Dell Networking OS Command Line Reference Guide
Dell Networking OS 8.4.6.0
E-Series TeraScale, C-Series, S-Series (S50/S25)
Notes, Cautions, and Warnings

🔍 **NOTE**: A NOTE indicates important information that helps you make better use of your computer.

⚠️ **CAUTION**: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

⚠️ **WARNING**: A WARNING indicates a potential for property damage, personal injury, or death.

---

Information in this publication is subject to change without notice.
© 2014 Dell Force10. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

© 2014 Dell Inc.

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

April 2014
1 Preface
About this Guide ......................................................... 13
Objectives ............................................................. 13
Audience ............................................................... 13
Conventions ........................................................... 13
Information Symbols .................................................. 14
Related Documents ................................................... 14

2 CLI Basics
Accessing the Command Line ....................................... 15
Multiple Configuration Users ....................................... 16
Navigating the Command Line Interface .......................... 16
Obtaining Help ....................................................... 17
Using the Keyword No ............................................... 19
Filtering show Commands ......................................... 19
  Displaying All Output ............................................. 20
  Filtering Command Output Multiple Times ..................... 20
Command Modes .................................................... 20
  EXEC Mode ........................................................ 21
  EXEC Privilege Mode ............................................. 21
  CONFIGURATION Mode .......................................... 21
  INTERFACE Mode ................................................ 21
  LINE Mode ......................................................... 22
  TRACE-LIST Mode ................................................. 22
  MAC ACCESS LIST Mode ....................................... 22
  IP ACCESS LIST Mode .......................................... 23
  ROUTE-MAP Mode ............................................... 23
  PREFIX-LIST Mode ............................................... 23
  AS-PATH ACL Mode .............................................. 23
  IP COMMUNITY LIST Mode .................................... 24
  REDIRECT-LIST Mode ......................................... 24
  SPANNING TREE Mode ......................................... 24
  Per-VLAN SPANNING TREE Plus Mode ......................... 24
  RAPID SPANNING TREE Mode ................................ 25
  MULTIPLE SPANNING TREE Mode ............................. 25
  PROTOCOL GVRP Mode ......................................... 25
  ROUTER OSPF Mode ............................................. 25
  ROUTER RIP Mode ............................................... 26
  ROUTER ISIS Mode .............................................. 26
  ROUTER BGP Mode .............................................. 26
Determining the Chassis Mode .................................... 26

3 File Management
Overview ............................................................. 27
Basic File Management Commands ............................... 27
12 Border Gateway Protocol IPv4 (BGPv4)
   Overview ................................................................. 319
   BGPv4 Commands ......................................................... 319
   MBGP Commands .......................................................... 396
   BGP Extended Communities (RFC 4360) .............................. 423

13 Content Addressable Memory (CAM)
   Overview ................................................................. 433
   CAM Profile Commands .................................................. 433
      Important Points to Remember ...................................... 434
   CAM IPv4flow Commands ............................................... 445
   CAM Layer 2 ACL Commands ............................................ 448

14 Configuration Rollback
   Overview ................................................................. 451
   Commands ................................................................. 451

15 Dynamic Host Configuration Protocol (DHCP)
   Overview ................................................................. 461
   Commands to Configure the System to be a DHCP Server ............ 461
   Commands to Configure Secure DHCP ................................ 469

16 Equal Cost Multi-Path
   Overview ................................................................. 477
   Commands ................................................................. 477

17 Far-End Failure Detection (FEFD)
   Overview ................................................................. 483
   Commands ................................................................. 483

18 Dell Networking OS Resilient Ring Protocol (FRRP)
   Overview ................................................................. 489
   Commands ................................................................. 489
      Important Points to Remember ...................................... 489

19 Dell Networking OS Service Agent
   Overview ................................................................. 497
   Commands ................................................................. 497
20 GARP VLAN Registration (GVRP)
   Overview .......................................................... 529
   Commands .......................................................... 529
   Important Points to Remember .................................. 530

21 High Availability (HA)
   Overview .......................................................... 539
   Commands .......................................................... 539

22 Internet Group Management Protocol (IGMP)
   Overview .......................................................... 549
   IGMP Commands ..................................................... 549
   Important Points to Remember .................................. 549
   IGMP Snooping Commands ......................................... 560
   Important Points to Remember for IGMP Snooping .......... 560
   Important Points to Remember for IGMP Querier .......... 560

23 Interfaces
   Overview .......................................................... 565
   Basic Interface Commands ....................................... 565
   Port Channel Commands .......................................... 622
   Time Domain Reflectometer (TDR) ............................... 632
   Important Points to Remember .................................. 632
   UDP Broadcast ...................................................... 634
   Important Points to Remember .................................. 634

24 IPv4 Routing
   Overview .......................................................... 639
   Commands .......................................................... 639

25 IPv6 Access Control Lists (IPv6 ACLs)
   Overview .......................................................... 691
   Important Points to Remember .................................. 691
   IPv6 ACL Commands ................................................. 692
   IPv6 Route Map Commands ........................................ 718

