.

Example

**Figure 14-11. Bulk Configuration Warning Message**

```
FTOS(conf)#interface range so 2/0 - 1 , te 10/0 , tengig 3/0 , fa 0/0
% Warning: Non-existing ports (not configured) are ignored by
```

**Example**

**Figure 14-12. Interface Range prompt with Multiple Ports**

```
FTOS(conf)#interface range tengig 2/0 - 23 , tengig 2/1 - 10
FTOS(conf-if-range-tengig-2/0-23#)
```
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.

Figure 14-14 is an example of a single range bulk configuration.

### Example

**Figure 14-13. 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 14-14. Single Range Bulk Configuration**

```
FTOS(conf)# interface range tengigabitethernet 5/1 - 23
FTOS(conf-if-range)# no shutdown
FTOS(conf-if-range)#
```

**Figure 14-15 shows how to use commas to add different interface types to the range enabling all Ten Gigabit Ethernet interfaces in the range 5/1 to 5/23 and both Ten Gigabit Ethernet interfaces 1/1 and 1/2.**

### Example

**Figure 14-15. 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)#
```

**Figure 14-16 shows how to use commas to add VLAN and port-channel interfaces to the range.**

### Example

**Figure 14-16. 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

```
define interface range macro name interface , interface , ...
```

## Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>Enter up to 16 characters for the macro name.</td>
</tr>
<tr>
<td><strong>interface , interface ,</strong></td>
<td>Enter the <code>interface</code> 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, <code>interface range tengigabitethernet 0/1 - 5</code> is valid; <code>interface range tengigabitethernet 0/1-5</code> 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

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

## Example

Figure 14-17. define interface-range macro Command Example

```
FTOS(conf)# define interface-range test tengigabitethernet 0/0 - 3 , tengigabitethernet 5/0 - 47 , tengigabitethernet 13/0 - 89
FTOS# show running-config | grep define
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 14-17 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><code>interface range</code></td>
<td>Configures a range of command (bulk configuration)</td>
</tr>
<tr>
<td><code>interface range macro name</code></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 MXL 10/40GbE Switch IO Module

**Usage Information**

- Figure 14-18 runs the macro named `test` that was defined earlier.

**Example**

**Figure 14-18. 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 MXL 10/40GbE Switch IO Module

**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).

**intf-type cr4 autoneg**
Set the interface type as CR4 with auto-negotiation enabled.

**Syntax**

```
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 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>
<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>

**keepalive**
Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

**Syntax**

```
keepalive [seconds]
```

To stop sending keepalive packets, use the **no keepalive** command.
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**

- **interface**
  (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For the management port, enter the keyword `managementethernet` followed by the slot (0-1) and the port (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.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

**Usage Information**

The delta column displays changes since the last screen refresh.
Example

**Figure 14-20. monitor Command Example of a Single Interface**

```
Example Figure 14-20. monitor Command Example of a Single Interface

systest-3   Monitor time: 00:00:06   Refresh Intvl.: 2s   Time: 03:26:26
Interface: tengig 0/3, Enabled, Link is Up, Linespeed is 1000 Mbit

Traffic statistics:          Current   Rate     Delta
Input bytes:                9069828   43 Bps    86
Output bytes:               606915800 43 Bps    86
Input packets:              54001     0 pps     1
Output packets:             9401589   0 pps     1
64B packets:                67        0 pps     0
Over 64B packets:           49166     0 pps     1
Over 127B packets:          350       0 pps     0
Over 255B packets:          1351      0 pps     0
Over 511B packets:          286       0 pps     0
Over 1023B packets:         2781      0 pps     0
Error statistics:
Input underruns:            0         0 pps     0
Input giants:               0         0 pps     0
Input throttles:             0         0 pps     0
Input CRC:                  0         0 pps     0
Input IP checksum:          0         0 pps     0
Input overrun:              0         0 pps     0
Output underruns:           0         0 pps     0
Output throttles:           0         0 pps     0
Error statistics:
Input underruns:            0         0 pps     0
Input giants:               0         0 pps     0
Input throttles:             0         0 pps     0
Input CRC:                  0         0 pps     0
Input IP checksum:          0         0 pps     0
Input overrun:              0         0 pps     0
Output underruns:           0         0 pps     0
Output throttles:           0         0 pps     0

m - Change mode
l - Change view to next interface
T - Increase screen refresh rate
T - Increase refresh interval
a - Change view to previous interface
q - Quit
```

**Table 14-2. monitor Command Menu Options**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>systest-3</td>
<td>Displays the host name assigned to the system.</td>
</tr>
<tr>
<td>monitor time</td>
<td>Displays the amount of time since the monitor interface command was entered.</td>
</tr>
<tr>
<td>time</td>
<td>Displays the amount of time the chassis is up (since last reboot).</td>
</tr>
<tr>
<td>m</td>
<td>Change the view from a single interface to all interfaces on the stack unit or visa-versa.</td>
</tr>
<tr>
<td>c</td>
<td>Refresh the view.</td>
</tr>
<tr>
<td>b</td>
<td>Change the counters displayed from Packets on the interface to Bytes.</td>
</tr>
<tr>
<td>r</td>
<td>Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.</td>
</tr>
<tr>
<td>l</td>
<td>Change the view to next interface on the stack unit, or if in the stack unit mode, the next stack unit in the chassis.</td>
</tr>
<tr>
<td>a</td>
<td>Change the view to the previous interface on the stack unit, or if the stack unit mode, the previous stack unit in the chassis.</td>
</tr>
<tr>
<td>T</td>
<td>Increase the screen refresh rate.</td>
</tr>
<tr>
<td>t</td>
<td>Decrease the screen refresh rate.</td>
</tr>
<tr>
<td>q</td>
<td>Return to the CLI prompt.</td>
</tr>
</tbody>
</table>

**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.
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 14-3. 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 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 14-21. negotiation auto Master/Slave Example

FTOS(conf)# int tengig 0/0
FTOS(conf-if)#neg auto
FTOS(conf-if-autoneg)# ?
end Exit from configuration mode
exit Exit from autoneg configuration mode
mode Specify autoneg mode
no Negate a command or set its defaults
show Show autoneg configuration information
FTOS(conf-if-autoneg)#mode ?
forced-master Force port to master mode
forced-slave Force port to slave mode
FTOS(conf-if-autoneg)#

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>
<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 14-23. 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 14-23 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 14-24. Display the Tagged Hybrid Interface**

```plaintext
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)#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 14-25** 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 14-25. Unconfigure the hybrid port**

```plaintext
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>show interfaces switchport</td>
<td>Displays the configuration of switchport (Layer 2) interfaces on the switch.</td>
</tr>
<tr>
<td>vlan-stack trunk</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 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 MXL 10/40GbE Switch IO Module

**Example**

```
FTOS(conf-if)#show conf
!
interface TenGigabitEthernet 1/7
  no ip address
  switchport
  no shutdown
FTOS(conf-if)#
```

**show config (from INTERFACE RANGE mode)**

Display the bulk configured interfaces (interface range).

**Syntax**

`show config`

**Command Modes**

CONFIGURATION INTERFACE (conf-if-range)
**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 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 Force10 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 14-28. 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 14-5. Lines in show interfaces Command Example**

<table>
<thead>
<tr>
<th><strong>Line</strong></th>
<th><strong>Description</strong></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 <strong>show interfaces</strong> 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 14-5. Lines in show interfaces Command Example

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Statistics:</strong></td>
<td>Displays all the input statistics including:</td>
</tr>
<tr>
<td></td>
<td>- Number of packets and bytes into the interface</td>
</tr>
<tr>
<td></td>
<td>- Number of packets with IP headers and VLAN tagged headers.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Packet size and the number of those packets inbound to the interface</td>
</tr>
<tr>
<td></td>
<td>- Number of symbol errors, runts, giants, and throttles packets:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>symbol errors = number packets containing bad data. That is, the port MAC detected a physical coding error in the packet.</td>
</tr>
<tr>
<td></td>
<td>runts = number of packets that are less than 64B</td>
</tr>
<tr>
<td></td>
<td>giants = packets that are greater than the MTU size</td>
</tr>
<tr>
<td></td>
<td>throttles = packets containing PAUSE frames</td>
</tr>
<tr>
<td></td>
<td>- Number of CRC, IP Checksum, overrun, and discarded packets:</td>
</tr>
<tr>
<td></td>
<td>CRC = packets with CRC/FCS errors</td>
</tr>
<tr>
<td></td>
<td>IP Checksum = packets with IP Checksum errors</td>
</tr>
<tr>
<td></td>
<td>overrun = number of packets discarded due to FIFO overrun conditions</td>
</tr>
<tr>
<td></td>
<td>discarded = the sum of input symbol errors, runts, giants, CRC, IP Checksum, and overrun packets discarded without any processing</td>
</tr>
<tr>
<td><strong>Output Statistics:</strong></td>
<td>Displays output statistics sent out of the interface including:</td>
</tr>
<tr>
<td></td>
<td>- Number of packets, bytes and underruns out of the interface</td>
</tr>
<tr>
<td></td>
<td>packets = total number of packets</td>
</tr>
<tr>
<td></td>
<td>bytes = total number of bytes</td>
</tr>
<tr>
<td></td>
<td>underruns = number of packets with FIFO underrun conditions</td>
</tr>
<tr>
<td></td>
<td>- Number of Multicast, Broadcast and Unicast packets:</td>
</tr>
<tr>
<td></td>
<td>Multicasts = number of MAC multicast packets</td>
</tr>
<tr>
<td></td>
<td>Broadcasts = number of MAC broadcast packets</td>
</tr>
<tr>
<td></td>
<td>Unicasts = number of MAC unicast packets</td>
</tr>
<tr>
<td></td>
<td>- Number of throttles and discards packets:</td>
</tr>
<tr>
<td></td>
<td>throttles = packets containing PAUSE frames</td>
</tr>
<tr>
<td></td>
<td>discarded = number of packets discarded without any processing</td>
</tr>
<tr>
<td><strong>Rate information...</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Time since...</strong></td>
<td>Elapsed time since the last interface status change (hh:mm:ss format).</td>
</tr>
</tbody>
</table>
Example

**Figure 14-29. 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, 8496 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 FTOS#
```

**Figure 14-30. 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, 3442163 multicast
   Received 0 errors, 0 discarded
   Output 4627 packets, 814226 bytes, 0 multicast
   Output 0 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.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces configured</td>
<td>Displays any interface with a non-default configuration.</td>
</tr>
<tr>
<td>show interfaces stack-unit</td>
<td>Displays information on all interfaces on a specific stack unit.</td>
</tr>
<tr>
<td>strict-priority unicast</td>
<td>Displays information of either rate limiting or rate policing on the interface.</td>
</tr>
<tr>
<td>show interfaces switchport</td>
<td>Displays Layer 2 information about the interfaces.</td>
</tr>
<tr>
<td>show inventory</td>
<td>Displays the MXL switch type, components (including media), FTOS version including hardware identification numbers and configured protocols.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays Layer 3 information about the interfaces.</td>
</tr>
<tr>
<td>show memory</td>
<td>Displays the stack unit(s) status.</td>
</tr>
<tr>
<td>show range</td>
<td>Displays all interfaces configured using the interface range command.</td>
</tr>
</tbody>
</table>

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 MXL 10/40GbE Switch IO Module

Example

```
Figure 14-31. show interfaces configured Command 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Displays information on a specific physical interface or virtual interface.</td>
</tr>
</tbody>
</table>
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 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**

- Version 8.3.16.1 Introduced on 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 14-6. 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 stack-unit

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**

- Introduced on 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 5d5h24m
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 0.00 Mb/s, 0 packets/sec, 0.00% of line-rate
  Output 0.00 Mb/s, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 5d5h24m
!-----------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 MXL 10/40GbE Switch IO Module

Example

```
FTOS#show interface status

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Status</th>
<th>Speed</th>
<th>Duplex</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te 0/1</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/2</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/3</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/4</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/5</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/6</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/7</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/8</td>
<td>Up</td>
<td>10000 Mbit</td>
<td>Full</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Te 0/9</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/10</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/11</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/12</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/13</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/14</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/15</td>
<td>Down</td>
<td>Auto</td>
<td>Auto</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Te 0/16</td>
<td>Up</td>
<td>10000 Mbit</td>
<td>Full</td>
<td>--</td>
<td></td>
</tr>
</tbody>
</table>

FTOS#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Displays information on a specific physical interface or virtual interface.</td>
</tr>
</tbody>
</table>
**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 MXL 10/40GbE Switch IO Module

**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 tagged

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 14-7. 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configures a physical interface on the switch.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays Layer 3 information about the interfaces.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays information on a specific physical interface or virtual interface.</td>
</tr>
<tr>
<td>show interfaces transceiver</td>
<td>Displays the physical status and operational status of an installed transceiver. The output also displays the transceiver’s serial number.</td>
</tr>
</tbody>
</table>
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 <code>tengigabitethernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td>fortyGigE</td>
<td>For a 40G interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</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**

See Figure 14-37 for an command example and see Table 14-8 for a description of the output fields.
Example

Figure 14-37. show interfaces tengigabitethernet transceiver Command 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 Transciever 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) 10m = 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 = 95.000°C
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 = -25.000°C
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 Temperature = 39.930°C
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 14-8. Diagnostic Data in show interfaces transceiver

<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”</td>
</tr>
<tr>
<td></td>
<td>(Receiver optical modulation amplitude).</td>
</tr>
<tr>
<td>Temp High Alarm threshold</td>
<td>Factory-defined setting, typically in Centigrade. Value differs between SFPs</td>
</tr>
<tr>
<td></td>
<td>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/</td>
</tr>
<tr>
<td></td>
<td>warning thresholds, then the temperature high alarm/warning flag is set to</td>
</tr>
<tr>
<td></td>
<td>true.</td>
</tr>
<tr>
<td>Voltage</td>
<td>Current voltage of the sfps. If this voltage crosses voltage high alarm/warning</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>thresholds, then the tx bias high alarm/warning flag is set to true. If it</td>
</tr>
<tr>
<td></td>
<td>falls below the low alarm/warning thresholds, then the tx bias low alarm/warning</td>
</tr>
<tr>
<td></td>
<td>flag is set to true.</td>
</tr>
</tbody>
</table>
Table 14-8. 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>
Table 14-8. Diagnostic Data in show interfaces transceiver (continued)

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Power High Warning Flag</td>
<td>This can be either true or false, depending on the Current Tx power value</td>
</tr>
<tr>
<td>Rx Power High Warning Flag</td>
<td>This can be either true or false, depending on the Current Tx power value</td>
</tr>
<tr>
<td>Temperature Low Warning Flag</td>
<td>This can be either true or false, depending on the Current Temperature</td>
</tr>
<tr>
<td>Voltage Low Warning Flag</td>
<td>This can be either true or false, depending on the Current voltage value</td>
</tr>
<tr>
<td>Tx Bias Low Warning Flag</td>
<td>This can be either true or false, depending on the present Tx bias current</td>
</tr>
<tr>
<td>Tx Power Low Warning Flag</td>
<td>This can be either true or false, depending on the Current Tx power value</td>
</tr>
<tr>
<td>Rx Power Low Warning Flag</td>
<td>This can be either true or false, depending on the Current Rx power value</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 inventory` Displays the switch type, FTOS version including hardware identification numbers and configured protocols.

**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 MXL 10/40GbE Switch IO Module

**Example**

**Figure 14-38. 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.
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 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

interface port-channel Creates a port channel interface.

interface vlan Creates a VLAN.

show ip interface Displays the interface routing status. Add the keyword brief to display a table of interfaces and their status.

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}

Parameters

To return to the default setting, use the no speed {1000 | 10000 | auto} command.

<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/</td>
</tr>
<tr>
<td></td>
<td>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.
- **number**
  - 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 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 14-9. 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 17, 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 MXL 10/40GbE Switch IO Module
Usage Information

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

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 MXL 10/40GbE Switch IO Module

Example

    Figure 14-40.  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.
**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**

- **number**: Enter the number of links in a LAG that must be in “oper up” status.
  - Range: 1 to 16
  - Default: 1

**Defaults**

1

**Command Modes**

INTERFACE

**Command History**

- **Version 8.3.16.1**: Introduced on 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
```

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

- **Version 8.3.16.1**: Introduced on 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*. 
show config
Display the current configuration of the selected LAG.

Syntax
show config

Command Modes
INTERFACE PORTCHANNEL

Example
Figure 14-41. 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 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-number</td>
<td>For a Port Channel interface, enter the keyword port-channel followed by a</td>
</tr>
<tr>
<td></td>
<td>number:</td>
</tr>
<tr>
<td></td>
<td>Range: 1-128</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to display only the port channel</td>
</tr>
<tr>
<td></td>
<td>number, the state of the port channel, and the number of interfaces in the</td>
</tr>
<tr>
<td></td>
<td>port channel.</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 14-42. show interfaces port-channel Command Example (EtherScale)**

FTOS#show interfaces port-channel
Port-channel 1 is down, line protocol is down
Hardware address is 00:1e:c9:f1:00:05, Current address is 00:1e:c9:f1:00:05
Interface index is 1107755009
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :lag1001ec9f10005
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Members in this channel:
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 03:28:00
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

**Table 14-10. 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 14-10.  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 14-43.  show interfaces port-channel brief Command Example

FTOS#show int po 1 brief
Codes: L - LACP Port-channel

<table>
<thead>
<tr>
<th>LAG</th>
<th>Mode</th>
<th>Status</th>
<th>Uptime</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>L3</td>
<td>down</td>
<td>00:00:00</td>
<td>Te 0/16 (Down)</td>
</tr>
</tbody>
</table>

FTOS#

Table 14-11.  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). In Layer 2 port channels, an * (asterisk) indicates which interface is the primary port of the port channel. The primary port sends out interface PDU. 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
```

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 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
```
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 MXL 10/40GbE Switch IO Module

Example

**Figure 14-44. show tdr tengigabitethernet Command Example**

```
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 14-12. 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**

d 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 14-45. 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.
```
ip udp-broadcast-address
Configure an IP UDP address for broadcast.

Syntax
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 MXL 10/40GbE Switch IO Module

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

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
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. |

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 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 14-46. 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 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>
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**

- **ip-address**: Enter an IP address in dotted decimal format.
- **mac-address**: Enter a MAC address in nnnn.nnnn.nnnn format.
- **interface**: 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 0-1 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**

- Introduced on MXL 10/40GbE Switch IO Module

**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
```

---

**IPv4 Routing**
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

- 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

- `minutes`: To return to the default value, use the no arp timeout command.
  - `seconds`: Enter the number of minutes.
    - Range: 0 to 35790
    - Default: 240 minutes

Defaults

- 240 minutes (4 hours)

Command Modes

- INTERFACE

Command History

- 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**

<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 the Management interface, enter the keyword ManagementEthernet</td>
</tr>
<tr>
<td></td>
<td>followed by the slot/port information. The slot range is 0 and the port</td>
</tr>
<tr>
<td></td>
<td>range is 0.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword port-channel followed</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE</td>
</tr>
<tr>
<td></td>
<td>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>ip ip-address</td>
<td>(OPTIONAL) Enter the keyword ip followed by the IP address of the ARP entry</td>
</tr>
<tr>
<td></td>
<td>you wish to clear.</td>
</tr>
<tr>
<td>no-refresh</td>
<td>(OPTIONAL) Enter the keyword no-refresh to delete the ARP entry from CAM.</td>
</tr>
<tr>
<td></td>
<td>Or use this option with interface or ip ip-address to specify which</td>
</tr>
<tr>
<td></td>
<td>dynamic ARP entries you want to delete.</td>
</tr>
</tbody>
</table>

**Note:** Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and re-installed in CAM. Use this option with extreme caution.

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Enter the name of the host to delete.</td>
</tr>
<tr>
<td></td>
<td>Enter * to delete all host table entries.</td>
</tr>
</tbody>
</table>

**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  

unit-number
Enter the stack-unit number.
Range: 0 to 5

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  
show ip fib stack-unit  Shows the FIB entries.

clear ip route
Clear one or all routes in the routing table.

Syntax  clear ip route {* | ip-address mask}

Parameters  

*  Enter an asterisk (*) to clear all learned IP routes.

ip-address mask  Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.

Command Mode  EXEC Privilege

Command History  

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

Related Commands  
ip route  Assigns an IP route to the switch.
show ip route  Views the routing table.
show ip route summary  Views a summary of the routing table.

clear tcp statistics
Clear TCP counters.

Syntax  clear tcp statistics
**debug arp**

View information on ARP transactions.

**Syntax**

```
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**

```
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 15-1. 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
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP 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 = 113.3.3.17
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 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 = 113.3.3.17
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 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 = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2

FTOS#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip helper-address</td>
<td>Specifies the destination broadcast or host address for the DHCP server request.</td>
</tr>
<tr>
<td>ip helper-address hop-count disable</td>
<td>Disables the hop-count increment for the DHCP relay agent.</td>
</tr>
</tbody>
</table>

debug ip icmp

View information on the internal control message protocol (ICMP).

Syntax

debug ip icmp [interface] [count value]

To disable debugging, use the no debug ip icmp command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 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  
- Default: Infinity |

Command Modes

EXEC Privilege

Command History

Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
**debug ip packet**

View a log of IP packets sent and received.

**Syntax**

dump 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 fortygigethernet 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
**Example**  
**Figure 15-3. debug ip packet Command Example (Partial)**

| IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending  
TCP src=23, dst=40869, seq=2112994894, ack=606901739, win=8191 ACK PUSH  
IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd  
TCP src=0, dst=0, seq=0, ack=0, win=0  
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226, sending  
TCP src=23, dst=40869, seq=2112994896, ack=606901739, win=8192 ACK PUSH  
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd  
UDP src=0, dst=0  
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment  
IP Fragment, Ident = 4741, fragment offset = 0  
ICMP type=0, code=0  
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment  
IP Fragment, Ident = 4741, fragment offset = 1480  
IP: s=40.40.40.40 (local), d=224.0.0.5 (Te 4/11), len 64, sending broad/multicast proto=89  
IP: s=40.40.40.40 (local), d=224.0.0.6 (Te 4/11), len 28, sending broad/multicast proto=2  
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable  
ICMP type=8, code=0  
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable  
ICMP type=8, code=0

<p>| <strong>Table 15-1. debug ip packet Command Example Fields</strong> |</p>
<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 15-4). 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 0 to 255
- Internet Control Message Protocol* icmp
  * but not the ICMP message type (0-255)
- Any Internet Protocol ip
- Transmission Control Protocol* tcp
  * but not on the rst, syn, or urg bit
- User Datagram Protocol udp

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 15-4).

Example

```
Figure 15-4.  debug ip packet access-group Command Errors

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 [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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip domain-name</td>
<td>Specifies a DNS server.</td>
</tr>
</tbody>
</table>
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

<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

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 domain-name

Configure one domain name for the switch.

Syntax

```
ip domain-name name
```

To remove the domain name, use the `no ip domain-name` command.

Parameters

- `name`  
  Enter one domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults

Not configured.

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

You can only configure one domain name with the `ip domain-name` command. To configure more than one domain name, configure the `ip domain-list` command up to 6 times.

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 domainlookup` command.

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 domain-list</td>
<td>Configures additional names.</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
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter an IP address in dotted decimal format (A.B.C.D).</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

**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
```

**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...** | (OPTIONAL) Enter up 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. |
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

show ip route Views the switch routing table.
ip unreachable

Enable the generation of Internet Control Message Protocol (ICMP) unreachable messages.

Syntax

ip unreachable

To disable the generation of ICMP messages, use the no ip unreachable command.

Defaults

Disabled

Command Modes

INTERFACE

Command History

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address/mask</td>
<td>Enter an IPv4 address (A.B.C.D) followed by the prefix-length for the IP address of the management interface.</td>
</tr>
<tr>
<td>forwarding-router-address</td>
<td>Enter an IPv4 address of a forwarding router.</td>
</tr>
<tr>
<td>managementethernet</td>
<td>Enter the keyword managementethernet for the Management interface.</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

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).
- **macaddress mac-address mask** (OPTIONAL) Enter the keyword `macaddress` followed by a MAC address in nn:nn:nn:nn:nn:nn format. Enter the optional MAC address mask in nn:nn:nn:nn:nn format also.
- **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 15-5 shows two VLANs that are associated with a private VLAN (PVLAN) (refer to Chapter 23, Private VLAN (PVLAN)).

### Example

**Figure 15-5. show arp Command Example (Partial)**

```
FTOS#show arp

Protocol Address        Age(min) Hardware Address Interface VLAN
---------------------- -------- -------------------------- ------- ----- 
Internet              10.11.8.6   167 00:01:e9:45:00:03    Ma 0/0    -
Internet              10.11.68.14 124 00:01:e9:45:00:03    Ma 0/0    -
Internet              10.11.209.254 0   00:01:e9:45:00:03    Ma 0/0    -
```
Figure 15-6.  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>-</td>
<td>Vl 10 pv 200</td>
<td>CP</td>
</tr>
<tr>
<td>Internet</td>
<td>5.5.5.10</td>
<td>-</td>
<td>00:01:e8:44:99:55</td>
<td>-</td>
<td>Vl 10</td>
<td>CP</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>-</td>
<td>CP</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>-</td>
<td>CP</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>-</td>
<td>CP</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>-</td>
<td>CP</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>-</td>
<td>CP</td>
</tr>
</tbody>
</table>

Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN.

Line 2 shows primary VLAN 10.