26 IPv6 Basics
   Overview .......................................................... 723
   Commands .......................................................... 723
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>IPv6 Border Gateway Protocol (IPv6 BGP)</td>
<td>741</td>
</tr>
<tr>
<td>27</td>
<td>Overview</td>
<td>741</td>
</tr>
<tr>
<td>27</td>
<td>IPv6 BGP Commands</td>
<td>741</td>
</tr>
<tr>
<td>27</td>
<td>IPv6 MBGP Commands</td>
<td>803</td>
</tr>
<tr>
<td>28</td>
<td>Intermediate System to Intermediate System (IS-IS)</td>
<td>827</td>
</tr>
<tr>
<td>28</td>
<td>Overview</td>
<td>827</td>
</tr>
<tr>
<td>28</td>
<td>Commands</td>
<td>827</td>
</tr>
<tr>
<td>29</td>
<td>Link Aggregation Control Protocol (LACP)</td>
<td>869</td>
</tr>
<tr>
<td>29</td>
<td>Overview</td>
<td>869</td>
</tr>
<tr>
<td>29</td>
<td>Commands</td>
<td>869</td>
</tr>
<tr>
<td>30</td>
<td>Layer 2</td>
<td>875</td>
</tr>
<tr>
<td>30</td>
<td>Overview</td>
<td>875</td>
</tr>
<tr>
<td>30</td>
<td>MAC Addressing Commands</td>
<td>875</td>
</tr>
<tr>
<td>30</td>
<td>Virtual LAN (VLAN) Commands</td>
<td>896</td>
</tr>
<tr>
<td>31</td>
<td>Link Layer Detection Protocol (LLDP)</td>
<td>905</td>
</tr>
<tr>
<td>31</td>
<td>Overview</td>
<td>905</td>
</tr>
<tr>
<td>31</td>
<td>Commands</td>
<td>905</td>
</tr>
<tr>
<td>31</td>
<td>LLDP-MED Commands</td>
<td>914</td>
</tr>
<tr>
<td>32</td>
<td>Multicast Listener Discovery (MLD)</td>
<td>923</td>
</tr>
<tr>
<td>32</td>
<td>Overview</td>
<td>923</td>
</tr>
<tr>
<td>32</td>
<td>MLD Commands</td>
<td>923</td>
</tr>
<tr>
<td>32</td>
<td>MLD Snooping Commands</td>
<td>930</td>
</tr>
<tr>
<td>33</td>
<td>Multicast Source Discovery Protocol (MSDP)</td>
<td>935</td>
</tr>
<tr>
<td>33</td>
<td>Overview</td>
<td>935</td>
</tr>
<tr>
<td>33</td>
<td>Commands</td>
<td>935</td>
</tr>
<tr>
<td>34</td>
<td>Multiple Spanning Tree Protocol (MSTP)</td>
<td>945</td>
</tr>
<tr>
<td>34</td>
<td>Overview</td>
<td>945</td>
</tr>
<tr>
<td>34</td>
<td>Commands</td>
<td>945</td>
</tr>
<tr>
<td>35</td>
<td>Multicast</td>
<td>961</td>
</tr>
<tr>
<td>35</td>
<td>Overview</td>
<td>961</td>
</tr>
<tr>
<td>35</td>
<td>IPv4 Multicast Commands</td>
<td>961</td>
</tr>
<tr>
<td>35</td>
<td>IPv6 Multicast Commands</td>
<td>978</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
<td>Overview</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>36</td>
<td>Neighbor Discovery Protocol (NDP)</td>
<td>985</td>
</tr>
<tr>
<td>37</td>
<td>Object Tracking</td>
<td>993</td>
</tr>
<tr>
<td>38</td>
<td>Open Shortest Path First (OSPFv2 and OSPFv3)</td>
<td>1013</td>
</tr>
<tr>
<td>39</td>
<td>Policy-based Routing (PBR)</td>
<td>1095</td>
</tr>
<tr>
<td>40</td>
<td>PIM-Dense Mode (PIM-DM)</td>
<td>1105</td>
</tr>
<tr>
<td>41</td>
<td>PIM-Sparse Mode (PIM-SM)</td>
<td>1107</td>
</tr>
<tr>
<td>42</td>
<td>PIM-Source Specific Mode (PIM-SSM)</td>
<td>1141</td>
</tr>
<tr>
<td>43</td>
<td>Power over Ethernet (PoE) and Power over Ethernet Plus (PoE+)</td>
<td>1145</td>
</tr>
<tr>
<td>44</td>
<td>Port Monitoring</td>
<td>1153</td>
</tr>
</tbody>
</table>
Important Points to Remember ............................................. 1154

45 Private VLAN (PVLAN)
  Overview ................................................................. 1167
  Commands ............................................................... 1167
  Private VLAN Concepts .............................................. 1167

46 Per-VLAN Spanning Tree plus (PVST+)
  Overview ................................................................. 1177
  Commands ............................................................... 1177

47 Quality of Service (QoS)
  Overview ................................................................. 1191
  Global Configuration Commands .................................. 1191
  Per-Port QoS Commands .............................................. 1192
  Policy-Based QoS Commands ....................................... 1200
    Important Points to Remember—multicast-bandwidth option 1213
  Queue-Level Debugging .............................................. 1236

48 Router Information Protocol (RIP)
  Overview ................................................................. 1247
  Commands ............................................................... 1247

49 Remote Monitoring (RMON)
  Overview ................................................................. 1267
  Commands ............................................................... 1267

50 Rapid Spanning Tree Protocol (RSTP)
  Overview ................................................................. 1279
  Commands ............................................................... 1279

51 Security
  Overview ................................................................. 1291
  Commands ............................................................... 1291
  AAA Accounting Commands ....................................... 1291
  Authorization and Privilege Commands ......................... 1294
  Authentication and Password Commands ....................... 1298
  RADIUS Commands ................................................ 1309
  TACACS+ Commands ................................................ 1314
  Port Authentication (802.1X) Commands ....................... 1317
    Important Points to Remember ................................ 1317
SSH Server and SCP Commands .................................................. 1325
Trace List Commands ............................................................. 1337
Secure DHCP Commands ......................................................... 1346

52 Service Provider Bridging
Overview .............................................................................. 1351
Commands ............................................................................. 1351
Important Points to Remember ............................................... 1351

53 sFlow
Overview .............................................................................. 1357
Important Points to Remember ............................................... 1357
Commands ............................................................................. 1358

54 SNMP and Syslog
Overview .............................................................................. 1369
SNMP Commands .................................................................. 1369
Important Points to Remember ............................................... 1370
Syslog Commands .................................................................. 1385

55 SONET
Overview .............................................................................. 1399
Commands ............................................................................. 1399

56 S-Series Stacking Commands
Overview .............................................................................. 1417
Commands ............................................................................. 1417

57 Storm Control
Overview .............................................................................. 1425
Commands ............................................................................. 1425
Important Points to Remember ............................................... 1425

58 Spanning Tree Protocol (STP)
Overview .............................................................................. 1433
Commands ............................................................................. 1433

59 Time and Network Time Protocol (NTP)
Overview .............................................................................. 1445
Commands ............................................................................. 1445
60 Uplink Failure Detection (UFD)
  Overview ................................................................. 1461
  Commands .............................................................. 1461

61 VLAN Stacking
  Overview ................................................................. 1471
  Commands .............................................................. 1471
  Important Points to Remember ..................................... 1471

62 Virtual Routing and Forwarding (VRF)
  Overview ................................................................. 1481
  Commands .............................................................. 1481

62 Virtual Link Trunking (VLT)

63 Virtual Router Redundancy Protocol (VRRP)
  Overview ................................................................. 19
  IPv4 VRRP Commands .................................................. 19
  IPv6 VRRP Commands .................................................. 34

64 C-Series Diagnostics and Debugging
  Overview ................................................................. 39
  Inter-process Communication Commands .......................... 39
  RPM Management Port Commands ................................... 45
  Data Path Debugging Commands .................................... 47
  Interface Troubleshooting Commands ............................... 50
  Advanced ASIC Debugging Commands ............................... 54
  ACL and System-Flow Debug Commands ............................. 58
  Interface Management Debug Commands ............................ 60
  Layer 2 Debug Command .............................................. 62
  Trace Logging Commands ............................................. 63
  Offline Diagnostic Commands ....................................... 69
  PoE Hardware Status Commands .................................... 71
  Buffer Tuning Commands ............................................. 72

65 E-Series Debugging and Diagnostics
  Overview ................................................................. 79
  Diagnostics and Monitoring Commands ............................. 79
    Important Points to Remember .................................... 80
  Offline Diagnostic Commands ....................................... 100
  Hardware Commands .................................................. 102
66 S-Series Debugging and Diagnostics

Offline Diagnostic Commands ............................................. 119
Important Points to Remember ......................................... 119
Buffer Tuning Commands .................................................. 121
Hardware Commands ....................................................... 126

A  ICMP Message Types

B  SNMP Traps
Preface

About this Guide

This book provides information on the FTOS Command Line Interface (CLI). It includes some information on the protocols and features found in FTOS and on the Dell Networking systems supported by Dell Networking OS (C-Series C, E-Series E, and S-Series S).

This chapter includes:

• Objectives
• Audience
• Conventions
• Related Documents

Objectives

This document is intended as a reference guide for the Dell Networking OS command line interface (CLI) commands, with detailed syntax statements, along with usage information and sample output.

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

Audience

This document is intended for system administrators who are responsible for configuring or maintaining networks. This guide 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 should 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>
</tbody>
</table>
Information Symbols

Table 1-1 describes symbols contained in this guide.

Table 1-1. Information Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Brief</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[X]</td>
<td>Keywords and parameters within braces must be entered in the CLI.</td>
<td></td>
</tr>
<tr>
<td>[X]</td>
<td>Keywords and parameters within brackets are optional.</td>
<td></td>
</tr>
<tr>
<td>x</td>
<td>y</td>
<td>Keywords and parameters separated by bar require you to choose one.</td>
</tr>
<tr>
<td>x</td>
<td></td>
<td>y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Brief</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>C-Series</td>
<td>This symbol indicates that the selected feature is supported on the C-Series.</td>
</tr>
<tr>
<td>E</td>
<td>E-Series</td>
<td>This symbol indicates that the selected feature is supported on the E-Series TeraScale AND E-Series ExaScale.</td>
</tr>
<tr>
<td>E T</td>
<td>E-Series</td>
<td>This symbol indicates that the selected feature is supported on the E-Series TeraScale platform only.</td>
</tr>
<tr>
<td>S</td>
<td>S-Series</td>
<td>This symbol indicates that the selected feature is supported on the S-Series.</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 your system
- *Release Notes* for your system and Dell Networking OS version
This chapter describes the command structure and command modes. 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 covers the following topics:

• 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 the 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>

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

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

**Figure 2-2. Configuration Mode User Alert**

```plaintext
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)#FTOS#
```

When another user enters the CONFIGURATION mode, Dell Networking OS adds a message similar to the following, where the user in this case is “admin” on vty2:

```plaintext
% 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 Dell Networking OS 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, as 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 the CONFIGURATION mode, the command prompt adds modifiers to further identify the mode. The command modes are explained in Command Modes.

⚠️ **Note:** Some of the following modes are not available on C-Series or S-Series.

### 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>
</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:

## Table 2-1. Command Prompt and Corresponding Command Mode

<table>
<thead>
<tr>
<th>Prompt</th>
<th>CLI Command Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS(conf-if)#12</td>
<td>INTERFACE</td>
</tr>
<tr>
<td>FTOS(conf-if-gi-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-te-0/0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-lo-0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-nu-0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-po-0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-vl-0)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(conf-if-so-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>
<tr>
<td>FTOS(config-ext-nacl)#</td>
<td>IP ACCESS LIST</td>
</tr>
<tr>
<td>FTOS(config-std-nacl)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(config-line-aux)#</td>
<td>LINE</td>
</tr>
<tr>
<td>FTOS(config-line-console)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(config-line-vty)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(config-ext-macl)#</td>
<td>MAC ACCESS LIST</td>
</tr>
<tr>
<td>FTOS(config-std-macl)#</td>
<td></td>
</tr>
<tr>
<td>FTOS(config-mon-sess)#</td>
<td>MONITOR SESSION</td>
</tr>
<tr>
<td>FTOS(config-span)#</td>
<td>STP</td>
</tr>
<tr>
<td>FTOS(config-mstp)#</td>
<td>MULTIPLE SPANNING TREE</td>
</tr>
<tr>
<td>FTOS(config-pvst)#</td>
<td>Per-VLAN SPANNING TREE Plus</td>
</tr>
<tr>
<td>FTOS(config-rstp)#</td>
<td>RAPID SPANNING TREE</td>
</tr>
<tr>
<td>FTOS(config-gvrp)#</td>
<td>PROTOCOL GVRP</td>
</tr>
<tr>
<td>FTOS(config-route-map)#</td>
<td>ROUTE-MAP</td>
</tr>
<tr>
<td>FTOS(config-nprefixl)#</td>
<td>PREFIX-LIST</td>
</tr>
<tr>
<td>FTOS(config-router_rip)#</td>
<td>ROUTER RIP</td>
</tr>
<tr>
<td>FTOS(config-redirect-list)#</td>
<td>REDIRECT</td>
</tr>
<tr>
<td>FTOS(config-router_bgp)#</td>
<td>ROUTER BGP</td>
</tr>
<tr>
<td>FTOS(config-router_ospf)#</td>
<td>ROUTER OSPF</td>
</tr>
<tr>
<td>FTOS(config-router_isis)#</td>
<td>ROUTER ISIS</td>
</tr>
<tr>
<td>FTOS(config-trace-acl)#</td>
<td>TRACE-LIST</td>
</tr>
</tbody>
</table>
— 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 illustrates the results of entering `ip ?` at the prompt.

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