Table 15-2.  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 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 15-7.  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 15-3.  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 15-8. show hosts Command Example

<table>
<thead>
<tr>
<th>Host</th>
<th>Flags</th>
<th>TTL</th>
<th>Type</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ks</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>2.2.2.2</td>
</tr>
<tr>
<td>4200-1</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.68.69.2</td>
</tr>
<tr>
<td>1230-3</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.68.99.2</td>
</tr>
<tr>
<td>ZZr</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.71.18.2</td>
</tr>
<tr>
<td>Z10-3</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.71.23.1</td>
</tr>
</tbody>
</table>

FTOS#

Table 15-4. 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 uses static mappings</td>
<td>States if DNS is enabled on the system.</td>
</tr>
<tr>
<td>If DNS is enabled, the Name/Address lookup is domain service.</td>
<td></td>
</tr>
<tr>
<td>If DNS is not enabled, the Name/Address lookup is static mapping.</td>
<td></td>
</tr>
<tr>
<td>Name servers are not set</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**: (OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only.
- **longer-prefixes**: 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
Table 15-5. 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 15-10. show ip cam stack-unit ecmp-group detail Command Example

```
FTOS#show ip cam stack-unit 0 po 0 ecmp-group detail

Destination     EC CG V C  VId     Mac-Addr          Port        ECMP Group-Index
-----------------  -- -- - - ----- ----------------- ---------------  ---------------
1.1.1.2           0  0 1 0     0 00:01:e8:8a:d6:58   0004 Te 0/3          -
2.1.1.2           0  0 1 0     0 00:01:e8:8a:d6:58   0009 Te 0/8          -
1.1.1.1           0  0 1 1     0 00:00:00:00:00:00:00:00:00 3f01 CP            -
2.1.1.1           0  0 1 1     0 00:00:00:00:00:00:00:00:00 3f01 CP            -
1.1.1.0            0  0 1 1 0 00:00:00:00:00:00:00:00:00 3f01 CP            -
2.1.1.0            0  0 1 1 0 00:00:00:00:00:00:00:00:00 3f01 CP            -
100.1.1.0          1  0 1 0 0 00:01:e8:8a:d6:58   0004 Te 0/3          0
100.1.1.0          1  0 1 0 0 00:01:e8:8a:d6:58   0009 Te 0/8          0
0.0.0.0             0  0 1 1 0 00:00:00:00:00:00:00:00:00 3f01 CP            -
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-5</td>
<td>Enter the stack unit ID, from 0 to 5.</td>
</tr>
<tr>
<td>ip-address mask</td>
<td>(OPTIONAL) Enter the IP address of the network destination to view only</td>
</tr>
<tr>
<td></td>
<td>information on that destination. Enter the IP address in dotted decimal</td>
</tr>
<tr>
<td></td>
<td>format (A.B.C.D). You must enter the mask in slash prefix format (/X).</td>
</tr>
<tr>
<td>longer-prefixes</td>
<td>(OPTIONAL) Enter the keyword longer-prefixes to view all routes with a</td>
</tr>
<tr>
<td></td>
<td>common prefix.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword summary to view the total number of prefixes</td>
</tr>
<tr>
<td></td>
<td>in the FIB.</td>
</tr>
</tbody>
</table>

**Command Mode**

EXEC

EXEC Privilege

**Command History**

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

**Example**

**Figure 15-12. show ip fib stack-unit Command 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 15-6. 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip fib stack-unit</td>
<td>Clears FIB entries on a specified stack unit.</td>
</tr>
</tbody>
</table>
### show ip interface

View IP-related information on all interfaces.

#### Syntax

```
show ip interface [interface | brief] [configuration]
```

#### Parameter

- **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 0 to 16383.
  - For the Management interface, enter the keyword `ManagementEthernet` followed by zero (0).
  - For the Null interface, enter the keyword `null` followed by zero (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.

- **brief**: (OPTIONAL) Enter the keyword `brief` to view a brief summary of the interfaces and whether an IP address is assigned.

- **configuration**: (OPTIONAL) Enter the keyword `configuration` to display the physical interfaces with non-default configurations only.

#### Command Modes

- EXEC
- EXEC Privilege

#### Command History

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

#### Example

**Figure 15-13. 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 15-7. 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**

#### Figure 15-16. show ip protocols Command 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
       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 15-17. 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 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

Destiny Gateway Dist/Metric Last Change
----------------- --------- ---------------
FTOS#  
```
Example

Figure 15-18.  show ip route summary and show ip route static Command Examples

FTOS#show ip route summary

Route Source          Active Routes  Non-active Routes
connected             2              0
static                1              0
Total                 3              0
Total 3 active route(s) using 612 bytes
FTOS#show ip route static ?
|  >  Pipe through a command
<cr>
FTOS#show ip route static

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>*S 0.0.0.0/0</td>
<td>via 10.10.91.9, Te 1/2</td>
<td>1/0</td>
<td>3d2h</td>
</tr>
</tbody>
</table>
FTOS#

Table 15-9.  show ip route all Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| (undefined) | Identifies the type of route:
| 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 routes |
| Destination | Identifies the route’s destination IP 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. |

show ip route list

Display IP routes in an IP prefix list.

Syntax  show ip route list prefix-list
show ip route summary

View a table summarizing the IP routes in the switch.

**Syntax**

```
show ip route summary
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
### show ip route summary

The `show ip route summary` command is used to display the summary of IPv4 routes configured in the system. This command provides statistics on the number of active and non-active routes, as well as the memory usage of those routes. The command syntax is as follows:

```
show ip route summary
```

When executed, the command outputs a table that includes the following column headings:

- **Route Source**: Identifies how the route is configured in FTOS.
- **Active Routes**: Identifies the best route if a route is learned from two protocol sources.
- **Non-active Routes**: 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.

Here is an example of the output:

```
FTOS>show ip route summary
Route Source   Active Routes   Non-active Routes
connected      17              0
static         3               0
ospf 100       1368            2
Intra-area: 762 Inter-area: 1 External-1: 600 External-2: 5
Total          1388            2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
FTOS>
```

### Table 15-10. 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.</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. 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
show ip traffic Command Example (partial)

```
FTOS#show ip traffic
IP statistics:
  Rcvd: 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:
  Rcvd: 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:
  Rcvd: 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
```

--More--

Table 15-11. 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>Rcvd:</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 15-12. 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 |
Example

**Figure 15-22. show tcp statistics cp Command Example**

```
FTOS#show tcp statistics

Rcvd: 9849 Total, 0 no port
  0 checksum error, 0 bad offset, 0 too short
  5735 packets (7919 bytes) in sequence
  20 dup packets (2 bytes)
  0 partially dup packets (0 bytes)
  1 out-of-order packets (0 bytes)
  0 packets ( 0 bytes) with data after window
  0 packets after close
  0 window probe packets, 0 window update packets
  0 dup ack packets, 0 ack packets with unsend data
  6671 ack packets (152813 bytes)

Sent: 6778 Total, 0 urgent packets
  7 control packets
  6674 data packets (152822 bytes)
  12 data packets (1222 bytes) retransmitted
  85 ack only packets (5677 delayed)
  0 window probe packets, 0 window update packets
  0 Connections initiated, 7 connections accepted, 7 connections established
  8 Connections closed (including 4 dropped, 0 embryonic dropped)
  12 Total rxmt timeout, 1 connections dropped in rxmt timeout
  26 Keepalive timeout, 25 keepalive probe, 1 Connections dropped in keepalive

FTOS#
```

**Table 15-13. 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 15-13. 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>
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**

```plaintext
iscsi aging time time
```

To remove the iSCSI session aging time, use the `no iscsi aging time` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>time</code></td>
<td>Enter the aging time for the iSCSI session. Valid values: 5 to 43,200 minutes.</td>
</tr>
</tbody>
</table>

**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**

```plaintext
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enter the keyword <code>enable</code> 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.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Enter the keyword <code>disable</code> to disable the application of preferential QoS treatment to iSCSI frames.</td>
</tr>
<tr>
<td><code>dot1p</code></td>
<td>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 <code>iscsi priority-bits</code> command.</td>
</tr>
<tr>
<td><code>vlan-priority-value</code></td>
<td>Enter the VLAN priority tag assigned to the incoming packets in an iSCSI session.</td>
</tr>
<tr>
<td><code>dscp</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>dscp-value</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>remark</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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**

```markdown
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><code>enable</code></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**

```markdown
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**

```markdown
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**

```plaintext
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tcp-port-2...tcp-port-16</code></td>
<td>Enter the tcp-port number of the iSCSI target ports. The <code>tcp-port-n</code> 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.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>(OPTIONAL) Enter the ip-address that the iSCSI will monitor. The ip-address specifies the IP address of the iSCSI target.</td>
</tr>
</tbody>
</table>

**Defaults**

860, 3260.

**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>MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

**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**

```plaintext
show iscsi
```

**Command Modes**

EXEC

EXEC Privilege

**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>
### show iscsi sessions

Display information on active iSCSI sessions on the switch.

**Syntax**

```plaintext
show iscsi sessions
```

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

**Example**

#### Example 1

```
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
```

#### Example 2

```
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-x9l8v27yajg 
ISID: 400001370000.
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>show run iscsi</td>
<td>Display the currently configured iSCSI settings.</td>
</tr>
</tbody>
</table>
show iscsi sessions detailed

Display detailed information on active iSCSI sessions on the switch.

**Syntax**

```
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 16-3. 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 IP Address       TCP Port       Target 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 IP Address       TCP Port       Target 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
- show iscsi
  Display the currently configured iSCSI settings.
- show iscsi sessions
  Display information on active iSCSI sessions on the switch.
- show iscsi sessions detailed
  Display detailed information on active iSCSI sessions on the switch.
Link Aggregation Control Protocol (LACP)

Overview

This chapter contains commands for Dell Force10’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

<table>
<thead>
<tr>
<th><strong>port-channel-number</strong></th>
<th>Enter a port-channel number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range: 1 to 128</td>
</tr>
</tbody>
</table>

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
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show lACP</code></td>
<td>Displays the LACP configuration</td>
</tr>
</tbody>
</table>

### debug lACP

**Debug LACP (configuration, events etc.)**

**Syntax**

```
debug 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**

- `config` (OPTIONAL) Enter the keyword `config` to debug the LACP configuration.
- `events` (OPTIONAL) Enter the keyword `events` to debug LACP event information.
- `pdu in | out` (OPTIONAL) Enter the keyword `pdu` to debug LACP Protocol Data Unit information. Optionally, enter an `in` or `out` parameter to:
  - Receive enter `in`
  - Transmit enter `out`
- `interface in | out` 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.
  Optionally, enter an `in` or `out` parameter:
  - Receive enter `in`
  - Transmit enter `out`

**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
This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, the command has no effect.

**Usage Information**

**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>Range: 1 to 65535</td>
<td></td>
</tr>
<tr>
<td>Default: 32768</td>
<td></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>Range: 1 to 65535</td>
<td></td>
</tr>
<tr>
<td>Default: 32768</td>
<td></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]
```

**Usage Information**

This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, the command has no effect.
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

Example

Figure 17-1.  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)#port-channel-protocol lacp
FTOS(conf-if-tengig-3/16-lacp)#port-channel 32 mode active
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lacp</td>
<td>Displays the LACP information.</td>
</tr>
<tr>
<td>show interfaces port-channel</td>
<td>Displays information on configured Port Channel groups.</td>
</tr>
</tbody>
</table>

**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 17-2.  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 ACEHJLMP Key 1   Priority 128
  Oper: State ACEGIKNP Key 1   Priority 128
Partner Admin: State BDFHLJMP Key 0   Priority 0
  Oper: State BCEGJKNP Key 1   Priority 128
FTOS#
```

**Example 2**

```
Figure 17-3.  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#
```
Example 3

**Figure 17-4.  show lacp counter Command Example**

```
FTOS#show lacp 1 counters
-------------------------------------------------------------------
Port   LACP  Marker  Unknown  Illegal
       Xmit   Recv   Xmit   Recv   Pkts Rx  Pkts Rx
-------------------------------------------------------------------
TenGig 10/6  200  200  0  0  0  0
FTOS#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lacp counters</td>
<td>Clears the LACP counters.</td>
</tr>
<tr>
<td>show interfaces port-channel</td>
<td>Displays the information on configured Port Channel groups.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th><strong>address mac-address</strong></th>
<th>Enter the keyword <strong>address</strong> followed by a MAC address in nn:nn:nn:nn:nn:nn format.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Enter the keyword <strong>all</strong> to delete all MAC address entries in the MAC address table.</td>
</tr>
</tbody>
</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 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 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 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**

none

**Command Modes**

CONFIGURATION

**Command History**

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

**Usage Information**

For details about using this command, refer to the “NIC Teaming” section of the Layer 2 chapter in the *FTOS Configuration Guide*.

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address_limit</td>
<td>Enter the maximum number of MAC addresses that can be learned on the interface. Range: 1 to 1000000</td>
</tr>
<tr>
<td>dynamic</td>
<td>(OPTIONAL) Enter the keyword dynamic to allow aging of MACs even though a learning limit is configured.</td>
</tr>
</tbody>
</table>
no-station-move  (OPTIONAL) Enter the keyword 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 keyword 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 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 the `vlan` option is not specified, the MAC address counters is 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 a channel member is added to a port-channel and there is not enough ACL 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` Clears counters used in the `show interface` command
- `clear mac-address-table dynamic` Clears the MAC address table of all MAC address learned dynamically.
- `show mac learning-limit` Displays MAC learning-limit configuration.
**mac learning-limit learn-limit-violation**
Configure an action for a MAC address learning-limit violation.

**Syntax**
```plaintext
mac learning-limit learn-limit-violation {log | shutdown}
```
To return to the default, use the `no mac learning-limit learn-limit-violation {log | shutdown}` command.

**Parameters**
- **log**
  - Enter the keyword `log` to generate a syslog message on a learning-limit violation.
- **shutdown**
  - Enter the keyword `shutdown` to shut down the port on a learning-limit violation.

**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

**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**
```plaintext
mac learning-limit station-move-violation {log | shutdown-both | shutdown-offending | shutdown-original}
```
To disable a configuration, use the `no mac learning-limit station-move-violation` command, followed by the configured keyword.

**Parameters**
- **log**
  - Enter the keyword `log` to generate a syslog message on a station move violation.
- **shutdown-both**
  - Enter the keyword `shutdown` to shut down both the original and offending interface and generate a syslog message.
- **shutdown-offending**
  - Enter the keyword `shutdown-offending` to shut down the offending interface and generate a syslog message.
- **shutdown-original**
  - Enter the keyword `shutdown-original` to shut down the original interface and generate a syslog message.

**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
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
mac learning-limit reset

Defaults
none

Command Modes
EXEC
EXEC Privilege

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

show cam mac stack-unit
Display the Content Addressable Memory (CAM) size and the portions allocated for MAC addresses and for MAC ACLs.

Syntax
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 keyword 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 keyword 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 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 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.

- **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.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

**Example**

```
Router# show mac-address-table
```

**Description**

Display the MAC address table.
**Command Modes**

EXEC

EXEC Privilege

---

**Command History**

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

---

**Example**

### Figure 18-1. 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#
```

### Table 18-1. 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 32 for EtherScale, 1 to 255 for TeraScale  
|                | • so — Sonet followed by a slot/port.  
|                | • te — 10-Gigabit Ethernet followed by a slot/port.  
| State          | Lists if the MAC address is in use (Active) or not in use (Inactive). |

### Figure 18-2. 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 18-2. 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>
<tr>
<td>Static Address...</td>
<td>Lists the number of user-defined MAC addresses.</td>
</tr>
<tr>
<td>Total MAC...</td>
<td>Lists the total number of MAC addresses used by the switch.</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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan vlan-id</td>
<td>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.</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 18-3. show mac-address-table aging-time Command 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` (OPTIONALY) Enter the keyword `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 keyword `port-channel` followed by a number:
    Range: 1 to 128

**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 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. FTP, TFTP, ACLs, and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the virtual router redundancy protocol (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 14, 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

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Enter a text string description to identify the VLAN (80 characters maximum).</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

INTERFACE VLAN

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 vlan</td>
<td>Displays VLAN configuration.</td>
</tr>
</tbody>
</table>
**default vlan-id**

Specify a VLAN as the Default VLAN.

**Syntax**

default vlan-id vlan-id

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**

- **vlan-id**
  
  Enter the VLAN ID number of the VLAN to become the new Default VLAN.
  
  Range: 1 to 4094.
  
  Default: 1

**Defaults**

The Default VLAN is VLAN 1.

**Command Modes**

CONFIGURATION

**Command History**

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

**Usage Information**

To return VLAN 1 as the Default VLAN, use this command syntax (default-vlan-id 1).

The default VLAN contains only untagged interfaces.

**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>
</tbody>
</table>

**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 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

To remove the name from the VLAN, use the no name command.

**Parameters**

- **vlan-name**
  
  Enter up to 32 characters as the name of the VLAN.
Defaults
Not configured.

Command Modes
INTERFACE VLAN

Command History
Version 8.3.16.1 Introduced on 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 18-5. 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 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
Table 18-3. show vlan Command Information

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Column 1 — no heading)</td>
<td>asterisk symbol (*) = Default VLAN, G = GVRP VLAN, P = primary VLAN, C = community VLAN, I = isolated VLAN</td>
</tr>
<tr>
<td>NUM</td>
<td>Displays existing VLAN IDs.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the word Inactive for inactive VLANs and the word Active for active VLANs.</td>
</tr>
<tr>
<td>Q</td>
<td>Displays G for GVRP tagged, M for member of a VLAN-Stack VLAN, T for tagged interface, U (for untagged interface), x (uncapitalized x) for Dot1x untagged, or X (capitalized X) for Dot1x tagged.</td>
</tr>
<tr>
<td>Ports</td>
<td>Displays the type, slot, and port information. For the type, Po = port channel, Fo = fortygigabit ethernet, and Te = ten gigabit ethernet.</td>
</tr>
</tbody>
</table>
### Figure 18-7. 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

<table>
<thead>
<tr>
<th>NUM</th>
<th>Status</th>
<th>Description</th>
<th>Q Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inactive</td>
<td>a</td>
<td></td>
</tr>
</tbody>
</table>

FTOS#
```

### Figure 18-8. 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 18-9. 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

<table>
<thead>
<tr>
<th>NUM</th>
<th>Status</th>
<th>Description</th>
<th>Q Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>222</td>
<td>Inactive</td>
<td></td>
<td>U TenGig 1/22</td>
</tr>
</tbody>
</table>

FTOS(conf-if-vl-222)#
```

### Related Commands

- `vlan-stack compatible`: Enables the Stackable VLAN feature on the selected VLAN.
- `interface vlan`: Configures a VLAN.

---

**tagged**

Add a Layer 2 interface to a VLAN as a tagged interface.

**Syntax**

`tagged interface`

To remove a tagged interface from a VLAN, use `no tagged interface` command.
Untagged interfaces can only belong to one VLAN at a time.

**Related Commands**

- `track ip` - Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

**Syntax**

```
track ip interface
```

To remove the tracking feature from the VLAN, use the `no track ip interface` command.

**Parameters**

- `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: 1-128
  - 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**

INTERFACE VLAN

**Command History**

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

---

**Parameters**

- `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: 1-128
  - 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 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.

**Related Commands**

- `track ip` - Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface vlan</code></td>
<td>Configures a VLAN.</td>
</tr>
<tr>
<td><code>tagged</code></td>
<td>Specifies which interfaces in a VLAN are tagged.</td>
</tr>
</tbody>
</table>

**untagged**

Add a Layer 2 interface to a VLAN as an untagged interface.

**Syntax**

```plaintext
untagged interface
```

**Parameters**

- `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: 1-128
  - 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 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><code>interface vlan</code></td>
<td>Configures a VLAN.</td>
</tr>
<tr>
<td><code>tagged</code></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

| 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>protocol lldp (Configuration)</td>
<td>Enables LLDP globally.</td>
</tr>
<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 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

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

advertise management-tlv

Advertise management TLVs (Type, Length, Value).

Syntax

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-capabilities</td>
<td>Enter the keyword system-capabilities to advertise the system capabilities TLVs.</td>
</tr>
<tr>
<td>system-description</td>
<td>Enter the keyword system-description to advertise the system description TLVs.</td>
</tr>
<tr>
<td>system-name</td>
<td>Enter the keyword system-description to advertise the system description TLVs.</td>
</tr>
</tbody>
</table>

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

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

clear lldp neighbors {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
```

ddebug lldp interface

Enable LLDP debugging to display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets.

Syntax

```
ddebug 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.

*brie*  
(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)

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol lldp (Configuration)</td>
<td>Enables LLDP globally.</td>
</tr>
<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>

**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**

- `integer`: Enter the number of consecutive misses before the LLDP declares the interface dead.
  - Range: 2 - 10

**Defaults**

4 x hello

**Command Modes**

- CONFIGURATION (conf-lldp) and INTERFACE (conf-if-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

### Command History

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

### Example

```
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:e2:4a
```

### 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 19-3.  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 Force10 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.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>Enter the VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 4094</td>
</tr>
<tr>
<td><code>layer2_priority</code></td>
<td>Enter the Layer 2 priority.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 7</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
- **vlan-id**
  - Enter the VLAN ID.
  - Range: 1 to 4094

- **layer2_priority**
  - Enter the Layer 2 priority.
  - Range: 0 to 7

- **DSCP_value**
  - Enter the DSCP value.
  - Range: 0 to 63

- **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 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>Enter the VLAN ID. Range: 1 to 4094</td>
</tr>
<tr>
<td>priority-tagged</td>
<td>Enter the keyword priority-tagged</td>
</tr>
<tr>
<td>number</td>
<td>followed the Layer 2 priority. Range: 0 to 7</td>
</tr>
</tbody>
</table>

Defaults
unconfigured

Command Modes
CONFIGURATION (conf-lldp)

Related Commands
debug lldp interface Configures the LLDP debugging
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>Enter the VLAN ID. Range: 1 to 4094</td>
</tr>
<tr>
<td>priority-tagged</td>
<td>Enter the keyword priority-tagged</td>
</tr>
<tr>
<td>number</td>
<td>followed the Layer 2 priority. Range: 0 to 7</td>
</tr>
</tbody>
</table>

Defaults
unconfigured

Command Modes
CONFIGURATION (conf-lldp)
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**

- **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
- show lldp neighbors
- show running-config lldp

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**

- **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
<table>
<thead>
<tr>
<th>Defaults</th>
<th>unconfigured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>CONFIGURATION (conf-lldp)</td>
</tr>
<tr>
<td>Command History</td>
<td>Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
<tr>
<td>Related Commands</td>
<td>debug lldp interface</td>
</tr>
<tr>
<td></td>
<td>show lldp neighbors</td>
</tr>
<tr>
<td></td>
<td>show lldp neighbors</td>
</tr>
</tbody>
</table>
Multiple Spanning Tree Protocol (MSTP)

Overview

The multiple spanning tree protocol (MSTP), as implemented by the Dell Force10 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

debug spanning-tree mstp [all | bpdu interface {in | out} | events]

To disable debugging, use the no debug spanning-tree mstp 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 MSTP events.

Command Modes

- EXEC Privilege

Command History

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

Example

Figure 20-1. 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

description {description}

To remove the description, use the no description {description} command.

Parameters

- **description** Enter a description to identify the Multiple Spanning Tree (80 characters maximum).

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
```

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
```

Parameters

- **seconds**: The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

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**: Changes the wait time before MSTP refreshes protocol configuration information.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-age</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

MULTIPLE SPANNING TREE

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</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

- `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` - Changes the time interval between BPDUs.
- `hello-time` - Changes the time interval between BPDUs.

### max-hops

Configure the maximum hop count.

**Syntax**

```
max-hops number
```

To return to the default values, use the `no max-hops` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>range</td>
<td>Enter a number for the maximum hop count. Range: 1 to 40. Default: 20</td>
</tr>
</tbody>
</table>

**Defaults**

20 hops

### Command Modes

MULTIPLE SPANNING TREE

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</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 `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.
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

- **region-name**: Enter the MST region name.
  - Range: 32 character limit

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

- **msti**: Maps the VLAN(s) to an MST instance.
- **revision**: Assigns the revision number to the MST configuration.
**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**

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

**Example**

**Figure 20-2. 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**

Version 8.3.16.1 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 20-3. 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

Example
Figure 20-4. 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]
Parameters

- **instance-number**  
  [OPTIONAL] Enter the Multiple Spanning Tree Instance number  
  Range: 0 to 63

- **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 20-5. 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 Name PortID Prio Cost Sts    Cost        Bridge ID        PortID
---------- -------- ---- ------- ----------- ------- --------------------
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

FTOS#
```
Example 2
Figure 20-6. 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 20-7. show spanning-tree msti guard Command Example

```
FTOS#show spanning-tree msti 0 guard
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 20-1. 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>MISTP interface</td>
</tr>
<tr>
<td>Instance</td>
<td>MISTP 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree</td>
<td>Enter the keyword <code>spanning-tree</code> to enable the MSTP on the interface.</td>
</tr>
<tr>
<td></td>
<td>Default: Enable</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msti instance</td>
<td>Enter the keyword <code>msti</code> and the MST Instance number.</td>
</tr>
<tr>
<td></td>
<td>Range: zero (0) to 63</td>
</tr>
<tr>
<td>cost cost</td>
<td>(OPTIONAL) Enter the keyword <code>cost</code> followed by the port cost value.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 200000</td>
</tr>
<tr>
<td></td>
<td>Defaults:</td>
</tr>
<tr>
<td></td>
<td>• 40-Gigabit Ethernet interface = 1400</td>
</tr>
<tr>
<td></td>
<td>• 10-Gigabit Ethernet interface = 2000</td>
</tr>
<tr>
<td></td>
<td>• Port Channel interface with one 10-Gigabit Ethernet = 2000</td>
</tr>
<tr>
<td></td>
<td>• Port Channel with two 10-Gigabit Ethernet = 1800</td>
</tr>
<tr>
<td></td>
<td>• Port Channel with two 100-Mbps Ethernet = 180000</td>
</tr>
<tr>
<td>priority priority</td>
<td>Enter keyword <code>priority</code> followed by a value in increments of 16 as the priority.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 240.</td>
</tr>
<tr>
<td></td>
<td>Default: 128</td>
</tr>
</tbody>
</table>

**Defaults**

`cost` = depends on the interface type; `priority` = 128

**Command Modes**

INTERFACE

---

**Table 20-1. 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`: (OPTIONAL) Enter the keyword `edgeport` to enable edge port configuration to move the interface into forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
- `bpdufilter`: (OPTIONAL) Enter the keyword `edgeport` to enable edge port configuration to move the interface into forwarding mode immediately after the root fails. Enter the keyword `bpdufilter` to stop sending and receiving BPDUs on the port-fast enabled ports.
- `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

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

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.
Open Shortest Path First (OSPFv2)

Overview

The MXL 10/40GbE Switch IO Module platform supports open shortest path first (OSPFv2) only. 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.

OSPFv2 Commands

The Dell Force10 implementation of OSPFv2 is based on IETF RFC 2328. The following commands allow you to configure and enable OSPFv2.

- area default-cost
- area nssa
- area range
- area stub
- auto-cost
- clear ip ospf
- clear ip ospf statistics
- debug ip ospf
- default-information originate
- default-metric
- description
- distance
- distance ospf
- distribute-list in
- distribute-list out
- fast-converge
- flood-2328
- graceful-restart helper-reject
- ip ospf auth-change-wait-time
- ip ospf authentication-key
- ip ospf cost
- ip ospf dead-interval
- ip ospf hello-interval
- ip ospf message-digest-key
- ip ospf mtu-ignore
- ip ospf network
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- log-adjacency-changes
- maximum-paths
- mib-binding
- network area
- passive-interface
- redistribute
- router-id
- router ospf
- show config
- show ip ospf
- show ip ospf asbr
- show ip ospf database
- show ip ospf database asbr-summary
- show ip ospf database external
- show ip ospf database network
- show ip ospf database nssa-external
- show ip ospf database opaque-area
- show ip ospf database opaque-as
- show ip ospf database opaque-link
- show ip ospf database router
- show ip ospf database summary
- show ip ospf interface
- show ip ospf neighbor
- show ip ospf routes
- show ip ospf statistics
- show ip ospf timers rate-limit
- show ip ospf topology
- summary-address
- timers spf
- timers throttle lsa all
- timers throttle lsa arrival
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.

Parameters

- **area-id**: Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from 0 to 65535.
- **cost**: Specifies the stub area’s advertised external route metric. Range: zero (0) to 65535.

Defaults

cost = 1; no areas are configured.

Command Modes

ROUTER OSPF

Command History

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

Usage Information

In FTOS, cost is defined with reference to bandwidth.

Related Commands

area stub Creates a stub area.

area nssa

Specify an area as a not so stubby area (NSSA).

Syntax

area area-id nssa [default-information-originate] [no-redistribution] [no-summary]

To delete an NSSA, use the no area area-id nssa command.

Parameters

- **area-id**: Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from 0 and 65535.
- **default-information-originate** (OPTIONAL): Allows external routing information to be imported into the NSSA by using Type 7 default.
- **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).
- **no-summary** (OPTIONAL): Specify that no summary LSAs should be sent into the NSSA.

Defaults

Not configured

Command Mode

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]
```

To disable route summarization, use the `no area area-id range ip-address mask` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Specify an IP address in dotted decimal format.</td>
</tr>
<tr>
<td>mask</td>
<td>Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).</td>
</tr>
<tr>
<td>not-advertise</td>
<td>(OPTIONAL) Enter the keyword <code>not-advertise</code> to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)</td>
</tr>
</tbody>
</table>

Defaults

No range is configured.