```
FTOS(conf)#ip ?
access-list           Named access-list
as-path              BGP autonomous system path filter
community-list       Add a community list entry
domain-list          Domain name to complete unqualified host name
domain-lookup        Enable IP Domain Name System hostname translation
domain-name          Define the default domain name
fib                   FIB configuration commands
ftp                   FTP configuration commands
host                  Add an entry to the ip hostname table
max-frag-count       Max. fragmented packets allowed in IP re-assembly
multicast-routing     Enable IP multicast forwarding
name-server          Specify address of name server to use
plm                  Protocol Independent Multicast
prefix-list          Build a prefix list
radius               Interface configuration for RADIUS
redirect-list        Named redirect-list
route                Establish static routes
scp                  SCP configuration commands
source-route         Process packets with source routing header options
ssh                  SSR configuration commands
tacacs               Interface configuration for TACACS+
telnet               Specify telnet options
tftp                 TFTP configuration commands
trace-group          Named trace-list
trace-list           Named trace-list
FTOS(conf)#ip
```

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

- The commands are not case sensitive.
- You can enter partial (truncated) command keywords. For example, you can enter `int gig int` for the `interface gigabitethernet interface` command.
- Use the TAB key to complete keywords in commands.
- Use the up arrow key to display the last enabled command.
- Use either the Backspace key or the Delete key to erase the previous character.
Use the **left** and **right arrow** keys to navigate left or right in the Dell Networking OS command line. 

**Table 2-2** defines the key combinations valid at the Dell Networking OS 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-L</td>
<td>Re-enters the previous command.</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-R</td>
<td>Re-enters the previous 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>Ends continuous scrolling of command outputs.</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 discussed 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:

- **display** — display additional configuration information
The `grep` command option has an `ignore-case` sub-option that makes the search case-insensitive. For example, the commands:

- `show run | grep Ethernet` would return a search result with instances containing a capitalized “Ethernet,” such as `interface GigabitEthernet 0/0.`
- `show run | grep ethernet` would not return the search result, above, because it only searches for instances containing a non-capitalized “ethernet.”

Executing the command `show run | grep Ethernet ignore-case` would return 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` 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. 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, you need to use specific commands to launch each mode. Navigation to these modes is discussed in the following sections.

- **Note:** Some of the following modes are not available on C-Series or S-Series.
EXEC Mode

When you initially log in to the switch, by default, you are logged into the EXEC mode. This mode allows you to view settings and to enter the EXEC Privilege mode to configure the device. While you are in the EXEC mode, the > prompt is displayed following the “hostname” prompt, as described above. which is “FTOS” by default. You can change it with the hostname command. See the command hostname. Each mode prompt is preceded by the hostname.

EXEC Privilege Mode

The enable command accesses the EXEC Privilege mode. If an administrator has configured an “Enable” password, you will be prompted to enter it here.

The 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 the CONFIGURATION mode to configure interfaces, routes, and protocols on the switch. While you are logged in to the EXEC Privilege mode, the # prompt is displayed.

CONFIGURATION Mode

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

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

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

INTERFACE Mode

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

To enter INTERFACE mode:
1. Verify that you are logged into the 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, as outlined in Table 2-3.

Table 2-3. Interface prompts

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Interface Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS(conf-if)#</td>
<td>INTERFACE mode</td>
</tr>
<tr>
<td>FTOS(conf-if-gi-0/0)#</td>
<td>Gigabit Ethernet interface followed by slot/port information</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-lo-0)#</td>
<td>Loopback interface number.</td>
</tr>
</tbody>
</table>
LINE Mode

Use the LINE mode to configure console or virtual terminal parameters.

To enter LINE mode:

1. Verify that you are logged in to the 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.

TRACE-LIST Mode

When in the CONFIGURATION mode, use the `trace-list` command to enter the TRACE-LIST mode and configure a Trace list.

1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the `ip trace-list` command. You must include the name of the Trace list. The prompt changes to include (conf-trace-acl).

You can exit this mode by using the `exit` command.

MAC ACCESS LIST Mode

While in the CONFIGURATION mode, use the `mac access-list standard` or `mac access-list extended` command to enter the 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 the 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 the CONFIGURATION mode by entering the `exit` command.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Interface Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTOS(conf-if-nu-0)#</td>
<td>Null Interface followed by zero</td>
</tr>
<tr>
<td>FTOS(conf-if-po-0)#</td>
<td>Port-channel interface number</td>
</tr>
<tr>
<td>FTOS(conf-if-vl-0)#</td>
<td>VLAN Interface followed by VLAN number (range 1 to 4094)</td>
</tr>
<tr>
<td>FTOS(conf-if-so-0/0)#</td>
<td>SONET interface followed by slot/port information.</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; see interface range).</td>
</tr>
</tbody>
</table>
**IP ACCESS LIST Mode**

While in the CONFIGURATION mode, use the `ip access-list standard` or `ip access-list extended` command to enter the 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 the 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 the CONFIGURATION mode by entering the `exit` command.

**ROUTE-MAP Mode**

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

To enter ROUTE-MAP mode:
1. Verify that you are logged in to the 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 the CONFIGURATION mode by entering the `exit` command.

**PREFIX-LIST Mode**

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

To enter PREFIX-LIST mode:
1. Verify that you are logged in to the 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 the CONFIGURATION mode by entering the `exit` command.

**AS-PATH ACL Mode**

Use the AS-PATH ACL mode to configure an AS-PATH Access Control List (ACL) on the E-Series. See Chapter 9, Access Control Lists (ACL).

To enter AS-PATH ACL mode:
1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the `ip as-path access-list` command. You must include a name for the AS-PATH ACL. The prompt changes to include (config-as-path).

You can return to the CONFIGURATION mode by entering the `exit` command.
**IP COMMUNITY LIST Mode**

Use the IP COMMUNITY LIST mode to configure an IP Community ACL on the E-Series. See Chapter 9, Access Control Lists (ACL).

To enter IP COMMUNITY LIST mode:
1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the `ip community-list` command. You must include a name for the Community list. The prompt changes to include (config-community-list).

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

**REDIRECT-LIST Mode**

Use the REDIRECT-LIST mode to configure a Redirect list on the E-Series, as described in Chapter 39, Policy-based Routing (PBR).

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

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

**SPANNING TREE Mode**

Use the STP mode to enable and configure the Spanning Tree protocol, as described in Chapter 58, Spanning Tree Protocol (STP).

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

You can return to the CONFIGURATION mode by entering 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 Chapter 46, 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 the CONFIGURATION mode.
2. Enter the `protocol spanning-tree pvst` command.

You can return to the CONFIGURATION mode by entering the `exit` command.
RAPID SPANNING TREE Mode

Use PVST+ mode to enable and configure the RSTP protocol, as described in Chapter 50, Rapid Spanning Tree Protocol (RSTP).

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

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

MULTIPLE SPANNING TREE Mode

Use MULTIPLE SPANNING TREE mode to enable and configure the Multiple Spanning Tree protocol, as described in Chapter 34, Multiple Spanning Tree Protocol (MSTP).

To enter MULTIPLE SPANNING TREE mode:
1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the `protocol spanning-tree mstp` command.

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

PROTOCOL GVRP Mode

Use the PROTOCOL GVRP mode to enable and configure GARP VLAN Registration Protocol (GVRP), as described in Chapter 20, GARP VLAN Registration (GVRP).

To enter PROTOCOL GVRP mode:
1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the `protocol gvrp` command syntax.

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

ROUTER OSPF Mode

Use the ROUTER OSPF mode to configure OSPF, as described in Chapter 38, Open Shortest Path First (OSPFv2 and OSPFv3).

To enter ROUTER OSPF mode:
1. Verify that you are logged into the CONFIGURATION mode.
2. Use the `router ospf {process-id}` command. The prompt changes to include (conf-router_ospf-id).

You can switch to the INTERFACE mode by using the `interface` command or you can switch to the ROUTER RIP mode by using the `router rip` command.
ROUTER RIP Mode

Use the ROUTER RIP mode to configure RIP on the C-Series or E-Series, as described in Chapter 48, Router Information Protocol (RIP).

To enter ROUTER RIP mode:
1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the `router rip` command. The prompt changes to include (conf-router_rip).

You can switch to the INTERFACE mode by using the `interface` command or you can switch to the ROUTER OSPF mode by using the `router ospf` command.

ROUTER ISIS Mode

Use the ROUTER ISIS mode to configure ISIS on the E-Series, as described in Intermediate System to Intermediate System (IS-IS).

To enter ROUTER ISIS mode:
1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the `router isis [tag]` command. The prompt changes to include (conf-router_isis).

You can switch to the INTERFACE mode by using the `interface` command or you can switch to the ROUTER RIP mode by using the `router rip` command.

ROUTER BGP Mode

Use the ROUTER BGP mode to configure BGP on the C-Series or E-Series, as described in Chapter 12, Border Gateway Protocol IPv4 (BGPv4).

To enter ROUTER BGP mode:
1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the `router bgp as-number` command. The prompt changes to include (conf-router_bgp).

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

Determining the Chassis Mode

The chassis mode in Dell Networking OS determines which hardware is being supported in an E-Series chassis. The chassis mode is programmed into an EEPROM on the backplane of the chassis and the change takes place only after the chassis is rebooted. Configuring the appropriate chassis mode enables the system to use all the ports on the card and recognize all software features.
File Management

Overview

This chapter contains commands needed to manage the configuration files and includes other file management commands found in Dell Networking OS. This chapter contains these sections:

- Basic File Management Commands
- Upgrading the C-Series FPGA

Basic File Management Commands

The commands included in this chapter are:

- boot config
- boot host
- boot network
- boot system
- boot system gateway
- cd
- change bootflash-image
- copy
- copy (Streamline Upgrade)
- copy running-config startup-config
- delete
- dir
- download alt-boot-image
- download alt-full-image
- download alt-system-image
- format (C-Series and E-Series)
- format flash (S-Series)
- logging coredump
- logging coredump server
- pwd
- rename
- boot system
- show boot system
- show boot verification
• show bootvar
• show file
• show file-systems
• show linecard
• show os-version
• show running-config
• show startup-config
• show version
• upgrade (E-Series version)
• upgrade (C-Series version)
• upgrade (S-Series management unit) on page 56
• upgrade fpga-image
• upgrade poe-controller-firmware

boot config

Set the location and name of the configuration file that is loaded at system start-up (or reload) instead of the default startup-configuration.

Syntax