Command Modes

ROUTER OSPF

Command History

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

Usage Information

Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.

Related Commands

- `area stub` Creates a stub area.
- `router ospf` Enters ROUTER OSPF mode to configure an OSPF instance.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>Specify the stub area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.</td>
</tr>
<tr>
<td>no-summary</td>
<td>(OPTIONAL) Enter the keyword <code>no-summary</code> to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.</td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

ROUTER OSPF

Command History

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

Usage Information

Use this command to configure all routers and access servers within a stub.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router ospf</td>
<td>Enters the ROUTER OSPF mode to configure an OSPF instance.</td>
</tr>
</tbody>
</table>

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**

- **process-id**
  - Enter the OSPF Process ID to clear statistics for a specific process.
  - If no Process ID is entered, all OSPF processes are cleared.

- **interface name**
  - (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:
      - 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.
    - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

- **neighbor router-id**
  - (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.

---

**debug ip ospf**

Display debug information on OSPF. Entering `debug ip ospf` enables OSPF debugging for the first OSPF process.

**Syntax**

```
debug ip ospf process-id [event | packet | spf | database-timer rate-limit]```

To cancel the debug command, enter `no debug ip ospf`.

**Parameters**

- **process-id**
  - Enter the OSPF Process ID to debug a specific process.
  - If no Process ID is entered, command applies only to the first OSPF process.

- **event**
  - (OPTIONAL) Enter the keyword event to debug only OSPF event information.

- **packet**
  - (OPTIONAL) Enter the keyword packet to debug only OSPF packet information.

- **spf**
  - (OPTIONAL) Enter the keyword spf to display the Shortest Path First information.

- **database-timer rate-limit**
  - (OPTIONAL) Enter the keyword database-timer rate-limit to display the LSA throttling timer information.

**Command Modes**

EXEC Privilege
**Command History**

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

**Figure 21-1. 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 21-1. 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>
</tbody>
</table>
| t:    | Displays the type of packet sent:  
  - 1 - Hello packet  
  - 2 - database description  
  - 3 - link state request  
  - 4 - link state update  
  - 5 - link state acknowledgement |
| l:    | Displays the packet length. |
| rid:  | Displays the OSPF router ID. |
| aid:  | Displays the Autonomous System ID. |
| chk:  | Displays the OSPF checksum. |
| aut:  | States if OSPF authentication is configured. One of the following is listed:  
  - 0 - no authentication configured  
  - 1 - simple authentication configured using the **ip ospf authentication-key** command  
  - 2 - MD5 authentication configured using the **ip ospf message-digest-key** command. |
| auk:  | If the **ip ospf authentication-key** command is configured, this field displays the key used. |
| keyid:| If the **ip ospf message-digest-key** command is configured, this field displays the MD5 key |
| to:   | Displays the interface to which the packet is intended. |
| dst:  | Displays the destination IP address. |
| netmask: | Displays the destination IP address mask. |
| pri:  | Displays the OSPF priority |
default-information originate

Configure the FTOS to generate a default external route into an OSPF 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

- **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 keyword 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 keyword 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. Range: 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]

To delete these settings, use the no distance ospf command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>weight</td>
<td>Specify an administrative distance.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>Default: 110.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(OPTIONAL) Enter a router ID in the dotted decimal format.</td>
</tr>
<tr>
<td></td>
<td>If you enter a router ID, you must include the mask for that router address.</td>
</tr>
<tr>
<td>mask</td>
<td>(OPTIONAL) Enter a mask in dotted decimal format or /n format.</td>
</tr>
<tr>
<td>access-list-name</td>
<td>(OPTIONAL) Enter the name of an IP standard access list, up to 140 characters.</td>
</tr>
</tbody>
</table>

Defaults

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]

To delete a filter, use the no distribute-list prefix-list-name in [interface] command.

Parameters

<table>
<thead>
<tr>
<th>prefix-list-name</th>
<th>Enter the name of a configured prefix list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>(OPTIONAL) Enter one of the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For Port Channel groups, 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 VLAN, enter the keyword vlan followed by a number from 1 to 4094.</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 Modes

ROUTER OSPF

Command History

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

---

distribute-list out

Apply a filter to restrict certain routes destined for the local routing table after the SPF calculation.

Syntax  
distribute-list prefix-list-name out [connected | rip | static]

To remove a filter, use the no distribute-list prefix-list-name out [connected | rip | static] command.

Parameters

<table>
<thead>
<tr>
<th>prefix-list-name</th>
<th>Enter the name of a configured prefix list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>(OPTIONAL) Enter the keyword connected to specify that connected routes are distributed.</td>
</tr>
<tr>
<td>rip</td>
<td>(OPTIONAL) Enter the keyword rip to specify that RIP routes are distributed.*</td>
</tr>
<tr>
<td>static</td>
<td>(OPTIONAL) Enter the keyword static to specify that only manually configured routes are distributed.</td>
</tr>
</tbody>
</table>

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 being redistributed by autonomous system boundary routers (ASBRs) 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-converge**

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-converge {number}
```

To cancel fast-convergence, use the `no fast converge` command.

**Parameters**

- `number` Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place.
  - Range: 1-4

**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 that the faster the convergence, the more frequent the route calculations and updates. This will impact 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 Force10 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 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**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

### 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.

**Parameters**
- `seconds`: Enter seconds
  
  Range: 0 to 300

**Defaults**
zero (0) seconds

**Command Modes**
- INTERFACE

**Command History**
- Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module
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 8 character string. Strings longer than 8 characters are truncated.

Defaults  
Not configured.

Command Modes  
INTERFACE

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

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

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

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

To change to a different key on the interface, enable the new key while the old key is still enabled. The FTOS will send 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, you must delete the old key. Dell Force10 recommends keeping only one key per interface.

Note: The MD5 secret is stored as plain text in the configuration file with service password encryption.

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**

```
ip ospf network {broadcast | point-to-point}
```

To return to the default, use the **no ip ospf network** command.

**Parameters**

- **broadcast**
  - Enter the keyword `broadcast` to designate the interface as part of a broadcast network.

- **point-to-point**
  - Enter the keyword `point-to-point` to designate the interface as part of a point-to-point network.

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

- 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**

```
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**

- Introduced on MXL 10/40GbE Switch IO Module

---

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
```

To return to the default values, use the **no ip ospf retransmit-interval** command.

**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.
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.

ip ospf transmit-delay
Set the estimated time elapsed to send a link state update packet on the interface.

Syntax

ip ospf transmit-delay seconds

To return to the default value, use the no ip ospf transmit-delay command.

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
Set FTOS to send a Syslog message about changes in the OSPF adjacency state.

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 MXL 10/40GbE Switch IO Module
maximum-paths

Enable the software to forward packets over multiple paths.

Syntax

maximum-paths number

To disable packet forwarding over multiple paths, use the no maximum-paths command.

Parameters

number Specify the number of paths.
Range: 1 to 64.
Default: 4 paths.

Defaults

4

Command Modes

ROUTER OSPF

Command History

Version 8.3.16.1 Introduced on MXL 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 MXL 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 will be 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

ip-address Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
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 will not list Area 0.

---

### passive-interface

Supress 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enter the keyword <code>default</code> to make all OSPF interfaces (current and future) passive.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For Port Channel groups, 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 VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</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>

**Command Modes**

ROUTER OSPF

**Command History**

Version 8.3.16.1 Introduced on 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 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]
```

To disable redistribution, use the **no redistribute {connected | ospf | rip | static}** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>connected</code></td>
<td>Enter the keyword <strong>connected</strong> to specify that information from active routes on interfaces is redistributed.</td>
</tr>
<tr>
<td><code>rip</code></td>
<td>Enter the keyword <strong>rip</strong> to specify that RIP routing information is redistributed.</td>
</tr>
<tr>
<td><code>ospf</code></td>
<td>Enter the keyword <strong>ospf</strong> to specify that RIP routing information is redistributed.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Enter the keyword <strong>static</strong> to specify that information from static routes is redistributed.</td>
</tr>
<tr>
<td><code>metric metric-value</code></td>
<td>(OPTIONAL) Enter the keyword <strong>metric</strong> followed by a number. Range: 0 (zero) to 16777214.</td>
</tr>
</tbody>
</table>
metric-type
type-value

(Optional) Enter the keyword 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 keyword 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.

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 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module

Example

Figure 21-2. 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#
You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If this command is used on an OSPF router process, which is already active (that is, has neighbors), a prompt reminding you that changing router-id will bring down the existing OSPF adjacency. The new router ID is effective at the next reload.

**router ospf**

Enter the ROUTER OSPF mode to configure an OSPF instance.

**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 21-3. 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 21-4. show config Command Example**

```
FTOS(conf-router_ospf)#show config
1 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 will not list Area 0.

Example

```
Figure 21-5. show ip ospf process-id Command 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 SPF 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#
```

Table 21-2. show ip ospf process-id Command Descriptions:

<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) rouse 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>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf database</td>
<td>Displays information about the OSPF routes configured.</td>
</tr>
<tr>
<td>show ip ospf interface</td>
<td>Displays the OSPF interfaces configured.</td>
</tr>
<tr>
<td>show ip ospf neighbor</td>
<td>Displays the OSPF neighbors configured.</td>
</tr>
</tbody>
</table>
show ip ospf asbr
Display all 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
No default values or behavior

Command Modes
EXEC
EXEC Privilege

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

Usage Information
Use this command to isolate problems with external routes. 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.

Example
Figure 21-6. show ip ospf process-id asbr Command Example

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#

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 figure above, router 1.1.1.1 is in a directly connected area since the Flag is E/-/-/. For remote ASBRs, the E flag is clear (-/-/-/)

show ip ospf database
Display all LSA information. If OSPF is not enabled on the switch, no output is generated.

Syntax
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 the 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

Example

Figure 21-7.  show ip ospf process-id database Command Example

FTOS> show ip ospf 1 database

OSPF Router with ID (11.1.2.1) (Process ID 1)

Router (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Link count</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1.2.1</td>
<td>11.1.2.1</td>
<td>673</td>
<td>0x80000005</td>
<td>0x707e</td>
<td>2</td>
</tr>
<tr>
<td>13.1.1.1</td>
<td>13.1.1.1</td>
<td>676</td>
<td>0x80000097</td>
<td>0x1035</td>
<td>2</td>
</tr>
<tr>
<td>192.68.135.2</td>
<td>192.68.135.2</td>
<td>1419</td>
<td>0x80000294</td>
<td>0x9cb7</td>
<td>1</td>
</tr>
</tbody>
</table>

Network (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.3.2</td>
<td>13.1.1.1</td>
<td>676</td>
<td>0x80000003</td>
<td>0x6592</td>
</tr>
<tr>
<td>10.2.4.2</td>
<td>192.68.135.2</td>
<td>908</td>
<td>0x80000055</td>
<td>0x683e</td>
</tr>
</tbody>
</table>

Type-5 AS External

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>192.68.135.2</td>
<td>908</td>
<td>0x80000052</td>
<td>0xeb83</td>
<td>100</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>192.68.135.2</td>
<td>908</td>
<td>0x8000002a</td>
<td>0xdbd7</td>
<td>0</td>
</tr>
<tr>
<td>10.1.1.0</td>
<td>11.1.2.1</td>
<td>718</td>
<td>0x80000002</td>
<td>0x9012</td>
<td>0</td>
</tr>
<tr>
<td>10.1.2.0</td>
<td>11.1.2.1</td>
<td>718</td>
<td>0x80000002</td>
<td>0x851c</td>
<td>0</td>
</tr>
<tr>
<td>10.2.2.0</td>
<td>11.1.2.1</td>
<td>718</td>
<td>0x80000002</td>
<td>0x7927</td>
<td>0</td>
</tr>
<tr>
<td>10.2.3.0</td>
<td>11.1.2.1</td>
<td>718</td>
<td>0x80000002</td>
<td>0x6e31</td>
<td>0</td>
</tr>
<tr>
<td>10.2.4.0</td>
<td>13.1.1.1</td>
<td>1184</td>
<td>0x80000068</td>
<td>0x45db</td>
<td>0</td>
</tr>
<tr>
<td>11.1.1.0</td>
<td>11.1.2.1</td>
<td>718</td>
<td>0x80000002</td>
<td>0x831e</td>
<td>0</td>
</tr>
<tr>
<td>11.1.2.0</td>
<td>11.1.2.1</td>
<td>718</td>
<td>0x80000002</td>
<td>0x7828</td>
<td>0</td>
</tr>
<tr>
<td>12.1.2.0</td>
<td>192.68.135.2</td>
<td>1663</td>
<td>0x80000054</td>
<td>0xdbd6</td>
<td>0</td>
</tr>
<tr>
<td>13.1.1.0</td>
<td>13.1.1.1</td>
<td>1192</td>
<td>0x8000006b</td>
<td>0x2718</td>
<td>0</td>
</tr>
<tr>
<td>13.1.2.0</td>
<td>13.1.1.1</td>
<td>1184</td>
<td>0x8000006b</td>
<td>0x1e22</td>
<td>0</td>
</tr>
<tr>
<td>172.16.1.0</td>
<td>13.1.1.1</td>
<td>148</td>
<td>0x8000006d</td>
<td>0x533b</td>
<td>0</td>
</tr>
</tbody>
</table>

FTOS>

Table 21-3.  show ip ospf process-id database Command Description

<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>

Related Commands

show ip ospf database asbr-summary  
Displays only ASBR summary LSA information.

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]

410  | Open Shortest Path First (OSPFv2)
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 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 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

Figure 21-8. 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)
                     LS type: Summary Asbr
                     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--

Table 21-4. show ip ospf database asbr-summary 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 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>
</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

- 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 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 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**

**Figure 21-9. show ip ospf database external Command 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#
```

**Table 21-5. 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>
</tbody>
</table>
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 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**: (OPTIONAL) Enter the keywords `adv-router` 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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

**Figure 21-10. 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)
        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)
        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 21-6. 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>

**Related Commands**

- `show ip ospf database`  
  Displays OSPF database information.
show ip ospf database nssa-external

Display NSSA-External (type 7) LSA information.

**Syntax**

```plaintext
show ip ospf database nssa-external [link-state-id] [adv-router ip-address]
```

**Parameters**

- `link-state-id` (OPTIONAL) Specify 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` 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 opaque-area

Display the opaque-area (type 10) LSA information.

**Syntax**

```plaintext
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 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` 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
Figure 21-11. show ip ospf process-id database opaque-area Command Example (Partial)

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)
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)
Link State ID: 1.0.0.2
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000002
Checksum: 0x19c2
--More--

Table 21-7. 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 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 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 State ID).</td>
</tr>
</tbody>
</table>

Related Commands

- show ip ospf database Displays OSPF database information.
### show ip ospf database opaque-as
Display the opaque-as (type 11) LSA information.

**Syntax**
```
show ip ospf process-id database opaque-as [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 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` 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 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 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 keyword `adv-router` followed by the IP address of an Advertising Router 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>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>
</tbody>
</table>
| link-state-id | (OPTIONAL) Specify 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 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

**Figure 21-12. 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
```

**Table 21-8. 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>
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 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 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.

### Table 21-8. 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>
Example

**Figure 21-13. show ip ospf process-id database summary Command Example**

```
FTOS#show ip ospf 100 database summary

OSPF Router with ID (1.1.1.10) (Process ID 100)
Summary Network (Area 0.0.0.0)

LS age: 1551
Options: (No TOS-capability, DC, E)
LS type: Summary Network
Link State ID: 192.68.16.0
Advertising Router: 192.168.17.1
LS Seq Number: 0x80000054
Checksum: 0xb5a2
Length: 28
Network Mask: /24
  TOS: 0 Metric: 1

LS age: 9
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.32.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x987c
Length: 28
Network Mask: /24
  TOS: 0 Metric: 1

LS age: 7
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.33.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x1241
Length: 28
Network Mask: /26
  TOS: 0 Metric: 1

FTOS#
```

**Table 21-9. 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>
Table 21-9.  `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>

Related Commands

- `show ip ospf database` Displays OSPF database information.

**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` followed by zero (0).
  - For loopback interfaces, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For Port Channel groups, 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 the VLAN ID. The range is from 1 to 4094.
  - 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

Figure 21-14.  show ip ospf process-id interface Command Example

FTOS>show ip ospf int
TenGigabitEthernet 13/17 is up, line protocol is up
  Internet Address 192.168.1.2/30, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.253.2, Interface address 192.168.1.2
  Backup Designated Router (ID) 192.168.253.1, Interface address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.253.1 (Backup Designated Router)

TenGigabitEthernet 13/23 is up, line protocol is up
  Internet Address 192.168.0.1/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.253.5, Interface address 192.168.0.4
  Backup Designated Router (ID) 192.168.253.3, Interface address 192.168.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:08
  Neighbor Count is 3, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.253.5 (Designated Router)
  Adjacent with neighbor 192.168.253.3 (Backup Designated Router)

Loopback 0 is up, line protocol is up
  Internet Address 192.168.253.2/32, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host.
FTOS>

Table 21-10.  show ip ospf process-id interface Command Description

<table>
<thead>
<tr>
<th>Line beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet...</td>
<td>This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.</td>
</tr>
<tr>
<td>Internet Address...</td>
<td>This line displays the IP address, network mask and area assigned to this interface.</td>
</tr>
<tr>
<td>Process ID...</td>
<td>This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.</td>
</tr>
<tr>
<td>Transmit Delay...</td>
<td>This line displays the interface’s settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.</td>
</tr>
<tr>
<td>Designated Router...</td>
<td>This line displays the ID of the Designated Router and its interface address.</td>
</tr>
<tr>
<td>Backup Designated...</td>
<td>This line displays the ID of the Backup Designated Router and its interface address.</td>
</tr>
<tr>
<td>Timer intervals...</td>
<td>This line displays the interface’s timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.</td>
</tr>
<tr>
<td>Hello due...</td>
<td>This line displays the amount time till the next Hello packet is sent out this interface.</td>
</tr>
<tr>
<td>Neighbor Count...</td>
<td>This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.</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 21-15. show ip ospf process-id neighbor Command Example

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/DROTHER00:00:36  192.10.10.4     TenGig 0/1   0.0.0.1
FTOS#
```

**Table 21-11. 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 as calculated by OSPF and stored 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
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 Port Channel groups, 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.
  • For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

neighbor router-id  (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

EXEC Privilege
Command History

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

Figure 21-17.  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>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>

Error packets (Receive statistics)

<table>
<thead>
<tr>
<th>Intf-Down</th>
<th>0</th>
<th>Non-Dr</th>
<th>0</th>
<th>Self-Org</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong-Len</td>
<td>0</td>
<td>Invd-Nbr</td>
<td>0</td>
<td>Nbr-State</td>
<td>0</td>
</tr>
<tr>
<td>Auth-Err</td>
<td>0</td>
<td>MD5-Err</td>
<td>0</td>
<td>Chksum</td>
<td>0</td>
</tr>
<tr>
<td>Version</td>
<td>0</td>
<td>AreaMis</td>
<td>0</td>
<td>Conf-Issues</td>
<td>0</td>
</tr>
<tr>
<td>No-Buffer</td>
<td>0</td>
<td>Seq-No</td>
<td>0</td>
<td>Socket</td>
<td>0</td>
</tr>
<tr>
<td>Q-Overflow</td>
<td>0</td>
<td>Unknown-Pkt</td>
<td>0</td>
<td>RtidZero</td>
<td>0</td>
</tr>
</tbody>
</table>

Error packets (Transmit statistics)

FTOS#

Table 21-12.  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>
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

### Table 21-13. `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>
Figure 21-18. show ip ospf process-id statistics Command Example

```
FTOS#show ip ospf 10 statistics
Interface TenGigabitEthernet 4/45
  Error packets (Receive statistics)
    Intf-Down          0  Non-Dr          0  Self-Org        0
    Wrong-Len          0  Invld-Nbr        0  Nbr-State       0
    Auth-Error         0  MD5-Error        0  Cksum-Err       0
    Version            0  AreaMisMatch     0  Conf-Issue      0
    SegNo-Err          0  Unknown-Pkt      0  Bad-LsReq       0
  RtidZero            0
  Neighbor ID 3.1.1.2
  Packet Statistics
    RX    47  DDiscr    2  LSReq    1  LSUpd    3  LSAck    2
    TX    46  3        1        3        2
  Timers
    Hello     1  Wait     0  Grace     0
    Dead    37  Transmit   0
  Queue Statistics
    LSU-Q-Len    0  LSU-Q-Wmark   1
    LSR-Q-Len    0  LSR-Q-Wmark   1
```

FTOS#

Related Commands

| clear ip ospf statistics | Clears the packet statistics in all interfaces and neighbors |

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

Figure 21-19. show ip ospf process-id timers rate-limit Command Example

```
FTOS#show ip ospf 10 timers rate-limit

List of LSA 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#
show ip ospf topology
Display routers in directly connected areas.

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
This command can be used to isolate problems with inter-area and external routes. 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 21-20. 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]
```

To disable summary address, use the no summary-address ip-address mask command.

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 keyword 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.
  Range: 0 to 4294967295

Defaults
- Not configured.

Command Modes
- ROUTER OSPF
The command `area range` summarizes routes for the different areas.

With "not-advertise" parameter configured, this command can be used to filter out some external routes. For example, 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 fall in range 1.1.0.0/16.

Related Commands

area range  Summarizes routes within an area.

**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`

**Parameters**

- `delay`  
  Enter a number as the delay.  
  Range: 0 to 4294967295.  
  Default: 5 seconds

- `holdtime`  
  Enter a number as the hold time.  
  Range: 0 to 4294967295.  
  Default: 10 seconds

**Defaults**

`delay = 5 seconds; holdtime = 10 seconds`

**Command Modes**

ROUTER OSPF

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-interval</td>
<td>Set the minimum interval between initial sending and resending the same LSA.</td>
<td>0-600,000 milliseconds</td>
</tr>
<tr>
<td>hold-interval</td>
<td>Set the next interval to send the same LSA. This is the time between sending the same LSA after the start-interval has been attempted.</td>
<td>1-600,000 milliseconds</td>
</tr>
<tr>
<td>max-interval</td>
<td>Set the maximum amount of time the system waits before sending the LSA.</td>
<td>1-600,000 milliseconds</td>
</tr>
</tbody>
</table>

Defaults

- start-interval: 0 msec
- hold-interval: 5000 msec
- max-interval: 5000 msec

Command Modes

- ROUTER OSPF

Command History

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

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 same LSA, so that the interval is multiplied until the maximum time is reached. For example, if the start-interval 5000 and hold-interval 1000 and max-interval 100,000, the LSA is sent at 5000 msec, then 1000 msec, then 2000 msec, then 4000 msec, 10,000 msec, and 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>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>arrival-time</td>
<td>Set the interval between receiving the same LSA repeatedly, to allow sufficient time for the system to accept the LSA.</td>
<td>0-600,000 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
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 Force10 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 

To remove the description, use the no description command.

**Parameters**

- **description**
  
  Enter a description regarding this session (80 characters maximum).

**Defaults**

none

**Command Modes**

MONITOR SESSION (conf-mon-sess-session-ID)

**Command History**

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

**Related Commands**

- **monitor session**
  
  Enables a monitoring session.

---

**monitor session**

Create a session for monitoring traffic with port monitoring.

**Syntax**

monitor session session-ID

To delete a session, use the no monitor session session-ID command.

To delete all monitor sessions, use the no monitor session all command.

**Parameters**

- **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 MXL 10/40GbE Switch IO Module

**Example**

Figure 22-1.  monitor session Command Example

```
FTOS(conf)# monitor session 60
FTOS(conf-mon-sess-60)
```

**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 MXL 10/40GbE Switch IO Module

Example

Figure 22-2. 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 MXL 10/40GbE Switch IO Module

Example

Figure 22-3. show monitor session Command Example

FTOS#show monitor session 11

<table>
<thead>
<tr>
<th>SessionID</th>
<th>Source</th>
<th>Destination</th>
<th>Direction</th>
<th>Mode</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>TenGig 10/0</td>
<td>TenGig 10/47</td>
<td>rx</td>
<td>interface</td>
<td></td>
</tr>
</tbody>
</table>
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

- 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 MXL 10/40GbE Switch IO Module

Example

Figure 22-4. 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

- `monitor session` - Creates a session for monitoring.
- `show monitor session` - Displays a monitor session.
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

- **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 MXL 10/40GbE Switch IO Module

Example

```
Figure 22-5. 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)#
```
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 15, IPv4 Routing
- `show vlan` in Chapter 18, Layer 2

Private virtual local area networks (VLANs) extend the Dell Force10 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>private-vlan mapping secondary-vlan</td>
<td>Maps the secondary VLANs to the selected primary VLAN.</td>
</tr>
<tr>
<td>show arp</td>
<td>Displays the ARP table.</td>
</tr>
<tr>
<td>show interfaces private-vlan</td>
<td>Displays the type and status of the PVLAN interfaces.</td>
</tr>
<tr>
<td>show vlan private-vlan</td>
<td>Displays PVLANs and/or interfaces that are part of a PVLAN.</td>
</tr>
<tr>
<td>switchport mode private-vlan</td>
<td>Sets PVLAN mode of the selected port.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community</td>
<td>Enter <code>community</code> to set the VLAN as a community VLAN, as described above.</td>
</tr>
<tr>
<td>isolated</td>
<td>Enter <code>isolated</code> to configure the VLAN as an isolated VLAN, as described above.</td>
</tr>
<tr>
<td>primary</td>
<td>Enter <code>primary</code> to configure the VLAN as a primary VLAN, as described above.</td>
</tr>
</tbody>
</table>

**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>
</tr>
</thead>
<tbody>
<tr>
<td><code>private-vlan mapping secondary-vlan</code></td>
</tr>
<tr>
<td><code>show interfaces private-vlan</code></td>
</tr>
<tr>
<td><code>show vlan private-vlan</code></td>
</tr>
<tr>
<td><code>show vlan private-vlan mapping</code></td>
</tr>
<tr>
<td><code>switchport mode private-vlan</code></td>
</tr>
</tbody>
</table>

### `private-vlan mapping secondary-vlan` command

Map secondary VLANs to the selected primary VLAN.

#### Syntax

```
[no] private-vlan mapping secondary-vlan vlan-list
```

To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan vlan-list` 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

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

#### 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.

#### Related Commands

- `private-vlan mode` | Sets the mode of the selected VLAN to community, isolated, or primary. |
- `show interfaces private-vlan` | Displays the type and status of PVLAN interfaces. |
- `show vlan private-vlan` | Displays the PVLANs and/or interfaces that are part of a PVLAN. |
- `show vlan private-vlan mapping` | Displays the primary-secondary VLAN mapping. |
- `switchport mode private-vlan` | Sets the PVLAN mode of the selected port. |
show interfaces private-vlan

Display type and status of PVLAN interfaces.

**Syntax**

```
show interfaces private-vlan [interface interface]
```

**Parameters**

- `interface interface` (OPTIONAL) Enter the keyword `interface`, followed by the ID of the specific interface for which to display PVLAN status.

**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 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 23-1. 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

FTOS# show interfaces private-vlan TenGig 2/2
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
TenGig 2/2    100  Isolated   Host Up
```

**Figure 23-2. 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 23-1 defines the fields in the output, above.**

**Table 23-1. show interfaces Command Description**

<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>

**Related Commands**

- `private-vlan mode` Sets the mode of the selected VLAN to community, isolated, or primary.
- `show vlan private-vlan` Displays the PVLANs and/or interfaces that are part of a PVLAN.
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 23-3. show vlan private-vlan Command Example**

```
FTOS# show vlan private-vlan
Primary Secondary Type  Active Ports
---------- --------- ------ ------------------------
10        primary  Yes  TenGig 2/1,3
100       isolated Yes  TenGig 2/2
101       community Yes  TenGig 2/10
20        primary  Yes  Po 10, 12-13
           TenGig 3/1
200       isolated Yes  TenGig 3/2,4-6
201       community No
202       community Yes  TenGig 3/11-12
```
If the VLAN ID is that of a primary VLAN, then the entire private VLAN output will be displayed, as shown in Figure 23-8. 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 23-9.

Figure 23-4.  show vlan private-vlan Command Example (Primary)

FTOS# show vlan private-vlan primary
Primary Secondary Type      Active Ports
------- --------- --------- ------ ------------------------
10      primary Yes    TenGig 2/1,3
20      primary Yes    TenGig 3/1,3

Figure 23-5.  show vlan private-vlan Command Example (Isolated)

FTOS# show vlan private-vlan isolated
Primary Secondary Type      Active Ports
------- --------- --------- ------ ------------------------
10      primary Yes    TenGig 2/1,3
100     isolated Yes   TenGig 2/2,4-6
200     isolated Yes   TenGig 3/2,4-6

Figure 23-6.  show vlan private-vlan Command Example (Community)

FTOS# show vlan private-vlan community
Primary Secondary Type      Active Ports
------- --------- --------- ------ ------------------------
10      primary Yes    TenGig 2/1,3
101     community Yes  TenGig 2/7-10
20      primary Yes    Po 10, 12-13
201     community No
202     community Yes  TenGig 3/11-12

Figure 23-7.  show vlan private-vlan Command Example (Interface)

FTOS# show vlan private-vlan interface TenGig 2/1
Primary Secondary Type      Active Ports
------- --------- --------- ------ ------------------------
10      primary Yes    TenGig 2/1

Figure 23-8.  Output of show vlan private-vlan (primary)

FTOS# show vlan private-vlan 10
Primary Secondary Type      Active Ports
------- --------- --------- ------ ------------------------
10      primary Yes    TenGig 2/1,3
102     isolated Yes   TenGig 0/4
101     community Yes  TenGig 2/7-10

Figure 23-9.  Output of show vlan private-vlan (secondary)

FTOS# show vlan private-vlan 102
Primary Secondary Type      Active Ports
------- --------- --------- ------ ------------------------
10      Primary Yes    Po 1
102     Isolated Yes   TenGig 0/2
Table 23-2 defines the fields in the output.

<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>

**show vlan private-vlan mapping**

Display primary-secondary VLAN mapping.

**Syntax**

show vlan private-vlan mapping

**Defaults**

none

**Command Modes**

EXEC

EXEC Privilege

**Command History**

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

**Usage Information**

The output of this command (Figure 23-10), displays the community and isolated VLAN IDs that are associated with each primary VLAN.

**Figure 23-10. show vlan private-vlan mapping Command Output**

FTOS# show vlan private-vlan mapping
Private Vlan:
Primary : 100
Isolated : 102
Community : 101
Unknown : 200

**Related Commands**

- private-vlan mode: Sets the mode of the selected VLAN to either community or isolated.
- show interfaces private-vlan: Displays the type and status of PVLAN interfaces.
- show vlan private-vlan mapping: Displays the primary-secondary VLAN mapping.
- switchport mode private-vlan: Sets PVLAN mode of the selected port.
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 23-11. switchport mode private-vlan Command Example**

```
FTOS(conf)#interface TenGigabitEthernet 2/1
FTOS(conf-if-te-2/1)#switchport mode private-vlan promiscuous

FTOS(conf)#interface TenGigabitEthernet 2/2
FTOS(conf-if-te-2/2)#switchport mode private-vlan host

FTOS(conf)#interface TenGigabitEthernet 2/3
FTOS(conf-if-te-2/3)#switchport mode private-vlan trunk

FTOS(conf)#interface port-channel 10
FTOS(conf-if-te-2/3)#switchport mode private-vlan promiscuous
```

Related Commands

- **private-vlan mode**: Sets the mode of the selected VLAN to either community or isolated.
- **private-vlan mapping secondary-vlan**: Sets the mode of the selected VLAN to primary and then associate secondary VLANs to it.
- **show interfaces private-vlan**: Displays the type and status of PVLAN interfaces.
- **show vlan private-vlan mapping**: Display the primary-secondary VLAN mapping.
Per-VLAN Spanning Tree Plus (PVST+)

Overview

The FTOS implementation of PVST+ (Per-VLAN Spanning Tree plus) is based on the IEEE 802.1d 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

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

Enter a description of the PVST+

Syntax
description {description}

To remove the description, use the no description {description} command.

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Enter a description to identify the Spanning Tree (80 characters maximum).</td>
</tr>
</tbody>
</table>

Defaults

No default behavior or values

Command Modes

SPANNING TREE PVST+ (The prompt is “config-pvst”)

Command History

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

Related Commands

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol spanning-tree pvst Enter SPANNING TREE mode on the switch.</td>
</tr>
</tbody>
</table>

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 (The prompt is “config-pvst”.)

Command History

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.3.16.1</td>
</tr>
<tr>
<td>Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>
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**

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

**Example**

**Figure 24-1. 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                                      Designated
Name      PortID   Prio Cost    Sts        Cost        Bridge ID
---------- -------- ---- ------  ----------- -------
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                                      Edge BpduFilter
Name      Role   PortID   Prio Cost    Sts        Cost    Link-type
---------- ------ -------- ---- ------- ----------- -------
Po 23      Desg   128.24   128  1600    FWD         0       P2P    No
Te 5/41    Dis    128.450  128  2000    DIS         0       P2P    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

```
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 24-2. Configuring with protocol spanning-tree pvst Command

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)#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

- disable
- show spanning-tree pvst

show spanning-tree pvst

View the Per-VLAN Spanning Tree configuration.

Syntax

```
show spanning-tree pvst [vlan vlan-id] [brief] [guard]
```

Parameters

- `vlan vlan-id` (OPTIONAL) Enter the keyword `vlan` followed by the VLAN ID. Range: 1 to 4094
- `brief` (OPTIONAL) Enter the keyword `brief` to view a synopsis of the PVST+ configuration information.
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 24-3. 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

Interface                  Designated
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  Bridge ID  Link-type  Edge  Filter
---------- ------ -------- ---- ------- --- ------- ---------- ---- -----
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    No

FTOS#
```
Example 2

**Figure 24-4. show spanning-tree pvst vlan Command**

```plaintext
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
Bpdus 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 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 24-5. show spanning-tree pvst command with EDS and LBK**

```plaintext
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
Bpdus sent 152, received 27562
Interface Designated
Name PortID Pri Cost Sts Cost Bridge ID PortID
---------- ---- ---- ---- -------------------- --------
TenGig 1/0 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223
```
Example 4  Figure 24-6.  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 24-7.  show spanning-tree pvst guard Command

FTOS#show spanning-tree pvst vlan 5 guard

<table>
<thead>
<tr>
<th>Interface</th>
<th>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>
<td></td>
</tr>
<tr>
<td>TenGig 0/2</td>
<td>0</td>
<td>FWD</td>
<td>Loopguard</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>TenGig 0/3</td>
<td>0</td>
<td>EDS(Shut)</td>
<td>Bpduguard</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Table 24-1.  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**

- **edge-port**
  - Enter the keyword `edge-port` to configure the interface as a PVST+ 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 stop sending and receiving BPDU's on port fast enabled ports.

- **err-disable**
  - Enter the keyword `err-disable` to enable the port to be put into error-disable state (EDS) if an error condition occurs.

- **vlan vlan-range**
  - Enter the keyword `vlan` followed by the VLAN number(s).
  - Range: 1 to 4094

- **cost number**
  - Enter the keyword `cost` followed by the port cost value.
  - Range: 1 to 20000
  - Defaults:
    - 10-Gigabit Ethernet interface = 2000
    - 40-Gigabit Ethernet interface = 1400
    - Port Channel interface with one 10-Gigabit Ethernet = 2000
    - Port Channel with two 10-Gigabit Ethernet = 1800
    - Port Channel with two 40-Gigabit Ethernet = 600

- **priority value**
  - Enter the keyword `priority` followed the Port priority value in increments of 16.
  - Range: 0 to 240. Default: 128

- **rootguard**
  - Enter the keyword `rootguard` to enable root guard on a PVST+ 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

**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 24-8. spanning-tree pvst vlan Command Example**

<table>
<thead>
<tr>
<th>Command Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS (conf-if-te-1/1)#spanning-tree pvst vlan 3 cost 18000</td>
<td>Place a port in an err-disabled state if it receives a PVST+ BPDU when it is members an untagged VLAN.</td>
</tr>
<tr>
<td>FTOS (conf-if-te-1/1)#end</td>
<td></td>
</tr>
<tr>
<td>FTOS (conf-if-te-1/1)#show config</td>
<td>View PVST+ configuration</td>
</tr>
<tr>
<td>interface TenGigabitEthernet 1/1</td>
<td>No ip address</td>
</tr>
<tr>
<td>switchport</td>
<td></td>
</tr>
<tr>
<td>spanning-tree pvst vlan 3 cost 18000</td>
<td></td>
</tr>
<tr>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td>FTOS (conf-if-te-1/1)#end</td>
<td></td>
</tr>
<tr>
<td>FTOS#</td>
<td></td>
</tr>
</tbody>
</table>

### Related Commands

- `show spanning-tree pvst` View PVST+ configuration

---

### spanning-tree pvst err-disable

**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 Force10 systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU.

Dell Force10 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**

```plaintext
vlan <vlan-id> forward-delay seconds
```

To return to the default setting, enter `no vlan forward-delay` command.

**Parameters**

- `vlan vlan-range` Enter the keyword `vlan` followed by the VLAN number(s).
  - Range: 1 to 4094
- `forward-delay seconds` Enter the keyword `forward-delay` 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

**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+ 7Bridge Protocol Data Units (BPDUs).

**Syntax**

```plaintext
vlan <vlan-id> hello-time seconds
```

To return to the default value, enter `no vlan hello-time` command.

**Parameters**

- `vlan vlan-range` Enter the keyword `vlan` followed by the VLAN number(s).
  - Range: 1 to 4094
- `hello-time seconds` Enter the keyword `hello-time` followed by the time interval, in seconds, between transmission of BPDUs.
  - Range: 1 to 10 seconds
  - Default: 2 seconds

**Defaults**

2 seconds

**Command Modes**

- CONFIGURATION (conf-pvst)

**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>vlan bridge-priority</td>
<td>Set the bridge-priority value</td>
</tr>
<tr>
<td>vlan forward-delay</td>
<td>Change the time interval before FTOS transitions to the forwarding state</td>
</tr>
<tr>
<td>vlan max-age</td>
<td>Change the time interval before PVST+ refreshes</td>
</tr>
<tr>
<td>show spanning-tree pvst</td>
<td>Display the PVST+ configuration</td>
</tr>
</tbody>
</table>

### 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 Force10 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><code>priority-value</code></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

- **kbps**
  - 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)

- **committed-rate**
  - Enter a number as the bandwidth in Mbps.
  - Range: 0 to 10000

- **burst-KB**
  - (OPTIONAL) Enter a number as the burst size in KB.
  - Range: 16 to 200000
  - Default: 50

- **peak peak-rate**
  - (OPTIONAL) Enter the keyword `peak` followed by a number to specify the peak rate in Mbps.
  - Range: 0 to 10000

- **vlan vlan-id**
  - (OPTIONAL) Enter the keyword `vlan` followed by a VLAN ID to police traffic to those specific VLANs.
  - Range: 1 to 4094

#### Defaults

Granularity for `committed-rate` and `peak-rate` is Mbps unless the `kbps` option is used.

**Command Mode**

INTERFACE

**Version 8.3.16.1**

Introduced on MXL 10/40GbE Switch IO Module

---

**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

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

Related Commands

- **rate-police**: Police traffic output as part of the designated policy.

- **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>
<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**

```
service-class bandwidth-percentage queue0 number queue1 number queue2 number queue3 number
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter the bandwidth-weight. The value must be a power of 2. Range 1-100.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION
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**

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

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.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list extended</code></td>
<td>Configures an extended IP ACL.</td>
</tr>
<tr>
<td><code>ip access-list standard</code></td>
<td>Configures a standard IP ACL.</td>
</tr>
<tr>
<td><code>match ip access-group</code></td>
<td>Configures the match criteria based on the access control list (ACL)</td>
</tr>
<tr>
<td><code>match ip precedence</code></td>
<td>Identifies IP precedence values as match criteria</td>
</tr>
<tr>
<td><code>match ip dscp</code></td>
<td>Configures the match criteria based on the DSCP value</td>
</tr>
<tr>
<td><code>match mac access-group</code></td>
<td>Configures a match criterion for a class map, based on the contents of the designated MAC ACL.</td>
</tr>
<tr>
<td><code>match mac dot1p</code></td>
<td>Configures a match criterion for a class map, based on a dot1p value.</td>
</tr>
<tr>
<td><code>match mac vlan</code></td>
<td>Configures a match criterion for a class map based on VLAN ID.</td>
</tr>
<tr>
<td><code>service-queue</code></td>
<td>Assigns a class map and QoS policy to different queues.</td>
</tr>
<tr>
<td><code>show qos class-map</code></td>
<td>Views the current class map information.</td>
</tr>
</tbody>
</table>

**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**

```markdown
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 set-ip-dscp 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**

<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**

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**

```markdown
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**

<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>

**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 [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.
### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-precedence-list</td>
<td>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</td>
</tr>
<tr>
<td>set-ip-dscp value</td>
<td>(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</td>
</tr>
</tbody>
</table>

### Defaults

none

### Command Modes

CLASS-MAP CONFIGURATION (conf-class-map)

### 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

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

```plaintext
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

<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

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 dot1p

Configure a match criterion for a class map, based on a dot1p value.

**Syntax**

```plaintext
match mac dot1p {dot1p-list}
```

**Parameters**

- **dot1p-list**: Enter a dot1p value.
  - Range: 0 to 7

**Defaults**

none

**Command Modes**

CLASS-MAP

**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**

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**

```plaintext
match mac vlan number
```

**Parameters**

- **number**: Enter the VLAN ID.
  - Range: 1 to 4094

**Defaults**

none

**Command Modes**

CLASS-MAP

**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**

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-queue</td>
<td>Assigns a class map and QoS policy to different queues.</td>
</tr>
<tr>
<td>policy-aggregate</td>
<td>Allows an aggregate method of configuring per-port QoS via policy maps.</td>
</tr>
<tr>
<td>service-policy input</td>
<td>Applies an input policy map to the selected interface.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-queue</td>
<td>Assigns a class map and QoS policy to different queues.</td>
</tr>
<tr>
<td>policy-aggregate</td>
<td>Allows an aggregate method of configuring per-port QoS via policy maps.</td>
</tr>
<tr>
<td>service-policy output</td>
<td>Applies an output policy map to the selected interface.</td>
</tr>
</tbody>
</table>

**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
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 “show qos statistics” command is reset.

Related Commands
rate-police
Incoming traffic policing function

qos-policy-output
Create a QoS output policy.

Syntax
qos-policy-output qos-policy-name

Parameters
qos-policy-name
Enter your output QoS policy name in character format (32 character maximum).

Defaults
none

Command Modes
CONFIGURATION

Usage Information
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.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kbps</td>
<td>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)</td>
</tr>
<tr>
<td>committed-rate</td>
<td>Enter the committed rate in Mbps. Range: 0 to 10000 Mbps</td>
</tr>
<tr>
<td>burst-KB</td>
<td>(OPTIONAL) Enter the burst size in KB. Range: 16 to 200000 KB Default: 100 KB</td>
</tr>
<tr>
<td>peak peak-rate</td>
<td>(OPTIONAL) Enter the keyword peak followed by the peak rate in Mbps. Range: 0 to 10000 Mbps Default: Same as designated for committed-rate</td>
</tr>
</tbody>
</table>

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 police Specifies traffic policing on the selected interface.
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kbps</td>
<td>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)</td>
</tr>
<tr>
<td>rate</td>
<td>Enter the outgoing rate in multiples of 10 Mbps. Range: 10 to 10000</td>
</tr>
<tr>
<td>burst-KB</td>
<td>(OPTIONAL) Enter a number as the burst size in KB. Range: 0 to 10000 Default: 50</td>
</tr>
</tbody>
</table>

Defaults
Burst size is 50 KB. Granularity for rate is Mbps unless the kbps option is used.

Command Modes
QOS-POLICY-OUT
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.

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)

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 25-1. 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 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

**Figure 25-2. 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 diffserv
Queue#  Class-map-name  Qos-policy-name
0       -              q0
1       CM1            q1
2       CM2            q2
3       CM3            q3
FTOS#
```

Example 2

**Figure 25-3. 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                      -
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 25-4.  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 quesPolicyInput
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

- **qos-policy-name**: Enter the QoS policy name.

Defaults
none

Command Modes
- EXEC
- EXEC Privilege

Command History

- Introduced on MXL 10/40GbE Switch IO Module

Example

```plaintext
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

- **qos-policy-name**: Enter the QoS policy name.

Defaults
none

Command Modes
- EXEC
- EXEC Privilege

Command History

- Introduced on MXL 10/40GbE Switch IO Module
**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 25-2. 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</td>
</tr>
<tr>
<td></td>
<td>incremented in this field.</td>
</tr>
</tbody>
</table>

Example 2

Figure 25-9. 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 25-3. 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
Example

Figure 25-10. show qos wred-profile Command Example

```
FTOS#show qos wred-profile

 Wred-profile-name       min-threshold   max-threshold
 wred_drop               0               0
 wred_ge_y               1024            2048
 wred_ge_g               2048            4096
 wred_teng_y             4096            8192
 wred_teng_g             8192            16384
 WRED1                   2000            7000
```

### 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-map</td>
<td>Enter the policy map name.</td>
</tr>
<tr>
<td>stack-unit number</td>
<td>(OPTIONAL) Enter the keyword stack-unit followed by the stack-unit number.</td>
</tr>
<tr>
<td>stack-unit all</td>
<td>(OPTIONAL) Enter the keywords stack-unit all to indicate all stack units.</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**

Figure 25-11. 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></td>
<td></td>
<td>L2ACL</td>
<td>500</td>
<td>200</td>
<td>Allowed (2)</td>
</tr>
<tr>
<td>0</td>
<td>0</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></td>
<td></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.

### 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**

- none

**Command Modes**

- CONFIGURATION (conf-policy-map-in)

**Command History**

- Introduced on MXL 10/40GbE Switch IO Module

### Table 25-4. test cam-usage Command Description

<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>
</tbody>
</table>
| Available CAM | Indicates the free CAM space, in the partition, for the classification rules.
  - **Note:** 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. |
| Estimated CAM per Port | Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface.
  - **Note:** 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. |
| Status (Allowed ports) | 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. |
Usage Information

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>
<thead>
<tr>
<th>Table 25-5. Standard Default DSCP Mapping Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP/CP hex range (XXX)</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>111XXX</td>
</tr>
<tr>
<td>110XXX</td>
</tr>
<tr>
<td>101XXX</td>
</tr>
<tr>
<td>100XXX</td>
</tr>
<tr>
<td>011XXX</td>
</tr>
<tr>
<td>010XXX</td>
</tr>
<tr>
<td>001XXX</td>
</tr>
<tr>
<td>000XXX</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_ecn`,

- **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
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

- **wred-profile-name**: 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`

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 Force10 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
• show running-config rip
• timers basic
• version

**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
(metric metric-value)
(route-map map-name)

Defaults

Disabled
metric: 1

Command Modes

ROUTER RIP

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**

- `number` Specify a number.
  - Range: 1 to 16.
  - The default is 1.

**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**

- `description` Enter a description to identify the RIP protocol (80 characters maximum).

**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.

**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** (OPTIONAL): 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**

- `default-metric`: Assigns one distance metric to all routes learned using the `redistribute` command.

### 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 [interface]` 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip prefix-list</td>
<td>Enters PREFIX-LIST mode and configures a prefix list.</td>
</tr>
</tbody>
</table>

## 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

- **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 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.
- **connected**: (OPTIONAL) Enter the keyword `connected` to filter only directly connected routes.
- **ospf**: (OPTIONAL) Enter the keyword `ospf` to filter all OSPF routes.
- **static**: (OPTIONAL) Enter the keyword `static` to filter manually configured routes.

### Defaults

Not configured.

### Command Modes

- **ROUTER RIP**

### Command History

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

## 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
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

ip split-horizon Sets the RIP routing updates to exclude routing prefixes.

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.

The default is RIPv1.

2 (OPTIONAL) Enter the number 2 for RIP version 2.

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

ip split-horizon Sets the RIP routing updates to exclude routing prefixes.
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address, in dotted decimal format, of a router with which to exchange information.</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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive-interface</td>
<td>Sets the interface to only listen to RIP broadcasts.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Specify an IP network address in dotted decimal format. You cannot specify a subnet.</td>
</tr>
</tbody>
</table>

Defaults

No RIP network is configured.

Command Modes

ROUTER RIP

Command History

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

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>prefix-list-name</code></td>
<td>Enter the name of an established Prefix list to determine which incoming routes will be modified.</td>
</tr>
<tr>
<td><code>offset</code></td>
<td>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.</td>
</tr>
<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 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, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER RIP

**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 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
```

To return to the switch software defaults for interpacket delay, use the `no output-delay` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delay</code></td>
<td>Specify a number of milliseconds as the delay interval. Range: 8 to 50</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER RIP

**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**

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.

```
Parameters

interface 

Enter the following 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**

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.

```
Parameters

connected

Enter the keyword connected to specify that information from active routes on interfaces
is redistributed.

static

Enter the keyword static to specify that information from static routes is redistributed.
```

Defaults

Not configured.

Command Modes

ROUTER RIP

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-information originate</td>
<td>Generates a default route for RIP traffic.</td>
</tr>
</tbody>
</table>

## 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**

- **process-id**
  - Enter a number that corresponds to the OSPF process ID to be redistributed.
  - Range: 1 to 65535.

- **match external {1 | 2}**
  - (OPTIONAL) Enter the keywords `match external` followed by the numbers 1 or 2 to indicated that external 1 routes or external 2 routes should be redistributed.

- **match internal**
  - (OPTIONAL) Enter the keywords `match internal` to indicate that internal routes should be redistributed.

- **metric metric-value**
  - (OPTIONAL) Enter the keyword `metric` followed by a number as the metric value.
  - Range: 0 to 16

- **route-map map-name**
  - (OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map.

**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.
### 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**

```plaintext
show config
```

**Command Modes**

- ROUTER RIP

**Example**

```plaintext
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**

```plaintext
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

**Example**

```plaintext
FTOS(conf-router_rip)#show config
!
router rip
  network 172.31.0.0
  passive-interface TenGigabitEthernet 0/1
FTOS(conf-router_rip)#
```
show running-config rip

Use this feature to display the current RIP configuration.

Syntax show running-config rip

Defaults none

Command Modes EXEC Privilege

Example

Figure 26-4. show running-config rip Command Example

```
show running-config rip
!
routing 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

    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><strong>invalid</strong></td>
<td>Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The <code>invalid</code> value should be at least three times the <code>update</code> timer value.</td>
</tr>
<tr>
<td><strong>holddown</strong></td>
<td>Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The <code>holddown</code> value should be at least three times the <code>update</code> timer value.</td>
</tr>
<tr>
<td><strong>flush</strong></td>
<td>Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The <code>flush</code> value should be greater than the <code>update</code> value.</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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enter the keyword 1 to specify RIP version 1.</td>
</tr>
<tr>
<td>2</td>
<td>Enter the keyword 2 to specify RIP version 2.</td>
</tr>
</tbody>
</table>
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 Force10 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

```
show rmon history
show rmon log
show rmon statistics
```

```
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.</td>
</tr>
<tr>
<td><code>variable</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>interval</code></td>
<td>Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds</td>
</tr>
<tr>
<td><code>delta</code></td>
<td>Enter the keyword <code>delta</code> to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.</td>
</tr>
<tr>
<td><code>absolute</code></td>
<td>Enter the keyword <code>absolute</code> to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.</td>
</tr>
<tr>
<td><code>rising-threshold value</code></td>
<td>Enter the keyword <code>rising-threshold</code> 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.</td>
</tr>
<tr>
<td><code>falling-threshold value</code></td>
<td>Enter the keyword <code>falling-threshold</code> 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.</td>
</tr>
<tr>
<td><code>owner string</code></td>
<td>(OPTIONAL) Enter the keyword <code>owner</code> followed by the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.</td>
</tr>
</tbody>
</table>

#### Default

| Default     | owner |

#### Command Modes

| 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>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON Event Table.</td>
</tr>
<tr>
<td>log</td>
<td>(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</td>
</tr>
<tr>
<td>trap community</td>
<td>(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</td>
</tr>
<tr>
<td>description string</td>
<td>(OPTIONAL) Enter the keyword description followed by a string describing the event.</td>
</tr>
<tr>
<td>owner name</td>
<td>(OPTIONAL) Enter the keyword owner followed by the name of the owner of this event.</td>
</tr>
</tbody>
</table>

Defaults

as described above

Command Modes

CONFIGURATION

Command History

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.</td>
</tr>
<tr>
<td>variable</td>
<td>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.</td>
</tr>
<tr>
<td>interval</td>
<td>Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds</td>
</tr>
<tr>
<td>delta</td>
<td>Enter the keyword delta to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.</td>
</tr>
<tr>
<td>absolute</td>
<td>Enter the keyword absolute to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.</td>
</tr>
</tbody>
</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 27-1. 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
  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>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 <code>brief</code> 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 27-2. 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 27-3. show rmon alarms brief Command Example

```plaintext
FTOS#show rmon alarm br
index SNMP OID
------------------------------------------
- 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

- **index**: (OPTIONAL) Enter the table index number to display just that entry.
- **brief**: (OPTIONAL) Enter the keyword brief to display the RMON Event Table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

- Introduced on MXL 10/40GbE Switch IO Module

Example 1

**Figure 27-4. 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 27-5. 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
index (OPTIONAL) Enter the table index number to display just that entry.

brief (OPTIONAL) Enter the keyword brief to display the RMON High-Capacity Alarm 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 27-6. 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
FTOS#
```

Example 2
Figure 27-7. 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
FTOS#
```

show rmon history

Display the contents of the RMON Ethernet History table.

Syntax
show rmon history [index] [brief]

Parameters
index (OPTIONAL) Enter the table index number to display just that entry.

brief (OPTIONAL) Enter the keyword brief to display the RMON Ethernet History table in an easy-to-read format.

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 27-10. 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#
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.

Example 2

Example 2 Figure 27-11. show rmon log brief Command Example

<table>
<thead>
<tr>
<th>eventIndex</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

show rmon statistics

Display the contents of RMON ethernet statistics table.