```
boot config {remote-first | rpm0 file-url | rpm1 file-url}
```

Parameters

- **remote-first**: Enter the keywords `remote-first` to attempt to load the boot configuration files from a remote location.
- **rpm0**: Enter the keywords `rpm0` first to specify the local boot configuration file for RPM 0.
- **rpm1**: Enter the keywords `rpm1` first to specify the local boot configuration file for RPM 1.
- **file-url**: Enter the location information:
  - For a file on the internal Flash, enter `flash://` followed by the filename.
  - For a file on the external Flash, enter `slot0://` followed by the filename.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

Usage Information

To display these changes in the show bootvar command output, you must save the running configuration to the startup configuration (copy running-config startup-config or write).

Dell Networking OS strongly recommends using local files for configuration (RPM0 or RPM1 flash or slot0).

When you specify a file as the **boot config** file, it is listed in the boot variables (bootvar) as LOCAL CONFIG FILE. If you do not specify a boot config file, then the startup-configuration is used, although the bootvar shows LOCAL CONFIG FILE = variable does not exist. When you specify a boot config file, the switch reloads with that config file, rather than the startup-config. Note that if you specify a local config file which is not present in the specified location, then the startup-configuration is loaded.
The **write memory** command always saves the running-configuration to the file labeled `startup-configuration`. When using a local config file other than the `startup-config`, use the **copy** command to save any running-configuration changes to that local file.

**Output for show bootvar with no boot configuration configured**