Syntax

show rmon statistics [index] [brief]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>(OPTIONAL) Enter the index number to display just that entry.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to display the RMON Ethernet Statistics 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 27-12.  show rmon statistics index Command Example

```
FTOS#show rmon statistics 6001
RMON statistics entry 6001
   interface: ifIndex.100974631 TenGigabitEthernet 2/1
   packets dropped: 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
FTOS#
```
Rapid Spanning Tree Protocol (RSTP)

Overview

The Dell Force10 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

Parameters

- **priority-value**
  - Enter a number as the bridge priority value in increments of 4096.
  - Range: 0 to 61440
  - Default: 32768

Defaults

32768
**debug spanning-tree rstp**

Enable debugging of RSTP and view information on the protocol.

**Syntax**

```plaintext
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.
  (OPTIONAL) 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**

**Figure 28-1. debug spanning-tree rstp bpdu Command Example**

```plaintext
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**

```plaintext
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)

Related Commands
protocol spanning-tree rstp

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)

Related Commands
protocol spanning-tree rstp

Description

Enter a description to identify the Rapid Spanning Tree (80 characters maximum).

Parameters

description

Defaults
none

Command Modes
SPANNING TREE (The prompt is “config-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.
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 \((x/1000)*256\).

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

Related Commands
- max-age
  Changes the wait time before RSTP transitions to the Forwarding state.
- hello-time
  Changes the time interval between BPDUs.

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

Related Commands
- max-age
  Changes the wait time before RSTP transitions to the Forwarding state.
- hello-time
  Changes the time interval between BPDUs.

Example

Figure 28-2.  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.
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 28-3. 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
**Example 1**  
**Figure 28-4. show spanning-tree rstp brief Command Example**

```
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</th>
<th>Bridge ID</th>
<th>PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGig 4/0</td>
<td>128.418 128</td>
<td>20000</td>
<td>FWD 20000</td>
</tr>
<tr>
<td>TenGig 4/1</td>
<td>128.419 128</td>
<td>20000</td>
<td>FWD 20000</td>
</tr>
<tr>
<td>TenGig 4/8</td>
<td>128.426 128</td>
<td>20000</td>
<td>FWD 20000</td>
</tr>
<tr>
<td>TenGig 4/9</td>
<td>128.427 128</td>
<td>20000</td>
<td>BLK 20000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Bpdu</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGig 4/0</td>
<td>No</td>
</tr>
<tr>
<td>TenGig 4/1</td>
<td>No</td>
</tr>
<tr>
<td>TenGig 4/8</td>
<td>No</td>
</tr>
<tr>
<td>TenGig 4/9</td>
<td>No</td>
</tr>
</tbody>
</table>
```

FTOS#
Example 2

Figure 28-5. 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          | Name  | 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 28-6. show spanning-tree rstp guard Command Example

```
FTOS#show spanning-tree rstp 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 BLK      Bpduguard  No
```

Table 28-1. 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

```plaintext
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 28-7. 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**

<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>
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 Force10 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

```
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

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

Example

```
FTOS(conf)# aaa accounting exec default start-stop tacacs+
FTOS(conf)# aaa accounting command 15 default start-stop tacacs+
```

Usage Information

In Figure 29-1, 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

```plaintext
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

```plaintext
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

```plaintext
show accounting
```

Defaults

none
Command Modes

EXEC

Command History

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

Example

Figure 29-2. show accounting Command Example

```
FTOS#show accounting
Active accounted actions on tty2, User admin Priv 1
  Task ID 1, EXEC Accounting record, 00:00:39 Elapsed, service=shell
Active accounted actions on tty3, User admin Priv 1
  Task ID 2, EXEC Accounting record, 00:00:26 Elapsed, service=shell

FTOS#
```

Usage Information

This command steps through all active sessions and then displays the accounting records for the active account functions.

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
```
### 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 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

**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 exec

Set parameters that restrict (or permit) a user’s access to EXEC-level commands.

Syntax

```
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 MXL 10/40GbE Switch IO Module

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

Syntax

```
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 the ROUTE-MAP
  - `router` for the ROUTER OSPF, ROUTER RIP, and ROUTER BGP modes.
- **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 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

aaa authentication enable \{default | method-list-name\} method [... method2]

Parameters

- **default**: Enter the keyword default followed by the authentication methods to use as the default sequence of methods to be used for the Enable log-in.
  
  Default: default enable

- **method-list-name**: Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at log in.

- **method**: Enter one of the following methods:
  - **enable**: use the password defined by the enable password command in the CONFIGURATION mode.
  - **line**: use the password defined by the password command in the LINE mode.
  - **none**: no authentication.
  - **radius**: use the RADIUS server(s) configured with the radius-server host command.
  - **tacacs+**: use the TACACS+ server(s) configured with the tacacs-server host command.

- **method2**: (OPTIONAL) In the event of a “no response” from the first method, FTOS applies the next configured method.

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

- **enable password**: Changes the password for the enable command.
- **login authentication**: Enables AAA login authentication on terminal lines.
- **password**: Creates a password.
- **radius-server host**: Specifies a RADIUS server host.
- **tacacs-server host**: Specifies a TACACS+ server host.
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.

Parameters

<table>
<thead>
<tr>
<th>Parameter</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 default to specify that the method list specified is the default method for all terminal lines.</td>
</tr>
</tbody>
</table>
| `method`        | Enter one of the following methods:  
|                 | • enable - use the password defined by the enable password command in the CONFIGURATION mode.  
|                 | • line - use the password defined by the password command in the LINE mode.  
|                 | • local - use the user name/password defined by the in the local configuration.  
|                 | • none - no authentication.  
|                 | • radius - use the RADIUS server(s) configured with the radius-server host command.  
|                 | • tacacs+ - use the TACACS+ server(s) configured with the tacacs-server host command. |
| `... method4`   | (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). |

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>
<th>login authentication</th>
<th>Applies an authentication method list to designated terminal lines.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>password</td>
<td>Creates a password.</td>
</tr>
<tr>
<td></td>
<td>radius-server host</td>
<td>Specifies a RADIUS server host.</td>
</tr>
<tr>
<td></td>
<td>tacacs-server host</td>
<td>Specifies a 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**

```
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**

```
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 Force10 router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Force10 router.
- **password**: Enter a text string, up to 32 characters long, as the clear text password.
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`. 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 within the switch.

enable restricted

Allows Dell Force10 technical support to access restricted commands.

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 Force10 router.
  Use this parameter only with a password that you copied from the show running-config file of another Dell Force10 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 Force10 Technical Support staff use this command.
enable secret

Change the password for the enable command.

Syntax

```
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 Force10 router.
  - Use this parameter only with a password that you copied from the show running-config file of another Dell Force10 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

```
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min-length number</td>
<td>(OPTIONAL) Enter the keyword min-length followed by the number of characters. Range: 0 - 32 characters</td>
</tr>
<tr>
<td>max-retry number</td>
<td>(OPTIONAL) Enter the keyword max-retry followed by the number of maximum password retries. Range: 0 - 16</td>
</tr>
<tr>
<td>character-restriction</td>
<td>(OPTIONAL) Enter the keyword character-restriction to indicate a character restriction for the password.</td>
</tr>
<tr>
<td>upper number</td>
<td>(OPTIONAL) Enter the keyword upper followed the upper number. Range: 0 - 31</td>
</tr>
<tr>
<td>lower number</td>
<td>(OPTIONAL) Enter the keyword lower followed the lower number. Range: 0 - 31</td>
</tr>
<tr>
<td>numeric number</td>
<td>(OPTIONAL) Enter the keyword numeric followed the numeric number. Range: 0 - 31</td>
</tr>
<tr>
<td>special-char number</td>
<td>(OPTIONAL) Enter the keyword special-char followed the number of special characters permitted. Range: 0 - 31</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.16.1</td>
<td>Introduced</td>
<td>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>password</td>
<td>Specifies a password for users on terminal lines.</td>
</tr>
</tbody>
</table>
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

Usage Information
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.

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 29-3. show privilege Command Example

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>privilege level (CONFIGURATION mode)</td>
<td>Assigns access control to different command modes.</td>
</tr>
</tbody>
</table>
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       | Introduced on MXL 10/40GbE Switch IO Module |

Example

**Figure 29-4. show users Command Example**

```
FTOS#show user
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 1 show users Command Description**

<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
```

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]
```

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` user command.
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**

```
display 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**

```
ipo 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

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.
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.

```
auth-port port-number
retransmit retries
timeout seconds
key [encryption-type] key
```

**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.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>login authentication</td>
</tr>
<tr>
<td>radius-server key</td>
</tr>
<tr>
<td>radius-server retransmit</td>
</tr>
<tr>
<td>radius-server timeout</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

Parameters

seconds

Enter the number of seconds between an unsuccessful attempt and the FTOS times out.

Range: zero (0) to 1000 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
debug tacacs+

To disable debugging of TACACS+, use the no debug tacacs+ command.

Defaults

Disabled.

Command Modes

EXEC Privilege
The image contains two sections of text. The first section is about the `ip tacacs source-interface` command, which specifies an interface’s IP address as the source IP address for TACACS+ connections. The command syntax is:

```
ip tacacs source-interface interface
```

This command is used to specify which interface's IP address will be used as the source IP address for TACACS+ connections. To delete a source interface, you can use the `no ip tacacs source-interface` command.

The second section is about the `tacacs-server host` command, which specifies a TACACS+ host. The command syntax is:

```
tacacs-server host {hostname | ipv4-address} [port number] [timeout seconds] [key key]
```

This command is used to specify a TACACS+ server host. The parameters include specifying the host name or IP address, port number, timeout seconds, and a key for encryption.

Both sections include details on how to configure these commands, including their parameters and default settings.
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</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
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication login</td>
<td>Specifies the login authentication method.</td>
</tr>
<tr>
<td>tacacs-server key</td>
<td>Configures a TACACS+ key for the TACACS server.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</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 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**

- **rsa**
  - Enter the keyword `rsa` followed by the key size to generate a SSHv2 RSA host keys.
  - Range: 1024 to 2048
  - Default: 1024

- **rsa1**
  - Enter the keyword `rsa1` followed by the key size to generate a SSHv1 RSA host keys.
  - Range: 1024 to 2048
  - Default: 1024

**Defaults**

Key size 1024

**Command Modes**

CONFIGURATION

**Command History**

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

ddebug ip ssh {client | server}

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 todir

Identify a location for files used in secure copy transfer.

Syntax

ip scp todir directory

To return to the default setting, use the no ip scp todir command.
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.

---

**ip ssh authentication-retries**

Configure the maximum number of attempts that should be used to authenticate a user.

Syntax

```plaintext
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.

---

**ip ssh connection-rate-limit**

Configure the maximum number of incoming SSH connections per minute.

Syntax

```plaintext
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

*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

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

**Example**

```plaintext
Figure 29-6.  ip ssh pub-key-file Command 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 AAAAB3NzaC1yc2EAAAABlwAAAIEAox/QQp8xYhzOxt07yh4VGIPAoUfgKoieTWO9G4sNV+ui+DWEc3cgYAcU5Lai1MU2ODzhCwyDNp0stKBU3tReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc+Rs4p2uzrV0F4pRKnaXdH3Lk4D460HZRlhVrxqeNxPDpEnW1MPJIods= ashwani@poclab4```

**Note:** For rhostfile and pub-key-file, the administrator must FTP the file to the switch.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ssh client-pub-keys</code></td>
<td>Displays the client-public keys used for the host-based authentication.</td>
</tr>
</tbody>
</table>

### 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**

```
Figure 29-7.  ip ssh rhostsfile Command Example

FTOS#conf
FTOS(conf)# ip ssh rhostsfile flash://shosts
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/shosts 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-userame
```

(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**

- **enable**
  
  Enter the key word `enable` to start the SSH server.

- **port port-number**
  
  (OPTIONAL) Enter the keyword `port` followed by the port number of the listening port on the SSH server.
  
  Range: 1 to 65535
  
  Default: 22

- **[version {1 | 2}]**
  
  (OPTIONAL) Enter the keyword `version` followed by the SSH version 1 or 2 to specify only SSHv1 or SSHv2.

**Defaults**

Default listening port is 22.

**Command Modes**

CONFIGURATION

**Command History**

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**

```
Figure 29-8.  ip ssh server port Command Example

FTOS# conf
FTOS(conf)# ip ssh server port 45
FTOS(conf)# ip ssh server enable
FTOS#
```

**Related Commands**

- `show ip ssh`
  
  Displays the ssh information

--

show crypto

Display the public part of the SSH host-keys.

**Syntax**

```
show crypto key mypubkey {rsa | rsa1}
```

**Parameters**

- **Key**
  
  Enter the keyword `key` to display the host public key.

- **mypubkey**
  
  Enter the keyword `mypubkey` to display the host public key.
### show crypto key

#### Description

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.

#### Syntax

```
rsa
rsa1
```

- **rsa**: Enter the keyword `rsa` to display the host SSHv2 RSA public key.
- **rsa1**: Enter the keyword `rsa1` to display the host SSHv1 RSA public key.

#### Defaults

- **rsa**: none
- **rsa1**: none

#### Command Modes

- EXEC

#### Command History

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

#### Example

**Figure 29-9. show crypto Command Examples**

FTOS#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAAB1wAAAIEAtzkZME/e8V8mmXR22EJBQo9cNKEKmuia+OILVoMYU1ZKGfjW5BPCSvF/x51fgYFFWuzJNOcsJK7vjSanmMhChFYZSvXi1VtJ6h97IFJAqI0sgd0ycpoc5F+DNLKfJnx7SAjhaFQMwGg/q78ZkDT3Ydr8KKjfsi14Bg/NS8B740=

FTOS#show crypto key mypubkey rsa1
1024 35
13106005154808733989532575153724965785007220644294963674080935683088961020317226679895675466676250637962218977992760927852363839223055081191660099281326164086634357746022192295189039929663345791173742474315537505816769296027379060149443405000001517986442562961338577491923608177134105953360063913083

FTOS#

**Usage Information**

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**

- **crypto key generate**: Generates SSH keys.

---

### show ip ssh

#### Description

Display information about established SSH sessions.

#### Syntax

```
show ip ssh
```

#### Command Modes

- EXEC
- EXEC Privilege

#### Example

**Figure 29-10. show ip ssh Command Example**

```
FTOS#show ip ssh
2#show ip ssh
SSH server : disabled.
SSH server version : v1 and v2.
Password Authentication : enabled.
Hostbased Authentication : disabled.
RSA Authentication : disabled.
FTOS#
```

#### Related Commands

- `ip ssh server`: Configures an SSH server.
- `show ip ssh client-pub-keys`: Displays the client-public 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 29-11.  show ip ssh client-pub-keys Command Example

FTOS#show ip ssh client-pub-keys
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/Qp8yxzOxn7y94VgPaoUIfgKol5TH0994eNV+ui+iR4Ec3cqYAc0SLa1lMU20DrzhCwyDNp0StKBt3tReG1o8AxLi6+S4HyEMqHzkzBFNVqHzpQc+Rs4p2urzV0F4pRkNaXdhf3Lk4D460HZRhhVrxqeNxFDPenWIMPJ10ds= ashwan@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 29-12.  show ip ssh rsa-authentication Command Example

FTOS#show ip ssh rsa-authentication my-authorized-keys
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB1714qFp4r2DRH1vMc1Vz0sG5QxRVly1X1JOMe06Nd0uYzyrQMM4qJuBoTne0XfLBcHf3V2hcMiqa2ZN+CRChw/zCMlnCF0+qYldoofsea5r9S0ytP0CMfHXZ3NuGcQ90v33m9+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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 65536</td>
</tr>
<tr>
<td></td>
<td>Default: 22</td>
</tr>
<tr>
<td>-v {1</td>
<td>2}</td>
</tr>
<tr>
<td></td>
<td>Default: The version from the protocol negotiation</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 29-13. 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 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**

<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**

- `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**

<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>
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 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

Default
EXEC Privilege

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 Force10 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.
Commands

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow collector ipv4-address</td>
<td>Enter the IPv4 (A.B.C.D) of the sFlow collector device.</td>
</tr>
<tr>
<td>agent-addr ipv4-address</td>
<td>Enter the IPv4 (A.B.C.D) of the sFlow agent in the router.</td>
</tr>
<tr>
<td>number</td>
<td>(OPTIONAL) Enter the UDP port number (User Datagram Protocol). Range: 0 to 65535 Default: 6343</td>
</tr>
<tr>
<td>max-datagram-size number</td>
<td>(OPTIONAL) Enter the keyword max-datagram-size followed by the size number in bytes. Range: 400 to 1500 Default: 1400</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

**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

| enable | Enter the keyword enable to enable global extended information. |

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

<table>
<thead>
<tr>
<th>interval value</th>
<th>Enter the interval value in seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range: 15 to 86400 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 20 seconds</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval value</td>
<td>Enter the interval value in seconds.</td>
</tr>
<tr>
<td></td>
<td>Range: 15 to 86400 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: The current global default counter polling interval</td>
</tr>
</tbody>
</table>

Defaults
The same value as the current global default counter polling interval.

Command Modes
INTERFACE

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 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Enter the sampling rate value.</td>
</tr>
<tr>
<td></td>
<td>Range: 256 to 8388608 packets</td>
</tr>
<tr>
<td></td>
<td>Enter values in powers of 2 only, for example 4096, 8192, 16384 etc.</td>
</tr>
<tr>
<td></td>
<td>Default: 32768 packets</td>
</tr>
</tbody>
</table>

Defaults
32768

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>

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

Command History

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

Example

    Figure 30-2.  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#
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 Force10 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 Force10 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**

Figure 31-1. show snmp Command 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
```
Simple Network Management Protocol (SNMP) and Syslog

show snmp engineID

Display the group name, security model, status, and storage type of each group.

Syntax

show snmp group

Command Modes

EXEC
EXEC Privilege

Command History

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

Usage Information

Figure 31-3 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.

Example

Figure 31-3. show snmp group Command Example

Related Commands

snmp-server engineID Configures local and remote SNMP engines on the router.

show snmp group

Display the information configured on each SNMP user name.

Syntax

show snmp user

Command Modes

EXEC
EXEC Privilege

Command History

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

Usage Information

Related Commands

snmp-server group Configures an SNMP server group
**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**

EXEC

EXEC Privilege

**Command History**

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

**Example**

```
Example Figure 31-5. snmp ifmib ifalias long Command Example

FTOS#snmp ifmib ifalias long 
!------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. 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 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 31-6 configures a community named guest that is mapped to the security named guestuser with Read Only (ro) permissions.

**Example**

**Figure 31-6. 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:

- vl1v2creadu / vl1v2creadg — maps to a community with ro permissions
- vl1v2cwriteu/ vl1v2cwriteg — 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 31-7 shows the creation of a standard IPv4 ACL called “snmp-ro-acl” and then assigning it to the SNMP community “guest”:

**Example**

**Figure 31-7. snmp-server community Command Example**

```
FTOS(conf)# ip access-list standard snmp-ro-acl
FTOS(conf-std-nacl)#seq 5 permit host 10.10.10.224
FTOS(conf-std-nacl)#seq 10 deny any count
!
FTOS(conf)#snmp-server community guest ro snmp-ro-acl
FTOS(conf)#
```
snmp-server contact

Configure contact information for troubleshooting this SNMP node.

**Syntax**

```
snmp-server contact text
```

To delete the SNMP server contact information, use the `no snmp-server contact` command.

**Parameters**

- **text**: Enter an alphanumeric text string, up to 55 characters long.

**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**

```
snmp-server enable traps [notification-type] [notification-option]
```

To disable traps, use the `no snmp-server enable traps [notification-type] [notification-option]` command.
### Parameters

<table>
<thead>
<tr>
<th>notification-type</th>
<th>Enter the type of notification from the list below:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecfm</td>
<td>Notification of changes to ECFM</td>
</tr>
<tr>
<td>entity</td>
<td>Notification of changes to entity</td>
</tr>
<tr>
<td>envmon</td>
<td>Device notification when an environmental threshold is exceeded</td>
</tr>
<tr>
<td>eoam</td>
<td>Notification of changes to the EOAM state</td>
</tr>
<tr>
<td>ets</td>
<td>Notification of changes to the ets traps</td>
</tr>
<tr>
<td>fips</td>
<td>Notification of changes to the FIP snooping state</td>
</tr>
<tr>
<td>lACP</td>
<td>Notification of changes to the LACP state</td>
</tr>
<tr>
<td>pfC</td>
<td>Notification of changes to pfC traps</td>
</tr>
<tr>
<td>snmp</td>
<td>Notification of RFC 1157 traps.</td>
</tr>
<tr>
<td>stp</td>
<td>Notification of state change in Spanning Tree protocol (RFC 1493)</td>
</tr>
<tr>
<td>vrrp</td>
<td>Notification of state change in a VRRP group</td>
</tr>
<tr>
<td>xstp</td>
<td>Notification of state change in MSTP (802.1s), RSTP (802.1w), and PVST+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>notification-option</th>
<th>For the envmon notification-type, enter one of the following optional parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>temperature</td>
<td></td>
</tr>
</tbody>
</table>

For the snmp notification-type, enter one of the following optional parameters:

- authentication
- coldstart
- linkdown
- linkup

### Defaults

Not enabled.

### Command Modes

CONFIGURATION

### Command History

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

### Usage Information

FTOS supports up to 16 SNMP trap receivers.

If you do not configure this command, no traps controlled by this command are sent. If you do not specify a `notification-type` and `notification-option`, all traps are enabled.

### Related Commands

- `snmp-server community` Enables SNMP and set the community string.

---

### `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.

---

Simple Network Management Protocol (SNMP) and Syslog | 585
### Parameters

| **local engineID** | Enter the keyword `local` followed by the engine ID number that identifies the copy of the SNMP on the `local` device. Format (as specified in RFC 3411): 12 octets.
| **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 engineID** | Enter the keyword `udp-port` followed by the UDP (User Datagram Protocol) port number on the remote device. Range: 0 to 65535 Default: 162 |

### 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

| **show snmp engineID** | Displays SNMP engine and all remote engines that are configured on the router. |
| **show running-config snmp** | Displays the SNMP running configuration. |

### 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

**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.

- v1v2creadg — maps to a community/security-name with ro permissions
- v1v2cwriteg — maps to a community/security-name rw permissions

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

**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.

**read name**

(Optional) Enter the keyword **read** 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.

**write name**

(Optional) Enter the keyword **write** followed by a name (a string of up to 20 characters long) as the write view name.

**notify name**

(Optional) Enter the keyword **notify** followed by a name (a string of up to 20 characters long) as the notify view name.

**access-list-name**

(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).

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 31-8 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

**Figure 31-8. snmp-server group Command Example**

```
FTOS#conf
FTOS(conf)# snmp-server group harig 3 priv read rview
FTOS#
```

**Note**: The number of configurable groups is limited to 16 groups.
**snmp-server host**

Configure the recipient of an SNMP trap operation.

**Syntax**

```plaintext
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.
<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.3.16.1 Introduced on MXL 10/40GbE Switch IO Module</td>
</tr>
</tbody>
</table>

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 an inform, 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><strong>snmp-server enable traps</strong></td>
<td>Enables the SNMP traps.</td>
</tr>
<tr>
<td><strong>snmp-server community</strong></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>text</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>byte-count</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
**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.

**Parameter**

- **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.

**Parameters**

- **name**
  
  Enter the name of the user (not to exceed 20 characters), on the host, that connects to the agent.

- **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.
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 31-9 shows how to specify the command with an encrypted string.

**Figure 31-9.  snmp-server user Command Example (Encrypted)**

```
FTOS# snmp-server user privuser v3group v3 encrypted auth md5 9fc53d9d908110b2804fe80e3ba8763d priv des56 d0452401a8c3ce42804fe80e3ba8763d
```
Figure 31-10 shows how to enter a plain-text password as the string authpasswd for user authuser of group v3group.

**Figure 31-10. snmp-server user Command Example (Plain-text)**
```
FTOS#conf
FTOS(conf)# snmp-server user authuser v3group v3 auth md5 authpasswd
```

Figure 31-11 configures a remote user named n3user with a v3 security model and a security level of authNOPriv.

**Figure 31-11. 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp user</td>
<td>Displays the information configured on each SNMP user name.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>view-name</td>
<td>Enter the name of the view (not to exceed 20 characters).</td>
</tr>
<tr>
<td>oid-tree</td>
<td>Enter the OID sub tree for the view (not to exceed 20 characters).</td>
</tr>
<tr>
<td>included</td>
<td>(OPTIONAL) Enter the keyword <code>included</code> to include the MIB family in the view.</td>
</tr>
<tr>
<td>excluded</td>
<td>(OPTIONAL) Enter the keyword <code>excluded</code> to exclude the MIB family in the view.</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**

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 31-12 configures a view named rview that allows access to all objects under 1.3.6.1.

**Example**

**Figure 31-12. snmp-server view Command Example**
```
FTOS#(conf) snmp-server view rview 1.3.6.1 included
```
Related Commands  

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config snmp</td>
<td>Displays the SNMP running configuration.</td>
</tr>
</tbody>
</table>

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

Command History

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

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 Force10 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
Version 8.3.16.1  Introduced on MXL 10/40GbE Switch IO Module

Related Commands
show logging  Displays logging settings and system messages in the internal buffer.

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

Related Commands
logging buffered  Sets the logging buffered parameters.

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

Related Commands
logging console  Sets the logging console parameters.
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}

To disable logging, enter no logging.

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

To return to the default values, use the no logging history command.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging history</td>
<td>Displays information logged to the history buffer.</td>
</tr>
</tbody>
</table>

logging history size

Specify the number of messages stored in the FTOS logging history table.

Syntax
logging history size size

To return to the default values, use the no logging history size command.

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

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

When the number of messages reaches the limit you set with the `logging history size` command, older messages are deleted as newer ones are added to the table.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging history</code></td>
<td>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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>level</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

Defaults

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>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><code>default logging monitor</code></td>
<td>Returns the logging monitor parameters to the default setting.</td>
</tr>
</tbody>
</table>

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

<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

When you use the `no logging on` command, messages are logged only to the console.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>logging</code></td>
<td>Enables logging to Syslog server.</td>
</tr>
<tr>
<td><code>logging buffered</code></td>
<td>Sets the logging buffered parameters.</td>
</tr>
<tr>
<td><code>logging console</code></td>
<td>Sets the logging console parameters.</td>
</tr>
<tr>
<td><code>logging monitor</code></td>
<td>Sets the logging parameters for the terminal connections.</td>
</tr>
</tbody>
</table>
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

Simple Network Management Protocol (SNMP) and Syslog | 601
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 31-13. 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 vty2 (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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit unit#</td>
<td>Enter the keyword stack-unit followed by the stack member ID of the switch for which you want to display the driver log.</td>
</tr>
<tr>
<td>Range: 0 to 1</td>
<td></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
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.
Storm Control

Overview

The Dell Force10 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

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

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

Figure 32-3. show storm-control unknown-unicast Command Example

FTOS#show storm-control unknown-unicast tengigabitethernet 3/0

Unknown-unicast storm control configuration

Interface Direction Packets/Second
TenGig 3/0 Ingress 1000

storm-control broadcast (Configuration)

Configure the packets per second of broadcast traffic.

Syntax

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 broadcast (Interface)

Configure the packets per second of broadcast traffic to be limited on the interface.

Syntax

```plaintext
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

- `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

- 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

```plaintext
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

- `packets_per_second` Enter the packets per second of multicast traffic allowed from the network.

  Range: 0 to 33554368

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**

<table>
<thead>
<tr>
<th>packs per second</th>
<th>Enter the packets per second of broadcast traffic allowed from the network. Range: 0 to 33554368</th>
</tr>
</thead>
</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

**Usage Information**

Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

**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**

<table>
<thead>
<tr>
<th>packs per second</th>
<th>Enter the packets per second of broadcast traffic allowed from the network. Range: 0 to 33554368</th>
</tr>
</thead>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

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

**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**

- **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**

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

**Defaults**

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.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show redundancy</code></td>
<td>Displays the current redundancy status.</td>
</tr>
</tbody>
</table>

### 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

### reset stack-unit

Reset any designated stack member except the management unit (master unit).

**Syntax**

```
reset stack-unit 0-5 hard
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-5</td>
<td>Enter the stack member unit identifier of the stack member to reset.</td>
</tr>
<tr>
<td>hard</td>
<td>Reset the stack unit if the unit is in a problem state.</td>
</tr>
</tbody>
</table>

**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

**Example**

Figure 33-1. 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>reset stack-unit</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 33-2. 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy disable-auto-reboot</td>
<td>Prevents the system from auto-rebooting if it fails.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>(OPTIONAL) Enter the keyword <strong>status</strong> to display the command output without the Connection field.</td>
</tr>
<tr>
<td>topology</td>
<td>(OPTIONAL) Enter the keyword <strong>topology</strong> to limit the table to just the Interface and Connection fields.</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**

**Figure 33-3. 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 33-4. 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 33-5. 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>
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

---

### Table 33-1. 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**
- `reset stack-unit`: 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 unit <unit number>`: Displays the current status of the designated stack member.
- `show system upgrade`: Upgrades the system image of the management unit.
### 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

---

### 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

---
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-5</td>
<td>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.</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
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 33-6. 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Reboots FTOS.</td>
</tr>
<tr>
<td>reset stack-unit</td>
<td>Resets the designated stack member.</td>
</tr>
<tr>
<td>show system</td>
<td>Displays the current status of all stack members or a specific member.</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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-value</td>
<td>Enter a number as the bridge priority value. Range: 0 to 65535. Default: 32768.</td>
</tr>
<tr>
<td>primary</td>
<td>Enter the keyword primary to designate the bridge as the root bridge.</td>
</tr>
<tr>
<td>secondary</td>
<td>Enter the keyword secondary to designate the bridge as a secondary root bridge.</td>
</tr>
</tbody>
</table>

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
depth spanning-tree {stp-id [all | bpdu | events | exceptions] | protocol}

Parameters
stp-id
Enter zero (0). The switch supports one Spanning Tree group with a group ID of 0.

protocol
Enter the keyword for the type of STP to debug, either mstp, pvst, or rstp.

all
(OPTIONAL) Enter the keyword all to debug all spanning tree operations.

bpdu
(OPTIONAL) Enter the keyword bpdu to debug Bridge Protocol Data Units.

events
(OPTIONAL) Enter the keyword events to debug STP events.

Command Modes
EXEC Privilege

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
portfast bpdudfilter
Enters SPANNING TREE mode on the switch.

description

Enter a description of the spanning tree.

Syntax
description {description}

Parameters
description
Enter a description to identify the Spanning Tree (80 characters maximum).

Defaults
none

Command Modes
SPANNING TREE (The prompt is “conf-stp”.)

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

**Command History**

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

**Related Commands**

- portfast bpdufilter default Enters SPANNING TREE mode.

---

**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

**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.

---

**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.
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

- **seconds**: Enter a number of seconds the FTOS waits before refreshing configuration information.
  - Range: 6 to 40
  - Default: 20 seconds.

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 global 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>stp-id</code></td>
<td>Enter zero (0). FTOS supports one Spanning Tree group, group 0.</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

---

**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

---

**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.

---

**Example**

**Figure 34-1.  protocol spanning-tree Command Example**

```
FTOS(conf)#protocol spanning-tree 0
FTOS(conf-stp)#
```

**Figure 34-2.  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

**0**

Enter 0 (zero) to display information about that specific Spanning Tree group.

**active**

(Optional) Enter the keyword active to display only active interfaces in Spanning Tree group 0.

**brief**

(Optional) Enter the keyword brief to display a synopsis of the Spanning Tree group configuration information.

**guard**

(Optional) Enter the keyword guard to display the type of guard enabled on an STP interface and the current port state.

**interface interface**

(Optional) Enter the keyword interface and 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: 1-128
- 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.

**root**

(Optional) Enter the keyword root to display configuration information on the Spanning Tree group root.

**summary**

(Optional) Enter the keyword summary to only the number of ports in the Spanning Tree group and their state.

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 34-3.  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 34-1.  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 BPU 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 34-1. 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</td>
</tr>
<tr>
<td></td>
<td>of the interface (Disabled or Enabled).</td>
</tr>
<tr>
<td>“Port path...”</td>
<td>Displays the path cost, priority, and identifier for the</td>
</tr>
<tr>
<td></td>
<td>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 34-4. 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>Designated 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>

FTOS#

Figure 34-5. 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 34-2. 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 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 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 Force10 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

- **time**: 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.
- **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`.
- **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`.
- **year**: Enter a four-digit number as the year. Range: 1993 to 2035.

Command Modes

EXEC Privilege

Command History

- Introduced on MXL 10/40GbE Switch IO Module

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

- **clock read-calendar**: Sets the software clock based on the hardware clock.
- **clock set**: Sets the software clock.
- **clock update-calendar**: Sets the hardware clock based on the software clock.
- **show clock**: Displays the clock settings.

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**

```plaintext
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**

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

**Example**

```plaintext
Figure 35-2. clock set Command Example

FTOS#clock 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`. 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 Force10 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**

```
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**

- **time-zone**
  - Enter the three-letter name for the time zone. This name is displayed in the `show clock` output.
  - You can enter up to eight characters.

- **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 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**

- `calendar set` Sets the hardware clock.
- `clock summer-time date` Sets a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.
- `show clock` Displays the current clock settings.
**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**

- **timezone-name**
  - Enter the name of the timezone. You cannot use spaces.
- **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**

- `calendar set` Sets the hardware clock.
### 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><code>adjust</code></td>
<td>Enter the keyword <code>adjust</code> to display information on NTP clock adjustments.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Enter the keyword <code>all</code> to display information on all NTP transactions.</td>
</tr>
<tr>
<td><code>authentication</code></td>
<td>Enter the keyword <code>authentication</code> to display information on NTP authentication transactions.</td>
</tr>
<tr>
<td><code>events</code></td>
<td>Enter the keyword <code>events</code> to display information on NTP events.</td>
</tr>
<tr>
<td><code>loopfilter</code></td>
<td>Enter the keyword <code>loopfilter</code> to display information on NTP local clock frequency.</td>
</tr>
<tr>
<td><code>packets</code></td>
<td>Enter the keyword <code>packets</code> to display information on NTP packets.</td>
</tr>
<tr>
<td><code>select</code></td>
<td>Enter the keyword <code>select</code> to display information on the NTP clock selection.</td>
</tr>
<tr>
<td><code>sync</code></td>
<td>Enter the keyword <code>sync</code> 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><code>ntp authentication-key</code></td>
<td>Configures the authentication key for NTP traffic.</td>
</tr>
<tr>
<td><code>ntp trusted-key</code></td>
<td>Configures a key to authenticate.</td>
</tr>
</tbody>
</table>
**ntp authentication-key**

Specify a key for authenticating the NTP server.

**Syntax**

```plaintext
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**

```plaintext
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
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
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
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 Force10 recommends limiting the number of hosts configured.

Related Commands

- show ntp associations  Displays NTP servers configured and their status.

**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.

**Command Modes**

CONFIGURATION

**Command History**

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

**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.
Defaults: Not configured.

Command Modes: CONFIGURATION

Command History:

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

Usage Information:
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.

Related Commands:
- ntp authentication-key: Sets an authentication key for NTP.
- ntp authenticate: Enables the NTP authentication parameters you set.

ntp update-calendar

Configure the FTOS to update the calendar (the hardware clock) with the NTP-derived time.

Syntax:
npt update-calendar [minutes]

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 35-4.  show clock Command Example

FTOS#show clock
12:30:04.402 pacific Tue May 22 2012
FTOS#

Figure 35-5.  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#

Related Commands

clock summer-time recurring  Displays the time and date from the switch hardware clock.
show calendar  Displays the time and date from the switch software clock.

show ntp associations

Display the NTP master and peers.

Syntax

show ntp associations

Command Modes

EXEC

EXEC Privilege
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 35-1. 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. |

show ntp status Command

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 35-7. 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 0.00000 sec, peer dispersion is 0.000 msec
peer mode is unspec
FTOS#
```

Table 35-2. 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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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.
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}
```
debug uplink-state-group

Enable debug messages for events related to a specified uplink-state group or all groups.

**Syntax**

```plaintext
debug 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 36-1. 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

To delete a downstream interface, use the no downstream interface command.

Parameters
interface Enter one of the following interface types:
10-Gigabit Ethernet: tengigabitethernet {slot/port | slot/port-range}
40-Gigabit Ethernet: fortysigabitethernet {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
ton-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
**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.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>downstream</code></td>
<td>Assigns a port or port-channel to the uplink-state group as a downstream interface.</td>
</tr>
<tr>
<td><code>upstream</code></td>
<td>Assigns a port or port-channel to the uplink-state group as an upstream interface.</td>
</tr>
<tr>
<td><code>uplink-state-group</code></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**

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>downstream</code></td>
<td>Assigns a port or port-channel to the uplink-state group as a downstream interface.</td>
</tr>
<tr>
<td><code>upstream</code></td>
<td>Assigns a port or port-channel to the uplink-state group as an upstream interface.</td>
</tr>
<tr>
<td><code>uplink-state-group</code></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><code>number</code></td>
<td>Enter the number of downstream links to be brought down by UFD. Range: 1 to 1024.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Brings down all downstream links in the group.</td>
</tr>
</tbody>
</table>

**Defaults**

All

**Command Modes**

UPLINK-STATE-GROUP
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**

```markdown
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**

```markdown
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 36-3. show uplink-state-group Command Examples**

```plaintext
FTOS# show uplink-state-group
Uplink State Group: 1   Status: Enabled, Up
Uplink State Group: 3   Status: Enabled, Up
Uplink State Group: 5   Status: Enabled, Down
Uplink State Group: 6   Status: Enabled, Up
Uplink State Group: 7   Status: Enabled, Up
Uplink State Group: 16  Status: Disabled, Up

FTOS# show uplink-state-group 16
Uplink State Group: 16 Status: Disabled, Up

FTOS# show uplink-state-group detail
(Up): Interface up   (Dwn): Interface down   (Dis): Interface disabled
Uplink State Group : 1   Status: Enabled, Up
Upstream Interfaces :
Downstream Interfaces :
Uplink State Group : 3   Status: Enabled, Up
Upstream Interfaces : Te 0/46(Up) Te 0/47(Up)
Downstream Interfaces : Te 13/0(Up) Te 13/1(Up) Te 13/3(Up) Te 13/5(Up)
                      Te 13/6(Up)
Uplink State Group : 5   Status: Enabled, Down
Upstream Interfaces : Te 0/0(Dwn) Te 0/3(Dwn) Te 0/5(Dwn)
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)
Uplink State Group : 6   Status: Enabled, Up
Upstream Interfaces :
Downstream Interfaces :
Uplink State Group : 7   Status: Enabled, Up
Upstream Interfaces :
Downstream Interfaces :
Uplink State Group : 16  Status: Disabled, Up
Upstream Interfaces : Te 0/41(Dwn) Po 8(Dwn)
Downstream Interfaces : Te 0/40(Dwn)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</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**

```plaintext
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

<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>show uplink-state-group</td>
<td>Displays status information on a specified uplink-state group or all groups.</td>
</tr>
</tbody>
</table>

### Example

**Figure 36-4. 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Enter one of the following interface types: 10-Gigabit Ethernet: tengigabitethernet {slot/port</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

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

**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>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>downstream</td>
</tr>
<tr>
<td>upstream</td>
</tr>
<tr>
<td>uplink-state-group</td>
</tr>
</tbody>
</table>

**Example**

**Figure 36-5. 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 Force10 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

<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>

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>0</th>
<th>1</th>
<th>Enter the bit value you want to map to a color.</th>
</tr>
</thead>
<tbody>
<tr>
<td>green</td>
<td>red</td>
<td>yellow</td>
</tr>
</tbody>
</table>

Choose a color:

- **Green**: High priority packets that are the least preferred to be dropped.
- **Yellow**: Lower priority packets that are treated as best-effort.
- **Red**: Lowest priority packets that are always dropped (regardless of congestion status).

Defaults Disabled; packets with an unmapped DEI value are colored green.

Command Mode 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

You must first enable DEI for this configuration to take effect.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dei enable</td>
<td>Enables DEI.</td>
</tr>
</tbody>
</table>
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</td>
<td>Choose a color:</td>
</tr>
<tr>
<td>yellow</td>
<td>• Green: High priority packets that are the least preferred to be dropped.</td>
</tr>
<tr>
<td></td>
<td>• Yellow: Lower priority packets that are treated as best-effort.</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
```

To remove an interface from a Stackable VLAN, use the `no member interface` command.

**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 <code>port-channel</code> 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 <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabyte Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Mode**

`conf-if-vl-<vlan>-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 37-1.  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
```

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 37-2.  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
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dei mark</td>
<td>Sets the DEI value on egress.</td>
</tr>
</tbody>
</table>

**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**

<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**

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**

<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 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**

- 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 37-4**, a VLAN-Stack trunk port is configured and then also made part of a single-tagged VLAN.

In **Figure 37-5**, 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.)
Example 1

Figure 37-4. 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 Tengigabitethernet 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 Tengigabitethernet 0/42
FTOS(conf-if-vl-100-stack)#show config
!
interface Vlan 100
 no ip address
 vlan-stack compatible
 member Tengigabitethernet 0/42
 shutdown
FTOS(conf-if-vl-100-stack)#interface vlan 20
FTOS(conf-if-vl-20)#tagged Tengigabitethernet 0/42
FTOS(conf-if-vl-20)#show config
!
interface Vlan 20
 no ip address
 tagged Tengigabitethernet 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>1</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 37-5. Adding a Stackable VLAN Trunk Port to Tagged and Untagged VLANs

```
FTOS(conf)#vlan-stack protocol-type 802.1Q
FTOS(conf)#interface Tengigabitethernet 3/10
FTOS(conf-if-te-3/10)#no shutdown
FTOS(conf-if-te-3/10)#switchport
FTOS(conf-if-te-3/10)#vlan-stack access
FTOS(conf-if-te-3/10)#exit
FTOS(conf)#interface Tengigabitethernet 8/0
FTOS(conf-if-te-8/0)#no shutdown
FTOS(conf-if-te-8/0)#portmode hybrid
FTOS(conf-if-te-8/0)#switchport
FTOS(conf-if-te-8/0)#vlan-stack trunk
FTOS(conf-if-te-8/0)#exit
FTOS(conf)#interface vlan 10
FTOS(conf-if-vlan)#vlan-stack compatible
FTOS(conf-if-vlan)#member Te 7/0, Te 3/10, Te 8/0
FTOS(conf-if-vlan)#exit

FTOS(conf)#interface vlan 30
FTOS(conf-if-vlan)#untagged Te 8/0
FTOS(conf-if-vlan)#exit
FTOS(conf)#

FTOS(conf)#interface vlan 40
FTOS(conf-if-vlan)#tagged Te 8/0
FTOS(conf-if-vlan)#exit
FTOS(conf)#
```
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

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
authentication-type

Enable authentication of VRRP data exchanges.

Syntax

    authentication-type simple [encryption-type] password

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 a 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

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

debug vrrp

Allows you to enable debugging of VRRP.
### 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 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 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 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 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.
This document provides detailed information on the Virtual Router Redundancy Protocol (VRRP) configuration commands, including the `priority` command.

### priority

**Description:**
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
```

**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

**Usage Information:**
- 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.
- 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.

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

---

### show config

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

Example

```
Example Figure 38-1. show config Command Example

FTOS(conf-if-vrid-4)#show con
vrrp-group 4
  virtual-address 119.192.182.124
!
```

```
Example Figure 38-2. show vrrp brief Command Example

FTOS>Interface Grp Pri Pre State Master addr Virtual addr(s)
Description------------------------------------------------------------------------------------------------------------------
TenGig 10/37 1 100 Y Master 200.200.200.200 200.200.200.201
Description
TenGig10/37 3 100 Y Master 1.1.1.1 1.1.1.2
FTOS>
```
Table 38-1. 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>Y</td>
<td>Preempt is enabled.</td>
</tr>
<tr>
<td>N</td>
<td>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>NA/IF</td>
<td>the interface is not available.</td>
</tr>
<tr>
<td>MASTER</td>
<td>the interface associated with the MASTER router.</td>
</tr>
<tr>
<td>BACKUP</td>
<td>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 38-3. 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>
```
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**

<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 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. |
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</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 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
```

Defaults

Not configured.

Command Modes

VRRP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</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

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.
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.

You must save the configuration and reload the system for the delay timers to take affect.

**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 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp-id</td>
<td>Enter a number as the group ID. Range: 1 to 255.</td>
</tr>
</tbody>
</table>

Defaults
Not configured.

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
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-address</td>
<td>Assigns up to 12 virtual IP addresses per VRRP group.</td>
</tr>
</tbody>
</table>
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 Force10 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          | number                            | Enter the stack-unit number.               |
|                     | Range: 0 to 5                     |                                             |
| alllevels           | Enter the keyword alllevels to run the complete set of offline diagnostic tests. |
## offline stack-unit

Place a stack unit in the offline state.

### Syntax

```plaintext
offline stack-unit number
```

### Parameters

- **number**
  - Enter the stack unit number.
  - Range: 0 to 5

### Defaults

- none

### Command Modes

- EXEC Privilege

### Command History

- **Version 8.3.16.1**
  - Introduced on 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
   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 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 Force10 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
   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.
### buffer-profile

This command creates a buffer profile that can be applied to an interface.

#### Parameters

- **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

- Introduced on 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.
**Defaults**
none

**Command Mode**
BUFFER PROFILE

**Usage Information**
If you attempt to apply a buffer profile to a non-existent port-pipe, FTOS displays the following message. However, the configuration still appears in the running-config.

```
%DIFFSERV-2-DSA_BUFF_CARVING_INVALID_PORT_SET: Invalid FP port-set 2 for stack-unit 2. Valid range of port-set is <0-1>
```

When you remove a buffer-profile using the `no buffer-profile [fp | csf]` command from CONFIGURATION mode, the buffer-profile name still appears in the output of `show buffer-profile [detail | summary]`. After a line card reset, the buffer profile correctly returns to the default values, but the profile name remains. Remove it from the `show buffer-profile [detail | summary]` command output by entering `no buffer [fp-uplink | csf] buffer-policy` from CONFIGURATION mode and `no buffer-policy` from INTERFACE mode.

**Command History**

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

**Related Commands**

- `buffer-profile (Configuration)` Creates a buffer profile that can be applied to an interface.

---

### 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**

- global 4Q

**Command Mode**

- CONFIGURATION

**Command History**

- **Version 8.3.16.1** Introduced on MXL 10/40GbE Switch IO Module
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><code>buffer-profile</code></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**

```plaintext
buffer-profile profile-name
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile-name</td>
<td>Enter the name of the buffer profile you want to apply to the interface.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Mode**

INTERFACE

**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>buffer-profile (Configuration)</code></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**

```plaintext
show buffer-profile {detail | summary} {csf | fp-uplink}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Display the buffer allocations of the applied buffer profiles.</td>
</tr>
<tr>
<td>summary</td>
<td>Display the buffer-profiles that are applied to line card port-pipes in the system.</td>
</tr>
<tr>
<td>csf</td>
<td>Display the Switch Fabric Processor buffer profiles that you have applied to line card port-pipes in the system.</td>
</tr>
<tr>
<td>fp-uplink</td>
<td>Display the Field Processor buffer profiles that you have applied to line card port-pipes in the system.</td>
</tr>
</tbody>
</table>

**Defaults**

none

**Command Mode**

INTERFACE

**Command History**

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

Figure 39-1.  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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Display the buffer allocations of a buffer profile.</td>
</tr>
<tr>
<td>summary</td>
<td>Display the Field Processors and Switch Fabric Processors that are applied in the system.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter the keyword interface followed by the interface type, either tengigabitethernet or fortygigabitethernet.</td>
</tr>
<tr>
<td>slot/port</td>
<td>Enter the slot and port number of the interface.</td>
</tr>
</tbody>
</table>

Defaults

none

Command Mode

INTERFACE

Command History

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

Example

Figure 39-2.  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

<table>
<thead>
<tr>
<th>Queue#</th>
<th>Dedicated Buffer (Bytes)</th>
<th>Buffer Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>36960</td>
<td>718</td>
</tr>
<tr>
<td>1</td>
<td>18560</td>
<td>358</td>
</tr>
<tr>
<td>2</td>
<td>18560</td>
<td>358</td>
</tr>
<tr>
<td>3</td>
<td>18560</td>
<td>358</td>
</tr>
<tr>
<td>4</td>
<td>9600</td>
<td>64</td>
</tr>
<tr>
<td>5</td>
<td>9600</td>
<td>64</td>
</tr>
<tr>
<td>6</td>
<td>9600</td>
<td>64</td>
</tr>
<tr>
<td>7</td>
<td>9600</td>
<td>63</td>
</tr>
</tbody>
</table>

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}
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit 0-5</td>
<td>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.</td>
</tr>
<tr>
<td>counters</td>
<td>Enter the keyword counters to clear the counters on the selected stack member.</td>
</tr>
<tr>
<td>unit 0–0 counters</td>
<td>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.</td>
</tr>
<tr>
<td>cpu data-plane statistics</td>
<td>Enter the keywords cpu data-plane statistics to clear the data plane statistics.</td>
</tr>
<tr>
<td>cpu party-bus statistics</td>
<td>Enter the keywords cpu party-bus statistics to clear the management statistics.</td>
</tr>
<tr>
<td>stack-port 33–56</td>
<td>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</td>
</tr>
</tbody>
</table>

**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 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**
clear hardware system-flow layer2 stack-unit 0-5 port-set 0-0 counters

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit 0-5</td>
<td>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.</td>
</tr>
<tr>
<td>port-set 0-0</td>
<td>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.</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 |

**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**
show hardware layer2 acl stack-unit 0-5 port-set 0-0

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit 0-5</td>
<td>Enter the keyword stack-unit followed by 0 to 5 to select a stack ID.</td>
</tr>
<tr>
<td>port-set 0-0</td>
<td>Enter the keyword port-set with a port-pipe number — 0.</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 |

show hardware layer3

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

**Syntax**
show hardware layer3 {acl | qos} stack-unit 0-5 port-set 0-0

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>qos</td>
</tr>
</tbody>
</table>
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.

- **buffer**
  - Enter the keyword buffer, optionally followed by the keywords total-buffer to show the total buffer statistics per stack unit. Enter the keywords buffer unit then total-buffer to display the buffer details per unit and mode of allocation. To display the forwarding plane statistics containing the packet buffer usage per port per stack unit, enter the keywords buffer unit followed by port and the port number (1-56 or all), then buffer-info.
  - To display the forwarding plane statistics containing the packet buffer statistics per COS per port, enter the keywords buffer unit and port (1-56), and queue (0-14 or all), and buffer-info.
  - Buffer unit default: 1

- **phy-firmware-version**
  - Each member of the stack is updated automatically with the latest firmware while booting as well as during OIR. Enter the keyword phy-firmware-version, to dump the physical firmware version for stack units.

- **cpu data-plane statistics**
  - Enter the keywords cpu data-plane statistics, optionally followed by the keywords stack port and its number — 0 to 52 — to display the data plane statistics, which shows the High Gig (Higig) port raw input/output counter statistics to which the stacking module is connected.

- **cpu party-bus statistics**
  - Enter the keywords cpu party-bus statistics, to display the Management plane input/output counter statistics of the pseudo party bus interface.

- **cpu private-mgmt statistics**
  - Enter the keywords cpu private-mgmt statistics, to display the Management plane input/output counter statistics of the Private Management interface.
drops [unit 0-0 [port 1-56]]

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.

stack-port 33-56

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.

unit 0-0 {counters | details | port-stats [detail] | register}

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

none

Command Modes

EXEC

EXEC Privilege

Command History

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

Example 1

Figure 39-3. show hardware stack-unit phy-firmware-version Command Example

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#
In the above example, the “Status” field represents presence of OPTM ports, “Programmed version” field represents loaded firmware version, and “SW version” represents SDK version.

Example 2  
**Figure 39-4. 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
  noClus :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 3  
**Figure 39-5. show hardware stack-unit cpu party-bus statistics Command Example**

```
FTOS#show hardware stack-unit 0 cpu party-bus statistics
Input Statistics:
  8189 packets, 8076608 bytes
  0 dropped, 0 errors
Output Statistics:
  366 packets, 133100 bytes
  0 errors
FTOS#
```

Example 4  
**Figure 39-6. show hardware stack-unit drops (drop summary for entire switch) Command Example**

```
FTOS#show hard stack-unit 0 drops
UNIT No: 0
  Total Ingress Drops : 7841475
  Total IngMac Drops : 0
  Total Mmu Drops : 0
  Total EgMac Drops : 0
  Total Egress Drops : 43321
FTOS#
```
Example 5  Figure 39-7.  show hardware stack-unit drops unit (drop summary per port) Command Example

```
FTOS#show hard stack-unit 0 drops unit 0

<table>
<thead>
<tr>
<th>PortNumber</th>
<th>Ingress Drops</th>
<th>IngMac Drops</th>
<th>Total Mmu Drops</th>
<th>EgMac Drops</th>
<th>Egress Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

FTOS#
```

Example 6  Figure 39-8.  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#
```
### Example 7
**Figure 39-9. 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 discrd ops face frame back
xe0 !ena 1G FD SW Yes Forward Tag F GMII 1554
xe1 !ena 1G FD SW Yes Forward Tag F GMII 1550
xe2 up 1G FD SW Yes Forward None FA GMII 11996
xe3 !ena 1G FD SW Yes Forward Tag F GMII 1550
xe4 down 1G 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#

### Example 8
**Figure 39-10. show hardware stack-unit unit 0 register Command Example**

```
FTOS#show hardware stack-unit 0 unit 0 register
0xf180d34 ALTERNATE_EMIRROR_BITMAP_PARITY_CONTROL.ipipe0 = 0x00000001
0xf180d35 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_INTR.ipipe0 = 0x00000000
0xf180d36 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_NACK.ipipe0 = 0x00000000
0x0f18070c 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 = 0x00000000
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
0x0335a000 ASF_PORT_SPEED.xe13 = 0x00000000
0x03360000 ASF_PORT_SPEED.xe14 = 0x00000000
0x03364000 ASF_PORT_SPEED.xe15 = 0x00000000
0x03368000 ASF_PORT_SPEED.xe16 = 0x00000000
0x0336c000 ASF_PORT_SPEED.xe17 = 0x00000000
0x03370000 ASF_PORT_SPEED.xe18 = 0x00000000
0x03374000 ASF_PORT_SPEED.xe19 = 0x00000000
0x03378000 ASF_PORT_SPEED.xe20 = 0x00000000
0x0337c000 ASF_PORT_SPEED.xe21 = 0x00000000
0x03380000 ASF_PORT_SPEED.xe22 = 0x00000000
0x03384000 ASF_PORT_SPEED.xe23 = 0x00000000
0x03388000 ASF_PORT_SPEED.xe24 = 0x00000000
0x0338c000 ASF_PORT_SPEED.xe25 = 0x00000000
0x03390000 ASF_PORT_SPEED.xe26 = 0x00000000
0x03394000 ASF_PORT_SPEED.xe27 = 0x00000000
0x03398000 ASF_PORT_SPEED.xe28 = 0x00000000
0x0339c000 ASF_PORT_SPEED.xe29 = 0x00000000
!------------------ output truncated ------------------!
```
Example 9  Figure 39-11.  show hardware stack-unit unit details Command Example