```
FTOS#show bootvar
PRIMARY IMAGE FILE = flash://FTOS-EF-8.2.1.0.bin
SECONDARY IMAGE FILE = flash://FTOS-EF-7.6.1.0.bin
DEFAULT IMAGE FILE = flash://FTOS-EF-7.5.1.0.bin
LOCAL CONFIG FILE = variable does not exist
PRIMARY HOST CONFIG FILE = variable does not exist
SECONDARY HOST CONFIG FILE = variable does not exist
PRIMARY NETWORK CONFIG FILE = variable does not exist
SECONDARY NETWORK CONFIG FILE = variable does not exist
CURRENT IMAGE FILE = flash://FTOS-EF-8.2.1.0.bin
CURRENT CONFIG FILE 1 = flash://startup-config
CURRENT CONFIG FILE 2 = variable does not exist
CONFIG LOAD PREFERENCE = local first
BOOT INTERFACE GATEWAY IP ADDRESS = variable does not exist
```

**Output for show bootvar with boot configuration configured**

```
FTOS#show bootvar
PRIMARY IMAGE FILE = flash://FTOS-EF-8.2.1.0.bin
SECONDARY IMAGE FILE = flash://FTOS-EF-7.6.1.0.bin
DEFAULT IMAGE FILE = flash://FTOS-EF-7.5.1.0.bin
LOCAL CONFIG FILE = variable does not exist
PRIMARY HOST CONFIG FILE = variable does not exist
SECONDARY HOST CONFIG FILE = variable does not exist
PRIMARY NETWORK CONFIG FILE = variable does not exist
SECONDARY NETWORK CONFIG FILE = variable does not exist
CURRENT IMAGE FILE = flash://FTOS-EF-8.2.1.0.bin
CURRENT CONFIG FILE 1 = flash://CustomerA.cfg
CURRENT CONFIG FILE 2 = variable does not exist
CONFIG LOAD PREFERENCE = local first
BOOT INTERFACE GATEWAY IP ADDRESS = variable does not exist
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show bootvar</strong></td>
<td>Display the variable settings for the E-Series boot parameters.</td>
</tr>
</tbody>
</table>

**boot host**

Set the location of the configuration file from a remote host.

**Syntax**

```
boot host {primary | secondary} remote-url
```

**Parameters**

- **primary**
  - Enter the keywords `primary` to attempt to load the primary host configuration files.

- **secondary**
  - Enter the keywords `secondary` to attempt to load the secondary host configuration files.

- **remote-url**
  - Enter the following location keywords and information:
    - For a file on an FTP server, enter `ftp://user:password@hostip/filepath`
    - For a file on a TFTP server, enter `tftp://hostip/filepath`

**Defaults**

- Not configured.

**Command Modes**

- CONFIGURATION
**Command History**

Version 7.5.1.0 Introduced on C-Series

E-Series original Command

**Usage Information**

To display these changes in the show bootvar command output, you must save the running configuration to the startup configuration (using the copy command).

**Related Commands**

show bootvar Display the variable settings for the E-Series boot parameters.

---

**boot network**

Set the location of the configuration file in a remote network.

**Syntax**

```plaintext
boot network {primary | secondary} remote-url
```

**Parameters**

- `primary`: Enter the keywords `primary` to attempt to load the primary network configuration files.
- `secondary`: Enter the keywords `secondary` to attempt to load the secondary network configuration files.
- `remote-url`: Enter the following location keywords and information:
  - For a file on an FTP server, enter `ftp://user:password@hostip/filepath`
  - For a file on a TFTP server, enter `tftp://hostip/filepath`

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

Version 7.5.1.0 Introduced on C-Series

E-Series original Command

**Usage Information**

To display these changes in the show bootvar command output, you must save the running configuration to the startup configuration (using the copy command).

**Related Commands**

show bootvar Display the variable settings for the E-Series boot parameters.

---

**boot system**

Tell the system where to access the Dell Networking OS image used to boot the system.

**Syntax**

```plaintext
boot system {rpm0 | rpm1} {default | primary | secondary} file-url
```

**Parameters**

- `rpm0`: Enter the keyword `rpm0` to configure boot parameters for RPM0.
- `rpm1`: Enter the keyword `rpm1` to configure boot parameters for RPM1.
- `default`: After entering `rpm0` or `rpm1`, enter the keyword `default` to specify the parameters to be used if those specified by `primary` or `secondary` fail. The default location should always be the internal flash device (flash:), so that you can be sure that a verified image is available there.

**Command Modes**

CONFIGURATION

**Command History**

Version 7.5.1.0 Introduced on C-Series

E-Series original Command
### primary
After entering `rpm0` or `rpm1`, enter the keyword `primary` to configure the boot parameters used in the first attempt to boot Dell Networking OS.

### secondary
After entering `rpm0` or `rpm1`, enter the keyword `secondary` to configure boot parameters used if the primary operating system boot selection is not available.