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 starting unit no the SWF in the device is 0
*****************************************************************************
bcmLinkMonStatusShow: The Current Link Status Is
Front End Link Status 0x20000000000000000000000000000000
Front End Port Present Status 0x00000000000000000000000000000000
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 33 is FALSE
The linkStatus of Front End Port 34 is FALSE
The linkStatus of Front End Port 35 is FALSE
The linkStatus of Front End Port 36 is FALSE
The linkStatus of Front End Port 37 is FALSE
*****************************************************************************

Example 10  Figure 39-12.  show hardware stack-unit per stack unit buffer Command Example

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
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 Introduce on MXL 10/40GbE Switch IO Module
```
### Example 1

#### Figure 39-15. show hardware system-flow layer2 counters Command Example

```plaintext
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 Tunneled 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>
```

FTOS#
Example 2  Figure 39-16.  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  
0x00  
action={act=Drop, param0=0(0x00), param1=0(0x00)},  
action={act=CosQToCpu, param0=0(0x00), 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  
0x00  
action={act=Drop, param0=0(0x00), param1=0(0x00)},  
action={act=CosQToCpu, param0=0(0x00), 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  
0x00  
action={act=Drop, param0=0(0x00), param1=0(0x00)},  
action={act=CosQToCpu, param0=0(0x00), 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  
0x00  
action={act=Drop, param0=0(0x00), param1=0(0x00)},  
action={act=CosQToCpu, param0=0(0x00), 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  
0x00  
action={act=Drop, param0=0(0x00), param1=0(0x00)},  
action={act=CosQToCpu, param0=0(0x00), 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=4, mode=0x01, entries=1}

!--------- output truncated -----------------!
# 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>
<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>0</td>
<td>3</td>
<td>echo reply</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>!</td>
<td>0</td>
<td>3</td>
<td>timeout (no 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 40-1. 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>9</td>
<td>router advertisement</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>10</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>0</td>
<td></td>
<td></td>
<td>time-to-live equals 0 during transit</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>time-to-live equals 0 during reassembly</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>parameter problem:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>1</td>
<td>IP header bad (catchall error)</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>2</td>
<td>required option missing</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>13</td>
<td>timestamp request</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>14</td>
<td>timestamp reply</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>15</td>
<td>information request (obsolete)</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>16</td>
<td>information reply (obsolete)</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>17</td>
<td>address mask request</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>18</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 41-1. SNMP Traps and Error Messages

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Trap Type</th>
<th>Trap Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLD_START</td>
<td>SNMP</td>
<td>COLDSTART</td>
</tr>
<tr>
<td>%SNMP-5-SNMP_COLD_START:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP COLD_START trap sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARM_START</td>
<td>SNMP</td>
<td>WARMSTART</td>
</tr>
<tr>
<td>COPY_CONFIG_COMPLETE</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>SNMP Copy Config Command Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LINK_DOWN</td>
<td>SNMP</td>
<td>LINKDOWN</td>
</tr>
<tr>
<td>%IFA-1-PORT_LINKDN: changed interface state to down:%d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LINK_UP</td>
<td>SNMP</td>
<td>LINKUP</td>
</tr>
<tr>
<td>%IFA-1-PORT_LINKUP: changed interface state to up:%d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUTHENTICATION_FAIL</td>
<td>SNMP</td>
<td>AUTH</td>
</tr>
<tr>
<td>%SNMP-3-SNMP_AUTH_FAIL:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Authentication failed. Request with invalid community string.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EGP_NEIGHBOR_LOSS</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>OSTATE_DOWN</td>
<td>SNMP</td>
<td>LINKDOWN</td>
</tr>
<tr>
<td>%IFM-1-OSTATE_DN: changed interface state to down:%s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%IFM-5-CSTATE_DN: Changed interface Physical state to down: %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSTATE_UP</td>
<td>SNMP</td>
<td>LINKUP</td>
</tr>
<tr>
<td>%IFM-1-OSTATE_UP: changed interface state to up:%s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%IFM-5-CSTATE_UP: Changed interface Physical state to up: %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON_RISING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON_FALLING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON_HC_RISING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON_HC_FALLING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%STKUNIT0-M:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 41-1. SNMP Traps and Error Messages (continued)

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Trap Type</th>
<th>Trap Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESV</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALRM_TEMP</td>
<td>ENVMON</td>
<td>TEMP</td>
</tr>
<tr>
<td>%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALRM_TEMP_CLR</td>
<td>ENVMON</td>
<td>TEMP</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>
</tr>
<tr>
<td>CHM_MAJ_ALRM_TEMP</td>
<td>ENVMON</td>
<td>TEMP</td>
</tr>
<tr>
<td>%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s °d temperature reaches or exceeds threshold of °dC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_ALRM_TEMP_CLR</td>
<td>ENVMON</td>
<td>TEMP</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>
</tr>
<tr>
<td>TME_TASK_SUSPEND</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TME_TASK_TERM</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_CPU_THRESHOLD</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_CPU_THRESHOLD_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MEM_THRESHOLD</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MEM_THRESHOLD_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MACMGR_STN_MOVE</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRRP_BDAUTH</td>
<td>PROTO</td>
<td>NONE</td>
</tr>
<tr>
<td>%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on TenGig 11/12 rcvd pkt with authentication type mismatch. %RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on TenGig 11/12 rcvd pkt with authentication failure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRRP_GO_MASTER</td>
<td>PROTO</td>
<td>NONE</td>
</tr>
<tr>
<td>%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRRP_PROTOCOL_ERROR</td>
<td>PROTO</td>
<td>NONE</td>
</tr>
<tr>
<td>VRRP_PROTOERR: VRRP protocol error on %S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP4_ESTABLISHED</td>
<td>PROTO</td>
<td>NONE</td>
</tr>
<tr>
<td>%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP4_BACKW_XSITION</td>
<td>PROTO</td>
<td>NONE</td>
</tr>
<tr>
<td>%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ETS_TRAP_TYPE_MODULE_STATUS_CHANGE</td>
<td>ETS</td>
<td>NONE</td>
</tr>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 41-1. SNMP Traps and Error Messages (continued)

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Trap Type</th>
<th>Trap Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to disabled</td>
<td>ETS</td>
<td>NONE</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</tr>
<tr>
<td>%DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to enabled</td>
<td>PFC</td>
<td>NONE</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</tr>
</tbody>
</table>
Table 41-1. SNMP Traps and Error Messages (continued)

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Trap Type</th>
<th>Trap Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS_SESSION_DROP</td>
<td>FIPS</td>
<td>NONE</td>
</tr>
<tr>
<td>%FCOE-5-SESSION_DROP: New session(%d,%s) request in interface %s dropped as max-session-limit in system reached</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIPS_ACL_INSTALL_FAIL</td>
<td>FIPS</td>
<td>NONE</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>
</tr>
<tr>
<td>CHMGR_ENT_LAST_CHANGE_TIME</td>
<td>ENTITY</td>
<td>NONE</td>
</tr>
</tbody>
</table>

No error messages. Time, at which there is a change in a physical entity, is logged.
Index

Numerics
802.3x pause frames 241

A
aaa accounting suppress 533
aaa authentication login 539
ABR 387
Access Control Lists (ACLs) 91
access-class (common IP ACL) 95
access-group 540
ACCESS-LIST Mode 18
ACL 18
description 133
Address Resolution Protocol, See ARP.
advertise med guest-voice 363
advertise-interval 663
ANSI/TIA-1057 363
Area Border Router. See ABR.
area default-cost 387
area default-cost (OSPF) 387
area nssa 387
area nssa (OSPF) 387
area range 388
area range (OSPF) 388
area stub 388
area stub (OSPF) 388
area virtual-link 389
arp 290
arp timeout 291
AS (Autonomous System) 385
ASBR 410
asymmetric flow control 241
audience 9
authentication-type 664
authentication-type simple 664
auto-cost 389
auto-cost (OSPF) 389
auto-negotiation 254
Autonomous System. See AS
auto-summary 492

B
bandwidth-percentage 468
bandwidth-percentage (policy QoS) 468
Bare Metal Auto-Configuration 143
base VLAN 440
boot, interrupting 81
BPDU 374, 459, 522, 623
Bridge Protocol Data Units, See BPDU.
Bridge Protocol Data Units. See BPDU.
bridge-priority 621
bridge-priority (RSTP) 519
buffer 677, 678
buffer-profile 679, 680
Bulk Configuration
see interface range 245
Bulk Configuration Macro
see interface range macro 248

C
calendar set 632
CAM (Content Addressable Memory) 342
CAM Profiling
Important Points to Remember 147
cam-optimization 149
channel-member 277
class-map (policy QoS) 468
clear arp-cache 292
clear command history 41
clear counters 236
clear counters ip access-group (common IP ACL) 95
clear counters mac access-group 117
clear counters vrrp 664
clear dampening 237
clear gvrp statistics interface 218
clear hardware stack-unit 682
clear hardware system-flow 683
clear host 292
clear host (DNS) 292
clear ip fib stack-unit 293
clear ip ospf 389
clear ip ospf statistics 390
clear ip prefix-list 127
clear ip rip 492
clear ip route 293
clear lacp port 331
clear logging 595
clear mac-address-table dynamic 337
clear qos statistics (policy QoS) 469
clear tcp statistics 293
clear ufd-disable 645
CLI
case sensitivity 14
partial keywords 14
CLI Modes
CONFIGURATION 17
EXEC 16
EXEC Privilege 17
INTERFACE 17
IP ACCESS LIST 18
LINE 18
MAC ACCESS LIST 18
MULTIPLE SPANNING TREE 20
PREFIX-LIST 19
ROUTE-MAP 18
ROUTER OSPF 20
ROUTER RIP 20
SPANNING TREE 19
clock read-calendar 632
clock set 633
clock summer-time date 634
clock summer-time recurring 635
clock timezone 636
clock update-calendar 636
Command Modes 16
community port 440
community VLAN 440
CONFIGURATION mode 17
Content Addressable Memory (CAM) 342
contiguous subnet masks 98
continue (Route Map) 132
copy (Streamline Upgrade) 23
copy running-config startup-config duplicate 23
Core-Dump 25
CPU Traffic Statistics 42, 58
crypto key generate 555
CX4-cable-length command 237

dampening 238
debug arp 294
debug gvrp 219
debug ip dhcp 294
debug ip icmp 295
debug ip ospf 390
debug ip packet 296
debug ip rip 492
debug ip ssh 556
debug ip udp-helper 286
debug lacp 332
debug ntp 637
debug radius 548
debug spanning-tree 622
debug spanning-tree mstp 372
debug spanning-tree rstp 520
debug tacacs+ 552
debug uplink-state-group 646, 649
debug vrrp 664, 665
default logging buffered 595, 597
default logging console 595
default logging monitor 596
default logging trap 596, 602
Default VLAN 348
default vlan-id 348
default-information originate 392, 493
   RIP 493
default-metric
   OSPF 393
   RIP 494
default-metric (OSPF) 393
default-metric (RIP) 494
define interface range macro 248
delete
   EXEC privilege mode 24
deny
   extended IP ACL 102
   IP ACL (standard) 98
   standard IP ACL 98
deny (Extended MAC ACL) 123
deny (IP prefix ACL) 128
deny (standard MAC ACL) 120
deny ether-type 103
deny icmp (extended IP ACLs) 103
deny tcp
   IP ACL 105
deny tcp (extended IP ACLs) 105
deny udp
   IP ACL 107
deny udp (extended IP ACLs) 107
description 470, 647
   ACL 91
   INTERFACE 240
   VRRP 665
description (ACL) 91
description (interface) 240
description (OSPF) 393
description (Route Map) 133
description (VLAN) 347, 393
description (VRRP) 665
description, spanning-tree 372, 434, 450, 494, 520, 622
DHCP 301
   UDP ports 301
DHCP broadcast messages 301
DHCP server 301
diag stack-unit 675
dir
   EXEC privilege mode 24
disable
   Spanning Tree Protocol 372, 449, 450, 520, 622
   VRRP 665
disable (GVRP) 219
disable (MSTP) 373
disable (PVST+) 449
disable (RSTP) 521
disable (STP) 623
disable (VRRP) 666
disable-on-sfm-failure
  INTERFACE 240
discontiguous subnet masks 98
display parameter 15
distance
  OSPF 393
  RIP 495
distance (OSPF) 393
distance (RIP) 495
distance ospf 394
distribute-list (OSPF) 395
distribute-list (RIP) 495, 496
distribute-list in
  OSPF 395
  RIP 495
distribute-list out
  OSPF 395
  RIP 495
distribute-list out
  OSPF 395
  RIP 496
dNS commands 299, 300, 302
do 43
document conventions 9
dot1p-priority 157, 462
dot1p-priority (QoS) 462
download alt-boot-image 25
downstream 647
downstream auto-recover 648
downstream disable links 648
duplex 240
duplex flow control 241
dynamic LAG 277

e
egress ACLs 95
enable 44
Enable password 17
enable password 540, 542
enable restricted 541
end 45
except parameter 15
EXEC mode 16
exec-banner 45
exec-timeout 46
exit 46
extended MAC ACL 124

external flash, number of files supported 22

F
fast-convergence
  OSPF 396
fast-convergence (OSPF) 396
files, number supported on external flash 22
find parameter 15
flood-2328 (OSPF) 396
flow control values 242
flow control, asymmetric 241
flow control, duplex 241
flowcontrol 241
format flash 25
forward-delay 623
forward-delay (MSTP) 373
forward-delay (RSTP) 521
forward-delay (STP) 623
Forwarding Information Base (FIB) entries 311
ftp-server enable 47
ftp-server topdir 47
ftp-server username 48

G
GARP VLAN Registration Protocol. See GVRP.
GID (GARP Information Declaration) 217
GIP (GARP Information Propagation) 217
graceful-restart
  OSPF 397
graceful-restart helper-reject
  OSPF 397
graceful-restart helper-reject (OSPF) 397
grep command option 16
grep parameter 15
group (LAG sharing) 278
group (LAG) 278
GVRP 20
GVRP (GARP VLAN Registration Protocol) 217
gvrp enable 221
gvrp registration 221

H
hello-time 623
hello-time (MSTP) 374
hello-time (RSTP) 522
hello-time (STP) 623
hold-time 666
hold-time (VRRP) 666
hostname 48
ICMP 305
IEEE 802.1d 449
IETF RFCs
1058 491
2328 385
2453 491
IFM (interface management) 69
IGMP Snooping 227
   Important Things to Remember for IGMP Querier 228
   Important Things to Remember for IGMP Snooping 227
IGMP Snooping Commands 227
ignore-case sub-option 16
IGP (Interior Gateway Protocol) 385
ingress ACLs 95
interface 243
   interface command 243
   interface loopback 244
   interface management (IFM) 69
   interface ManagementEthernet 244
   interface null 245
   interface port-channel 279
   interface range 245
   interface range macro 249
   interface rate-interval 258
   interface suppress threshold (dampening) 239
Interface vlan 249, 250
   interface vlan 249, 250
Interior Gateway Protocol (IGP) 385
Internet Control Message Protocol. See ICMP.
ip access-group (common IP ACL) 95
ip access-list extended 109
ip access-list extended (extended IP ACLs) 109
ip access-list standard 99
ip address 298
ip default-network 300
ip directed-broadcast 299
ip domain-list 299
ip domain-lookup 300
ip domain-name 300
IP DSCP bit 480
ip fib download-igp-only 301
ip ftp password 49
ip ftp source-interface 49
ip ftp username 50
ip helper-address 301
ip helper-address hop-count disable 301
ip host 302
ip igmp access-group 228
ip local-proxy-arp command 440
ip max-frag-count 302
ip name-server 302
ip ospf auth-change-wait-time 397
   OSPF 397
ip ospf authentication-key 398
ip ospf cost 398
ip ospf dead-interval 399
ip ospf hello-interval 399
ip ospf message-digest-key 400
ip ospf mtu-ignore 400
ip ospf network 400, 401
ip ospf priority 401
ip ospf retransmit-interval 401
ip ospf transmit-delay 402
ip poison-reverse 496
ip poison-reverse (RIP) 496
ip prefix-list 128
ip proxy-arp 303
ip radius source-interface 548
ip rip receive version 497
ip rip send version 497
ip route 303
ip scp topdir 556
ip source-route 304
ip split-horizon 498
ip split-horizon (RIP) 498
ip ssh authentication-retries 557
ip ssh connection-rate-limit 557
ip ssh hostbased-authentication enable 558
ip ssh key-size 558
ip ssh password-authentication enable 559
ip ssh pub-key-file 559
ip ssh rehash file 560
ip ssh rsa-authentication 561
ip ssh rsa-authentication enable 561
ip ssh server 562
ip ssh server enable 562
ip tacacs source-interface 553
ip telnet server enable 50
ip telnet source-interface 51
ip tftp source-interface 51
ip udp-broadcast-address 287
ip udp-helper udp-port 287
ip unreachables 305
IPv4 ACLs
   cam-acl 148
isolated ACLs 440
isolated VLAN 440
J
JumpStart
  reload-type 144
  show reload-type 144

K
keepalive 250

L
LACP
  clear lacp counters 331
  debug lacp 332
  lacp port-priority 333
  port-channel mode 333
  port-channel-protocol lacp 334
  show lacp 335
  lacp system-priority 333
LAG
  channel-member 277
  group 278
  interface port-channel 279
  minimum-links 280
  port-channel failover-group 280
  show interfaces port-channel 281
LAG failover group 280
LAG failover-group 282
LAG fate-sharing group 282
LAG supergroup 278
LAGs 331
line 52
Link Aggregation Control Protocol (LACP) 331
Link Layer Detection Protocol (LLDP) 355
Link State Advertisements. See LSA.
link-state protocol 385
LLDP 355
LLDP-MED (Media Endpoint Discovery) 363
log-adjacency-changes 402
logging 596
logging buffered 597
logging console 597
logging facility 598
logging history 599
logging history size 599
logging monitor 600
logging on 600
logging source-interface 601
logging synchronous 601
logging trap 602
login authentication 542
LSA 388, 401

M
mac access-group 118
mac access-list extended (Extended MAC ACL) 124
mac access-list standard (standard MAC ACL) 121
mac accounting destination 338
MAC ACL, extended 124
mac learning-limit 339
mac learning-limit learn-limit-violation 341
mac learning-limit reset 342
mac learning-limit station-move-violation 341
mac-address-table aging-time 338
mac-address-table static 338
mac-address-table station-move 339
mac-address-table station-move refresh-arp 339
Management interface 244
management route 305
Management static route 305
management unit, MXL Switch member unit, resetting 612
master unit 612
match interface (Route Map) 134
match ip access-group 470
match ip access-group (policy QoS) 470
match ip address (Route Map) 134
match ip dscp 471
match ip dscp (policy QoS) 471
match ip next-hop (Route Map) 135
match ip precedence 471
match ip precedence (policy QoS) 471
match ip route-source (Route Map) 135
match mac access-group (policy QoS) 472
match mac dot1p (policy QoS) 473
match metric (Route Map) 136
match route-type (Route Map) 136
match tag (Route Map) 137
max-age 624
max-age (MSTP) 374
max-age (RSTP) 522
max-age (STP) 624
max-hops (MSTP) 375
maximum-paths 403
  OSPF 403
  RIP 498
maximum-paths (RIP) 498
Media Endpoint Discovery 363
member 657
member (Stackable VLAN) 657
mib-binding 403
minimum-links 280
monitor interface 251
monitor session 434
motd-banner 52
msti (MSTP) 375
MSTP 371
   debug spanning-tree mstp 372
mtu 252
MULTIPLE SPANNING TREE 20
Multiple Spanning Tree Protocol 371
MXL Switch -only commands
   reset stack-unit 612
MXL Switch stacking 611

N
name (MSTP) 376
name (VLAN) 348
negotiation auto 254
neighbor 498
neighbor (RIP) 498
network
   RIP 499
network (OSPF) 403
network (RIP) 499
network area
   OSPF 403
Network Time Protocol (NTP) 631
Network Time Protocol.  See NTP.
NIC Teaming 339
no-more 16
no-more parameter 16
non-contiguous subnet masks 98
Not So Stubby Area. See NSSA.
NSSA 387
NTP 637
NTP (Network Time Protocol) 631
ntp authenticate 637
ntp authentication-key 638
ntp broadcast client 638
ntp disable 639
ntp multicast client 639
ntp server 639
ntp source 640
ntp trusted-key 640
ntp update-calendar 641

O
offline stack-unit 676
offset-list 499
offset-list (RIP) 499
online stack-unit 677
OSPF
   link-state 385
   output-delay 500
   output-delay (RIP) 500

P
passive-interface
   OSPF 404
   RIP 501
passive-interface (OSPF) 404
passive-interface (RIP) 501
password 543
password, Enable 17
pause frames 241
PBR (Policy-Based Routing) 571
permit
   IP ACL (extended) 110
   permit (extended IP ACLs) 110
   permit (Extended MAC ACL) 125
   permit (IP prefix ACL) 129
   permit (standard MAC ACL) 121
   permit arp 111
   permit icmp (extended IP ACLs) 111
   permit tcp
      IP ACL 112
   permit tcp (extended IP ACLs) 112
   permit udp
      IP ACL 114
   permit udp (extended IP ACLs) 114
per-port QoS 462
ping 52
policy-aggregate (policy QoS) 474
Policy-Based QoS 179, 467
Policy-map
   description 470
   policy-map-input 474
   policy-map-input (policy QoS) 474
   policy-map-output (policy QoS) 475
Port Mirroring
   Important Points to Remember 433
port types (private VLAN) 440
port-based QoS 462
port-channel failover-group 280
port-channel mode 333
port-channel supergroup 278
port-channel-protocol lacp 334
port-channels 331
portmode hybrid command 255
power-off 54
preemphasis, CX4 cable length 237
preempt 666
preempt (VRRP) 666
PREFIX-LIST Mode 19
primary port 283
primary VLAN 440
priority 667
priority (VRRP) 667
private-vlan mapping secondary-vlan command 442
private-vlan mode command 441
privilege exec 536, 537
privilege level (CONFIGURATION mode) 536
privilege level (LINE mode) 537
promiscuous port 440
PROTOCOL
   Per-VLAN SPANNING TREE Mode 19
   SPANNING TREE Mode 19
protocol gvrp 222
PROTOCOL GVRP Mode 20
PROTOCOL MULTIPLE SPANNING TREE Mode 20
protocol route 305
protocol spanning-tree 624, 625
protocol spanning-tree mstp 377
protocol spanning-tree pvst (PVST+) 452
protocol spanning-tree rstp 523
provision type 618
PVST+ (Per-VLAN Spanning Tree plus) 449

Q
QinQ 655
QoS
   Per Port 462
   Policy-Based 467
QoS, per-port 462
QoS, port-based 462
qos-policy-input 475
qos-policy-input (policy QoS) 475
qos-policy-output 476

R
radius-server deadtime 549
radius-server host 549
radius-server key 551
radius-server retransmit 551
radius-server timeout 552
RAPID SPANNING TREE Mode 19
rate police (QoS) 463
rate shape (QoS) 464
rate-interval 258
rate-police 477
rate-shape (policy QoS) 477
redistribute
   OSPF 405
   RIP 501
redistribute (OSPF) 405
redistribute isis
   RIP 502
redistribute ospf
   RIP 502
redundancy disable-auto-reboot 611
redundancy disable-auto-reboot rpm 611, 617
redundancy force-failover 612
redundancy force-failover stack-unit command 612
reload 54
reload dhcp-client-mode 144
reload dhcp-client-only-mode 144
remark 92
Remote Network Monitoring (RMON) 507
resequence access-list 93
resequence prefix-list ipv4 93
reset stack-unit 612
resetting MXL Switch member unit 612
revision (MSTP) 373, 377
RFC 3069 439
RFC-2328 396
RIP 491
   version 1 491
   version 2 491
RMON 507
rmon alarm 508
rmon collection history 509
rmon collection statistics 509
rmon event 510
rmon hc-alarm 510
route-map 137
ROUTE-MAP Mode 18
Router Information Protocol. See RIP.
routing ospf 407
router rip 502
ROUTER RIP Mode 20
router-id 406
router-id (OSPF) 406
running config defined 22

S
searching show commands 16
   display 15
   except 15
   find 15
   grep 15, 16
secondary VLAN 440
Secure Copy (SCP) 22
Security
aaa accounting 532
aaa accounting suppress 533
aaa authorization 535
show accounting 533
seq
   IP ACL (extended) 115
   standard IP ACL 100
seq (extended IP ACLs) 115
seq (Extended MAC ACL) 126
seq (IP prefix ACL) 129
seq (standard MAC ACL) 122
seq arp 115
service password-encryption 545
service timestamps 55
service-class dynamic dot1p 464
service-class dynamic dot1p (QoS) 159, 160, 464, 465
service-policy input 478
service-policy output 478
service-queue 479
set (policy QoS) 480
set automatic-tag (Route Map) 138
set metric (Route Map) 139
set metric-type (Route Map) 139
set tag (Route Map) 140
sFlow 572
sFlow collector 572
sFlow enable (globally) 573
sFlow enable (Interface) 573
sFlow extended-switch enable 574
sFlow polling-interval (Global) 574
sFlow polling-interval (Interface) 575
sFlow sample-rate (Global) 575
sFlow sample-rate (Interface) 576
shortest path first (SPF) 431
show alarms 56
show arp 306
show cam mac stack-unit 342
show cam-acl 149, 151
show chassis 56
show command-history 56
show config
   Access list 93
   Interface 258
   OSPF 407
   RIP 503
   Spanning Tree 281, 349, 524, 625
   VRRP 667
show config (ACL) 94
show config (from INTERFACE RANGE mode) 258
show config (GVRP) 222, 225
show config (interface configuration) 258
show config (IP prefix ACL) 130
show config (LAG) 281
show config (MSTP) 378
show config (OSPF) 407
show config (port monitor) 435
show config (Route Map) 140
show config (RSTP) 524
show config (STP) 625
show config (VLAN) 349
show config (VRRP) 667
show crypto 562
show debugging 59, 69
show environment 59
show garp timers 222
show gvrp 223
show gvrp statistics 224
show hardware layer2 683
show hardware layer2 acl 684
show hardware layer3 683
show hardware stack-unit 684
show hardware system-flow 690
show hosts 308
show interface rate 157, 158, 159, 160, 161, 172
show interfaces 259, 267
show interfaces configured 258
show interfaces dampening 264
show interfaces description 265
show interfaces tengigabitethernet transceiver 270
show interfaces stack-unit 266
show interfaces port-channel 281
show interfaces private-vlan command 443
show interfaces stack-unit 266
show interfaces switchport 268
show ip accounting access-list (common IP ACL) 96
show ip cam 309
show ip cam stack-unit 309
show ip fib stack-unit 311
show ip fib stack-unit 311
show ip interface 312
show ip management-route 313
show ip ospf 408
show ip ospf asbr 409
show ip ospf database 409
show ip ospf database asbr-summary 410
show ip ospf database database-summary 421
show ip ospf database external 412
show ip ospf database network 414
show ip ospf database nssa-external 416
show ip ospf database opaque-area 416
show ip ospf database opaque-as 418
show ip ospf database opaque-link 418
show ip ospf database router 419
show ip ospf database summary 421
show ip ospf interface 423
show ip ospf neighbor 425
show ip ospf routes 425
show ip ospf statistics global 426
show ip ospf timers rate-limit 429
show ip prefix-list detail 130
show ip protocols 314
show ip rip database 503
show ip route 315
show ip route list 316
show ip route summary 317
show ip ssh 563
show ip ssh client-pub-keys 564
show ip ssh rsa-authentication 564
show ip traffic 318
show ip udp-helper 288
show lacp 335
show stack-unit 62
show logging 603
show mac accounting access-list 119
show mac learning-limit 346
show mac-address-table 343
show mac-address-table aging-time 345
show memory 62
show monitor session 435
show ntp associations 642
show ntp status 643
show privilege 545
show processes cpu 62
show processes memory 67
show processes switch-utilization 69
show qos class-map 480
show qos policy-map 481
show qos policy-map-input 482
show qos policy-map-output 482
show qos qos-policy-input 483
show qos qos-policy-output 483
show qos statistics 484
show qos wred-profile 485
show range 274
show redundancy 612, 613
show rmon 511
show rmon alarms 511
show route-map 140
show route-map (Route Map) 140
show running-config extcommunity-list 504
show running-config monitor session 436
show running-config uplink-state-group 649
show sflo 576
show sfim 32
show snmp 580, 581
show software ifin 69
show spanning-tree 0 626
show spanning-tree 0 (STP) 626
show spanning-tree mst configuration 378
show spanning-tree msti 378
show spanning-tree pvst 452
show spanning-tree rstp (RSTP) 524
show system 70
show system brief 70
show system stack-ports 614
show system stack-unit 70
show tcp statistics 320
show tcp statistics 320
show tdr 284
show tech-support 25, 28, 29, 72, 75
show uplink-state-group 650
show users 546
show version 33
show vlan 349
show vlan command 349
show vlan command 349
show vlan private-vlan command 444
show vlan private-vlan mapping command 446
show vrrp 668
shutdown 275
Single Window Protocol Queue (SWPQ) 66
SNMP
  number of traps supported 579
  versions supported 579
snmp ifmib ifalias long 582
snmp trap link-status 594
snmp-server community 582
snmp-server contact 584
snmp-server enable traps 584, 585
snmp-server host 588
snmp-server location 590
snmp-server trap-source 591
source (port monitoring) 437
Spanning Tree Protocol
  BPDU guard 629
  interface cost 629
  portfast 629
Index

Root guard 629
spanning-tree 629
spanning-tree (MSTP) 381
spanning-tree msti 381
spanning-tree mstp 382
spanning-tree rstp (RSTP) 527
speed 275
100/1000 Base-T Ethernet interfaces 275
SPF (Shortest Path First) 390
split 40G port 276
buffer 677, 678
buffer-profile 679, 680
diag stack-unit 675
offline stack-unit 676
online stack-unit 677
redundancy disable-auto-reboot rpm 611, 617
show environment 59
show hardware stack-unit 684
show hardware system-flow 690
show inventory 61
show memory 62
show processes cpu 62
show redundancy 613
show system stack-ports 614
stack-unit priority 618
stack-unit provision 618
stack-unit renumber 619
ssh 565
stack member identifier 618
stack standby unit 612
Stackable VLAN feature 655
stacking, MXL Switch 611
stack-unit priority 618
stack-unit provision 618
stack-unit renumber 619
standby master 612
static LAG commands 331
static route 305
Storm-Control 605
Important Points to Remember 605
Streamline Upgrade 24
strict-priority queue (QoS) 167, 466
subnet masks 98
summary-address 430
summary-address (OSPF) 430
suppress threshold (dampening), interface 239
switchport mode private-vlan command 447
SWPQ (Single Window Protocol Queue) 66
System Time and Date 631

T
tacacs-server host 553
tacacs-server key 554
tagged 351
tagged command 351
tc-flush-standard 528
tc-flush-standard (MSTP) 383
tc-flush-standard (PVST+) 458
tdr-cable-test 284
TDR
Important Points to Remember 284
timeout login response 546
timers basic 505
timers spf 431, 432
timers spf (OSPF) 431, 432
TOS 411, 412, 413, 415, 417, 420, 422
traceroute 77
track 670
track (VRRP) 670
trace route 305
streamline upgrade 24
Streamline Upgrade 24
switchport mode private-vlan command 447
SWPQ (Single Window Protocol Queue) 66
System Time and Date 631

U
u-Boot 81
undebug all 78
untagged 353
untagged command 353
uplink-state-group 651
upstream 652
username 547

V
version 505
Virtual LANs. See VLANs.
virtual-address 671
virtual-address (VRRP) 671
VLAN
description 347, 393
vlan bridge-priority (PVST+) 458
vlan forward-delay (PVST+) 459
vlan hello-time (PVST+) 459
vlan max-age (PVST+) 460
VLAN types (private VLAN) 439
VLANs
  ACL support 250
  definition 347
  IP features not supported 347
vlan-stack access 659
vlan-stack compatible 659
vlan-stack protocol-type 660
vlan-stack trunk 661
VLAN-Stack VLANs
  Important Points to Remember 655
VLAN-Stacking 655
VMAN tag 660
vrrp delay minimum 671, 672
vrrp-group 673

W
  wred 488
  wred-profile 489
  write 78

X
XML
  terminal xml 76
Command Index

A

aaa accounting 532
aaa accounting suppress 533
aaa authorization 535, 536
Access list
access-class 95, 540
clear counters ip access-group 95
ip access-group 95
show config 94, 140
show ip accounting access-list 96
Access list (extended)
deny 102
deny tcp 105
deny udp 107
ip access-list extended 109
permit 110
permit tcp 112
permit udp 114
seq 115
Access list (standard)
deny 98
ip access-list standard 99
permit 99
seq 100
access-class 95
ACL
description 91
advertise dot1-tlv 356
advertise dot3-tlv 356
advertise management -tlv 357
advertise med guest-voice-signaling 364
advertise med location-identification 365
advertise med power-via-mdi 365
advertise med softphone-voice 366
advertise med streaming-video 366
advertise med video-conferencing 367
advertise med video-signaling 367
advertise med voice 368
Alarms
clear alarms 41
show alarms 56
ARP
arp 290
arp timeout 291
clear arp-cache 292
debug arp 294
show arp 306

B

bandwidth-percentage 468

banner exec 38
banner login 39
banner motd 40
bridge-priority (RSTP) 519
bridge-priority (STP) 621
buffer 677

C

calendar set 632
cam-acl 148
cam-optimization 149
cd 22
channel-member 277
class-map 468
clear alarms 41
clear arp-cache 292
clear counters ip access-group 95
clear counters mac access-group 117
clear dampening 237
clear gyvrp statistics interface 218
clear hardware stack-unit 682
clear hardware system-flow 683
clear host (DNS) 292
clear ip fib linecard 293
clear ip ospf statistics 390
clear ip prefix-list 127
clear ip route 293
clear lacp counters 331
clear line 41
clear lldp counters 357
clear lldp neighbors 357
clear logging 595
clear mac-address-table dynamic 337
clear qos statistics 469
clear tcp statistics 293
clear ufd-disable 645
clock read-calendar 632
clock set 633
clock summer-time date 634
clock summer-time recurring 635
clock timezone 636
clock update-calendar 636
configure 42
continue (Route Map) 132
copy 22
copy flash 22
copy run start 25
copy running-config 22
copy running-config ftp 23

copy running-config startup-config duplicate 23
copy running-config tftp
23
copy slot0 22
copy startup-config 22
crypto key generate 555

D
Debug
debug arp 294
debug ftpserver 43
debug ip icmp 295
debug ip ospf 390
debug ip packet 296
debug ip rip 492
debug multiple spanning-tree 372
debug ntp 637
debug radius 548
debug spanning-tree 622
show debugging 59
undebug all 78
debug cpu-traffic-stats 42
debug gvrp 219
debug ip dhcp 294
debug ip ssh 556
debug ipv6 dhcp 294
debug lldp interface 358
debug spanning-tree rstp 520
debug uplink-state-group 646, 649
default logging buffered 595
default logging console 595
default logging monitor 596
default logging trap 596
delete 24
deny
  IP ACL (extended) 102
  MAC ACL (extended) 123
  MAC ACL (standard) 120
  Prefix List 128
  standard IP ACL 98
deny (Extended IP ACL) 102
deny arp 103
deny icmp (Extended IP ACL) 103
deny tcp (Extended IP ACL) 105
deny udp (Extended IP ACL) 107
description (ACL) 91
description (MSTP) 372
description (PVST) 450
description (RIP) 494
description (Route Map) 133
description (RSTP) 520
description (STP) 622
description (VLAN) 347, 393
diag stack-unit 675
dir 24
disable 43
disable (GVRP) 219
disable (LLDP) 359
disable (MSTP) 373
disable (PVST+) 449
disable (RSTP) 521
disable (STP) 623
DNS
clear host 292
  ip domain-list 299
  ip domain-lookup 300
  ip domain-name 300
downstream 647, 648
downstream auto-recover 648
duplex (10/100 Interfaces) 240
E
ecmp-group, LAG link bundle monitoring 241
enable 44
enable xfp-power-updates 44
end 45
exec-banner 45
exec-timeout 46
exit 46
F
failover group, LAG 278
fate-sharing group, LAG 278
flowcontrol 241
format flash (S-Series) 25
forward-delay (MSTP) 373
forward-delay (RSTP) 521
forward-delay (STP) 623
FTP
debug ftpserver 43
ftp-server enable 47
ftp-server topdir 47
ftp-server username 48
ip ftp password 49
ip ftp source-interface 49
ip ftp username 50
G
garp timers 220
gvrp enable 221
gvrp registration 221
**H**
- hello (LLDP) 359
- hello-time (MSTP) 374
- hello-time (RSTP) 522
- hello-time (STP) 623
- hostname 48

**I**

**IGMP**
- igmp snooping fast-leave 231
- ip igmp querier-timeout 229
- ip igmp query-interval 229
- ip igmp query-ma-resp-time 229
- show ip igmp groups 230

**IGMP Snooping**
- igmp snooping flood 231
- igmp snooping last-member-query-interval 232
- igmp snooping querier 233
- ip igmp snooping mrouter 232
- show ip igmp snooping mrouter 233

**Interface**
- clear counters 236
- description 240
- dot1p-priority 157, 207, 462
- interface 243
- interface loopback 244
- interface ManagementEthernet 244
- interface null 245
- interface port-channel 279
- interface vlan 249, 250
- ip unreachable 305
- negotiation auto 254
- show config 258
- show interfaces 259, 270
- show interfaces switchport 268
- shutdown 275

**LAG**
- lACP port-priority 333
- lACP system-priority 333

**L**
- line 52
- line console 52
- line vty 52

**Logging**
- clear logging 595
- default logging buffered 595
- default logging console 595
- default logging monitor 596
- default logging trap 596
- logging 596
- logging buffered 597
- logging console 597
logging facility 598
logging history 599
logging history size 599
logging monitor 600
logging on 600
logging source-interface 601
logging synchronous 601
logging trap 602
no logging on 600
show logging 603
logging 596
logging buffered 597
logging console 597
logging facility 599
logging history 599
logging history size 599
logging kernel-coredump 25
logging kernel-coredump server 26
logging monitor 600
logging on 600
logging source-interface 601
logging synchronous 601
logging trap 602

M
MAC Access list
clear counters mac access-group 117
mac access-group 118
show mac accounting access-list 96, 118, 119
MAC Access list (extended)
deny 123
mac-access-list extended 124
permit 125
seq 126
MAC Access list (standard)
deny 120
mac-access-list standard 121
permit 121
seq 122
mac access-group 118
mac access-list extended 124
mac access-list standard 121
mac learning-limit 339
mac learning-limit learn-limit-violation 341
mac learning-limit reset 342
mac learning-limit station-move-violation 341
mac-address-table aging-time 338
mac-address-table static 338
mac-address-table station-move refresh-arp 339
mac community (Route Map) 134
mac interface (Route Map) 134
match ip access-group 470
match ip address (Route Map) 134
match ip dscp 470
match ip next-hop (Route Map) 135
match ip precedence 471
match ip route-source (Route Map) 135
match mac access-group (policy QoS) 472
match mac dot1p (policy QoS) 473
match metric (Route Map) 136
match route-type (Route Map) 136
match tag (Route Map) 137
max-age (MSTP) 374
max-age (RSTP) 522, 523
max-age (STP) 624
max-hops (MSTP) 375
member (Stackable VLAN) 657
minimum-links 280
mode (LLDP) 359
monitor 251
Monitor Session
description 434
monitor session 434
motd-banner 52
msti (MSTP) 375
MSTP
debug spanning-tree mstp 372
disable 373
forward-delay 373
hello-time 374
max-age 374
max-hops 375
msti 375
name 376
protocol spanning-tree mstp 377
revision 373, 377
show config 378
show spanning-tree mst configuration 378
show spanning-tree msti 378
spanning-tree 381
spanning-tree msti 381
spanning-tree mstp 382
mtu 252
Multiple Spanning Tree Protocol
see MSTP 371
multiplier (LLDP) 360

N
name (MSTP) 376
name (VLAN) 348
NTP
debug ntp 637
ntp authenticate 637
ntp authentication-key 638
ntp broadcast client 638
ntp disable 639
ntp multicast client 639
ntp server 639
ntp source 640
ntp trusted-key 640
ntp update-calendar 641
show ntp associations 642
show ntp status 643

offline stack-unit 676
online stack-unit 677

OSPF
  area default-cost 387
  area nssa 387
  area range 388
  area stub 388
  auto-cost 389
  clear ip ospf 389
  debug ip ospf 390
  default-information originate 392
  default-metric 393
  distance 393
  distance ospf 394
  distribute-list in 395
  distribute-list out 395
  fast-convergence 396
  graceful-restart grace-period 397
  graceful-restart helper-reject 397
  graceful-restart mode 397
  graceful-restart role 397
  ip ospf auth-change-wait-time 397
  ip ospf authentication-key 398
  ip ospf cost 398
  ip ospf dead-interval 399
  ip ospf hello-interval 399
  ip ospf message-digest-key 400
  ip ospf mtu-ignore 400
  ip ospf network 401
  ip ospf priority 401
  ip ospf retransmit-interval 401
  ip ospf transmit-delay 402
  log-adjacency-changes 402
  maximum-paths 403
  mib-binding 403
  network area 403
  passive-interface 404
  redistribute 405
  router ospf 407
  show config 407
  show ip ospf 408
  show ip ospf database 409
  show ip ospf database asbr-summary 410
  show ip ospf database database-summary 421
  show ip ospf database external 412
  show ip ospf database network 414
  show ip ospf database nssa-external 416
  show ip ospf database opaque-area 416
  show ip ospf database opaque-as 418
  show ip ospf database opaque-link 418
  show ip ospf database router 419
  show ip ospf interface 423
  show ip ospf neighbor 425
  show ip ospf virtual-links 430
  summary-address 430
  timers throttle lsa 431, 432

permit
  IP ACL (standard) 99
  MAC ACL (extended) 125
  MAC ACL (standard) 121
  Prefix list 129
  standard IP ACL 99
  permit (Extended IP ACL) 110
  permit icmp (Extended IP ACL) 111
  permit tcp (Extended IP ACL) 112
  permit udp (Extended IP ACL) 114
  ping 52
  policy-aggregate 474
  policy-map-input 474
  policy-map-output 475

Port Channel
  channel-member 277
  interface port-channel 279
  minimum-links 280
  minimum-links command 280
  show interfaces port-channel 281
  port-channel failover-group 280
  port-channel mode 293, 307, 310
  port-channel-protocol lacp 334
  portmode hybrid 255

Prefix list
  clear ip prefix-list 127
  deny 128
  ip prefix-list 128
  permit 129
  seq 129
  show config 130
  show ip prefix-list detail 130
  show ip prefix-list summary 131
  private-vlan mapping secondary-vlan 442
private-vlan mode 441
protocol gvrp 222
protocol lldp (Configuration) 360
protocol lldp (Interface) 360
protocol spanning-tree (STP) 625
protocol spanning-tree mstp 377
protocol spanning-tree pvst 452
protocol spanning-tree rstp 523
PVST
  description 450
  pwd 26

Q
QoS
  bandwidth-percentage 468
  class-map 468
  match ip access-group 470
  match ip dscp 471
  match ip precedence 471
  policy-aggregate 474
  policy-map-input 474
  policy-map-output 475
  qos-policy-output 476
  rate shape 170, 205, 206, 325, 464
  rate-police 477
  rate-shape 477
  service-class dynamic dot1p 164, 207, 325, 464
  service-policy input 478
  service-policy output 478
  service-queue 479
  show interfaces rate 158, 159, 160, 161, 172
  show qos class-map 480
  show qos policy-map 481
  show qos policy-map-input 482
  show qos policy-map-output 482
  show qos qos-policy-input 483
  show qos qos-policy-output 483
  show qos statistics 484
  strict-priority queue 167, 170, 466
  trust diffserv 487
  wred 488
  wred-profile 489
qos 476
qos-policy-input 475
qos-policy-output 476

R
RADIUS
  debug radius 548
  ip radius source-interface 548
  radius-server deadtime 549
  radius-server host 549
  radius-server key 551
  radius-server retransmit 551
  radius-server timeout 552
  rate limit (QoS) 463
  rate police (QoS) 463
  rate shape (QoS) 170, 205, 206, 325, 464
  rate-interval 258
  rate-police 477
Redundancy
  show redundancy 613
  redundancy disable-auto-reboot 611
  redundancy force-failover stack-unit 612
  reload 54
  remark 92
  rename 27
  resequence access-list 93
  resequence prefix-list ipv4 93
  reset stack-unit 612
  revision (MSTP) 373, 377
RIP
  auto-summary 492
  clear ip rip 492
  debug ip rip 492
  default-information originate 493
  default-metric 494
  description 494
  distance 495
  distribute-list in 495
  distribute-list out 496
  ip poison-reverse 496
  ip rip receive version 497
  ip rip send version 497
  ip split-horizon 498
  maximum-paths 498
  neighbor 498
  network 499
  offset-list 499
  output-delay 500
  passive-interface 501
  redistribute 501
  redistribute ospf 502
  router rip 502
  show config 503
  show ip rip database 503
  show running-config rip 504
  timers basic 505
  version 505
rmon alarm 508
rmon collection history 509
rmon collection statistic 509
rmon collection statistics 509
RMON Commands 507
rmon event 510
rmon hc-alarm 510

Route map
  match interface 134
  match ip address 134
  match ip next-hop 135
  match ip route-source 135
  match metric 136
  match route-type 136
  match tag 137
  route-map 137
  set automatic-tag 138
  set metric 139
  set metric-type 139
  set tag 140
  show route-map 140

route-map (Route Map) 137

router-id 406

RSTP
  bridge-priority 519
  debug spanning-tree rstp 520
  disable 521
  forward-delay 521
  hello-time 522
  max-age 522, 523
  protocol spanning-tree rstp 523
  show config 524
  show spanning-tree rstp 524
  spanning-tree rstp 527

S

SCP
  ip scp topdir 556

Security
  aaa authentication login 539
  enable password 540
  enable restricted 541
  login authentication 542
  password 543
  privilege level 536, 537
  service password-encryption 545
  show privilege 545
  show users 546
  timeout login response 546
  username 547

send 55

seq
  IP ACL (standard) 100
  MAC Access list (extended) 126
  MAC ACL (standard) 122
  Prefix list 129
  seq (Extended IP ACL) 115
  service timestamps 55

service-policy-input 478, 485
service-policy-output 478
service-queue 479
set (policy QoS) 480
set as-path (Route Map) 138
set automatic-tag (Route Map) 138
set comm-list delete (Route Map) 139
set metric (Route Map) 139
set metric-type (Route Map) 139
set origin (Route Map) 140
set tag (Route Map) 140
sflow collector 572
sflow enable (Global) 573
sflow enable (Interface) 573
sflow extended-switch enable 574
sflow polling-interval (Global) 574
sflow polling-interval (Interface) 575
sflow sample-rate (Global) 575
sflow sample-rate (Interface) 576
show accounting 533
show calendar 641
show cam mac stack-unit 342
show cam-acl 149
show clock 642
show config
  Prefix list 130
show config (ACL) 94
show config (from INTERFACE RANGE mode) 258
show config (GVRP) 222, 225
show config (LAG) 281
show config (MSTP) 378
show config (port monitor) 435
show config (Route Map) 140
show config (RSTP) 524
show config (STP) 349, 625
show config (VLAN) 349
show cpu-traffic-stats 58
show crypto 562
show environment 59
show file 28
show file-systems 28
show garp timers 222
show gvrp 223
show gvrp statistics 224
show hardware layer2 acl 683
show hardware layer3 683
show hardware stack-unit 684
show hardware system-flow 690
show hosts 308
show interfaces 259
show interfaces configured 263
show interfaces dampening 264
show interfaces description 265
show interfaces gigabitethernet transceiver 270
<table>
<thead>
<tr>
<th>Command Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.dell.com">www.dell.com</a></td>
</tr>
<tr>
<td>show interfaces port-channel 281</td>
</tr>
<tr>
<td>show interfaces private-vlan 443</td>
</tr>
<tr>
<td>show interfaces rate 158, 159, 160, 161, 172</td>
</tr>
<tr>
<td>show interfaces stack-unit 266</td>
</tr>
<tr>
<td>show interfaces status 267</td>
</tr>
<tr>
<td>show inventory (S-Series) 61</td>
</tr>
<tr>
<td>show ip accounting access-list 96</td>
</tr>
<tr>
<td>show ip cam stack-unit 309</td>
</tr>
<tr>
<td>show ip interface 312</td>
</tr>
<tr>
<td>show ip management-route 313</td>
</tr>
<tr>
<td>show ip mroute 228, 229, 230</td>
</tr>
<tr>
<td>show ip ospf asbr 409</td>
</tr>
<tr>
<td>show ip prefix-list detail 130</td>
</tr>
<tr>
<td>show ip prefix-list summary 131</td>
</tr>
<tr>
<td>show ip protocols 314</td>
</tr>
<tr>
<td>show ip route list 316</td>
</tr>
<tr>
<td>show ip route summary 317</td>
</tr>
<tr>
<td>show ip ssh client-pub-keys 564</td>
</tr>
<tr>
<td>show ip ssh rsa-authentication 564</td>
</tr>
<tr>
<td>show ip traffic 318</td>
</tr>
<tr>
<td>show ip udp-helper 288</td>
</tr>
<tr>
<td>show lacp 335</td>
</tr>
<tr>
<td>show lldp neighbors 361</td>
</tr>
<tr>
<td>show lldp statistics 361</td>
</tr>
<tr>
<td>show logging 603</td>
</tr>
<tr>
<td>show mac accounting access-list 96, 118, 119</td>
</tr>
<tr>
<td>show mac learning-limit 346</td>
</tr>
<tr>
<td>show mac-address-table 343</td>
</tr>
<tr>
<td>show mac-address-table aging-time 345</td>
</tr>
<tr>
<td>show memory (S-Series) 62</td>
</tr>
<tr>
<td>show monitor session 435</td>
</tr>
<tr>
<td>show os-version 29</td>
</tr>
<tr>
<td>show processes cpu (S-Series) 62</td>
</tr>
<tr>
<td>show processes ipc flow-control 66</td>
</tr>
<tr>
<td>show processes memory 67</td>
</tr>
<tr>
<td>show qos class-map 480</td>
</tr>
<tr>
<td>show qos policy-map 481</td>
</tr>
<tr>
<td>show qos policy-map-input 482</td>
</tr>
<tr>
<td>show qos policy-map-output 482</td>
</tr>
<tr>
<td>show qos qos-policy-input 483</td>
</tr>
<tr>
<td>show qos qos-policy-output 483</td>
</tr>
<tr>
<td>show qos qos-policy-output 483</td>
</tr>
<tr>
<td>show qos qos-policy-output 483</td>
</tr>
<tr>
<td>show qos qos-policy-output 483</td>
</tr>
<tr>
<td>show qos qos-policy-output 483</td>
</tr>
<tr>
<td>show qos qos-policy-output 483</td>
</tr>
<tr>
<td>show qos statistics 484</td>
</tr>
<tr>
<td>show qos wred-profile 485</td>
</tr>
<tr>
<td>show range 274</td>
</tr>
<tr>
<td>show redundancy 613</td>
</tr>
<tr>
<td>show rmon 511</td>
</tr>
<tr>
<td>show rmon alarms 511</td>
</tr>
<tr>
<td>show rmon events 513</td>
</tr>
<tr>
<td>show rmon hc-alarm 514</td>
</tr>
<tr>
<td>show rmon history 514</td>
</tr>
<tr>
<td>show rmon log 515</td>
</tr>
<tr>
<td>show rmon statistics 516</td>
</tr>
</tbody>
</table>
hello-time 623
max-age 624
protocol spanning-tree 625
show config 349, 625
show spanning-tree 0 626
spanning-tree 629
spanning-tree (MSTP) 381
spanning-tree 0 (STP) 629
spanning-tree msti 381
spanning-tree mstp 382
spanning-tree pvst 456
spanning-tree rstp 527
speed
10/100/1000 Base-T Ethernet Interfaces 275
S-Series-only commands
redundancy disable-auto-reboot 611
reset stack-unit 612
show hardware layer2 acl 683
show hardware layer3 683
show hardware stack-unit 684
show hardware system-flow 690
show redundancy 613
show system stack-ports 614
stack-unit priority 276, 618
stack-unit provision 618
stack-unit renumber 619
SSH
show ip ssh 563
ssh 565
stack-unit portmode quad 276
stack-unit priority 276, 618
stack-unit provision 618
stack-unit renumber 619
storm-control broadcast 607, 608, 609
storm-control unknown-unicast 609, 610
strict-priority queue 466
switchport mode private-vlan 447

T
TACACS
ip tacacs source-interface 553
tc-flush-standard 458, 528
tc-flush-standard (MSTP) 383
tdr-cable-test 284
Telnet
ip telnet server enable 50
ip telnet source-interface 51
telnet 75
terminal monitor 604
terminal xml 76
TFTP
ip tftp source-interface 51

Time Domain Reflectometer
show tdr 284
tdr-cable-test 284
traceroute 77
track ip 352
trust diffserv 487

U
undebug all 78
upgrade (S-Series management unit) 34, 35
upgrade boot 34
upgrade system 34
uplink-state-group 651
upstream 647, 652

V
virtual-ip 78
VLAN
default vlan-id 348
description 347, 393
interface vlan 249, 250
show vlan 349
tagged 351
untagged 353
vrpdpdelay minimum 671
vrp-group 673
vlan bridge-priority (PVST+) 458
vlan forward-delay 459
vlan hello-time (PVST+) 459
vlan max-age (PVST+) 460
vlan-stack access 659
vlan-stack compatible 659
vlan-stack protocol-type 660
vlan-stack trunk 661
VRRP
advertise-interval 663
authentication-type 664
clear vrrp counters 664
description 665
disable 665
hold-time 666
preempt 666
priority 667
show config 667
show vrrp 668
show vrrp 668
track 670
virtual-address 671
**W**

wred 479, 488
wred-profile 489
write 78
write memory 25