### file-url
To boot from a file:
- on the internal Flash, enter `flash://` followed by the filename.
- on an FTP server, enter `ftp://user:password@hostip/filepath`
- on the external Flash, enter `slot0://` followed by the filename.
- on a TFTP server, enter `tftp://hostip/filepath`

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Not configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>CONFIGURATION</td>
</tr>
<tr>
<td>Command History</td>
<td>Version 7.5.1.0 Introduced on C-Series</td>
</tr>
<tr>
<td>Usage Information</td>
<td>To display these changes in the <code>show bootvar</code> command output, you must save the running configuration to the startup configuration (using the <code>copy</code> command) and reload system.</td>
</tr>
<tr>
<td>Related Commands</td>
<td>change bootflash-image Change the primary, secondary, or default boot image configuration.</td>
</tr>
</tbody>
</table>

### boot system gateway
Specify the IP address of the default next-hop gateway for the management subnet.

<table>
<thead>
<tr>
<th>Syntax</th>
<th><code>boot system gateway ip-address</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td><code>ip-address</code> Enter an IP address in dotted decimal format.</td>
</tr>
<tr>
<td>Command Modes</td>
<td>CONFIGURATION</td>
</tr>
<tr>
<td>Command History</td>
<td>Version 7.5.1.0 Introduced on C-Series</td>
</tr>
<tr>
<td>Usage Information</td>
<td>Saving the address to the startup configuration file preserves the address in NVRAM in case the startup configuration file is deleted.</td>
</tr>
<tr>
<td>Related Commands</td>
<td>change bootflash-image Change the primary, secondary, or default boot image configuration.</td>
</tr>
</tbody>
</table>
cd

Change to a different working directory.

Syntax

cd directory

Parameters

directory (OPTIONAL) Enter one of the following:

- flash: (internal Flash) or any sub-directory
- slot0: (external Flash) or any sub-directory (C-Series and E-Series only)

Command Modes

EXEC Privilege

Command History

Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
E-Series original Command

change bootflash-image

Change boot flash image from which to boot.

Syntax

change bootflash-image {cp | linecard linecard-slot | rp}

Parameters

cp Enter the keyword cp to change the bootflash image on the Control Processor on the RPM.

linecard linecard-slot Enter the keyword linecard followed by the slot number to change the bootflash image on a specific line card.

- C-Series Range: 0-7
- E-Series Range: 0 to 13 on the E1200; 0 on 6 on the E600, and 0 to 5 on the E300.

rp Enter the keyword rp to change the bootflash image on the RPM Route Processor.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

Version 7.5.1.0 Introduced on C-Series
E-Series original Command

Usage Information

A system message appears stating that the bootflash image has been changed. You must reload the system before the system can switch to the new bootflash image.

copy

Copy one file to another location. Dell Networking OS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the hostip field).

Syntax

copy source-file-url destination-file-url
Dell Networking OS supports a maximum of 100 files, at the root directory level, on both the internal and external Flash.

The `usbflash` and `rpm0usbflash` commands are supported on E-Series ExaScale platform only. Refer to the Dell Networking OS Release Notes for a list of approved USB vendors.

When copying a file to a remote location (for example, using Secure Copy (SCP)), enter only the keywords and Dell Networking OS 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. Dell Networking OS 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, Dell Networking OS creates a backup file on the internal flash of the startup configuration.

Dell Networking OS supports copying the running-configuration to a TFTP server or to an FTP server:

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

Command Example: copy running-config scp:

FTOS#copy running-config scp:
Address or name of remote host []: 10.10.10.1
Destination file name [startup-config]? old_running
User name to login remote host? sburgess
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.

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

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

copy (Streamline Upgrade)

Copy a system image to a local file and update the boot profile.

Syntax

copy source-url target-url [boot-image [synchronize-rpm [external]]]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-url</td>
<td>Enter the source file in url format. The source file is a valid Dell Networking release image. Image validation is automatic.</td>
</tr>
<tr>
<td>target-url</td>
<td>Enter the local target file in url format.</td>
</tr>
<tr>
<td>boot-image</td>
<td>Enter the keyword boot-image to designate this copy command as a streamline update.</td>
</tr>
<tr>
<td>synchronize-rpm</td>
<td>Enter the keyword synchronize-rpm to copy the new image file to the peer RPM.</td>
</tr>
<tr>
<td>external</td>
<td>Enter the keyword external to designate the target device on the peer RPM as external flash (instead of the default internal flash). Default: Internal Flash</td>
</tr>
</tbody>
</table>

Defaults

No default behavior

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added IPv6 addressing support for FTP, TFTP, and SCP.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
In this streamline copy command, the source image is copied to the primary RPM and then, if specified, to the standby RPM. After the copy is complete, the new image file path on each RPM is automatically configured as the primary image path for the next boot. The current system image (the one from which the RPM booted) is automatically configured as the secondary image path.

Dell Networking OS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP.

Note: The keywords `boot-image`, `synchronize-rpm`, and `external` can be used on the Primary RPM only.

copy running-config startup-config

Copy running configuration to the startup configuration.

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

Command Modes EXEC Privilege

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.

When you use the `copy running-config startup-config duplicate` command to copy the running configuration to the startup configuration, Dell Networking OS creates a backup file on the internal flash of the startup configuration.

delete

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

Syntax `delete flash-url [no-confirm]`

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 `slot0://` followed by the filename or directory name.

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

Command Modes EXEC Privilege

Command History

- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command
**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 `slot0://` followed by the filename or directory name.

**Command Modes**

- EXEC Privilege

**Command History**

- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series

**Example**

Command Example `dir` for the Internal Flash

```
FTOS#dir
Directory of flash:
1 -rwx 6478482 May 13 101 16:54:34 E1200.BIN
flash: 64077824 bytes total (57454592 bytes free)
FTOS#
```

**Related Commands**

- `cd` Change working directory.

---

**download alt-boot-image**

Download an alternate boot image to the chassis.

**Syntax**

```
download alt-boot-image file-url
```

**Command Modes**

- EXEC Privilege

**Command History**

- Version 7.7.1.0 Removed from E-Series and C-Series
- Version 7.5.1.0 Introduced on C-Series

**Usage Information**

Starting with Dell Networking OS 7.7.1.0, the functions of this command are incorporated into the `upgrade` command.

For software upgrade details, see the Dell Networking OS Release Notes.

**Related Commands**

- `upgrade (E-Series version)` Upgrade the bootflash or boot selector versions.
- `upgrade (C-Series version)` Upgrade the bootflash or boot selector versions.
download alt-full-image

Download an alternate Dell Networking OS image to the chassis.

Syntax

download alt-full-image file-url

Command Modes
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Removed from E-Series</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

Starting with Dell Networking OS 7.7.1.0, the functions of this command are incorporated into the upgrade command.

For software upgrade details, see the Dell Networking OS Release Notes.

Related Commands

upgrade (E-Series version) Upgrade the bootflash or boot selector versions

download alt-system-image

Download an alternate system image (not the boot flash or boot selector image) to the chassis.

Syntax

download alt-system-image file-url

Command Modes
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Removed from E-Series</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

Starting with Dell Networking OS 7.7.1.0, the functions of this command are incorporated into the upgrade command.

For software upgrade details, see the Dell Networking OS Release Notes.

Related Commands

upgrade (E-Series version) Upgrade the bootflash or boot selector versions

format (C-Series and E-Series)

Erase all existing files and reformat a file system. Once the file system is formatted, files cannot be restored.

Syntax

format filesystem: [dosFs1.0 | dosFs2.0]

Parameters

filesystem: Enter one of the following:
- To reformat the internal Flash, enter flash:.
- To reformat the external Flash, enter slot0:
**dosFs1.0**
Enter the keyword `dosFs1.0` to format in DOS 1.0 (the default)

**dosFs2.0**
Enter the keyword `dosFs2.0` to format in DOS 2.0

**Default**
DOS 1.0 (dosFs1.0)

**Command Modes**
EXEC Privilege

**Command History**
- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command

**Usage Information**
When you format flash:

1. The startup-config is erased.
2. All cacheboot data files are erased and you must reconfigure cacheboot to regain it.
3. All generated SSH keys are erased and you must recreate them.
4. All archived configuration files are erased.
5. All trace logs, crash logs, core dumps, and call-home logs are erased.
6. In-service Process patches are erased.

After reformatting is complete, three empty directories are automatically created on flash: CRASH_LOG_DIR, TRACE_LOG_DIR and NVTRACE_LOG_DIR.

**Note:** Version option is available on LC-ED-RPM only. LC-EE3-RPM, LC-EF-RPM, and LC-EF3-RPM supports DOS 2.0 only.

**Related Commands**
- `show file` Display contents of a text file in the local filesystem.
- `show file-systems` Display information about the file systems on the system.

---

**format flash (S-Series)**

S

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

**Syntax**
`format flash:`

**Default**
flash memory

**Command Modes**
EXEC Privilege

**Command History**
- Version 7.8.1.0 Introduced on S-Series

**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 `copy run start`).
Related Commands

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

logging coredump

Enable coredump.

Syntax

logging coredump {cp | linecard {number | all} | rps}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp</td>
<td>Enable coredump for the CP.</td>
</tr>
<tr>
<td>linecard</td>
<td>Enable coredump for a linecard.</td>
</tr>
<tr>
<td>rps</td>
<td>Enable coredump for RP 1 and 2.</td>
</tr>
</tbody>
</table>

Defaults

The kernel coredump is enabled by default for RP 1 and 2 on E-Series. The kernel coredump for CP and application coredump are disabled on all systems by default.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Restructured command to accommodate core dumps for CP. Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Application coredump naming convention enhanced to include application.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

The kernel core dump can be large and may take up to 5 to 30 minutes to upload. Dell Networking OS does not overwrite application core dumps so you should delete them as necessary to conserve space on the flash; if the flash is out of memory, the coredump is aborted. On the S-Series, if the FTP server is not reachable, the application coredump is aborted. Dell Networking OS completes the coredump process and wait 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>Designate a server 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 | ipv6-address} username name password [type] password

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>Enter the server IPv4 address (A.B.C.D) or IPv6 address (X:X::X::X).</td>
</tr>
<tr>
<td>ipv6-address</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>Enter a username to access the target server.</td>
</tr>
</tbody>
</table>
### 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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Restructured command to accommodate core dumps for CP. Introduced on C-Series and S-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

Since 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 will over-write 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`  
  Disable the kernel coredump

---

**pwd**

Display the current working directory.

**Syntax**

`pwd`

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**Example**

Command Example: `pwd`

```
FTOS#pwd  
flash: 
FTOS#
```

**Related Commands**

- `cd`  
  Change directory.
rename

Rename a file in the local file system.

Syntax

rename url url

Parameters

url

Enter the following keywords and a filename:
- For a file on the internal Flash, enter flash:// followed by the filename.
- For a file on the external Flash, enter slot0:// followed by the filename.

Command Modes

EXEC Privilege

Command History

Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
E-Series original Command

show boot system

Displays information about boot images currently configured on the system.

Syntax

show boot system {all | linecard [slot | all] | rpm}

Parameters

all

Enter this keyword to display boot image information for all linecards and RPMs.

linecard

Enter this keyword to display boot image information for the specified line card(s) on the system.

rpm

Enter this keyword to display boot image information for all RPMs on the system.

Defaults

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.7.1.0 Introduced on C-Series and E-Series
Example

FTOS#show boot system all

Current system image information in the system:

<table>
<thead>
<tr>
<th>Type</th>
<th>Boot Type</th>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>RP1</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>RP2</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>linecard 0</td>
<td>is not</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecard 1</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>linecard 2</td>
<td>DOWNLOAD</td>
<td>4.7.5.387</td>
<td>6.5.1.8</td>
</tr>
<tr>
<td>linecard 3</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>linecard 4</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>linecard 5</td>
<td>is not</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Peer RPM:

<table>
<thead>
<tr>
<th>Type</th>
<th>Boot Type</th>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>RP1</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
<tr>
<td>RP2</td>
<td>DOWNLOAD</td>
<td>invalid</td>
<td>invalid</td>
</tr>
</tbody>
</table>

show boot verification

Displays consistency information about boot images currently configured on the system.

Syntax

show boot verification {all | linecard [slot] | all | rpm}

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enter this keyword to display boot image information for all linecards and RPMs.</td>
</tr>
<tr>
<td>linecard</td>
<td>Enter this keyword to display boot image information for the specified line card(s) on the system.</td>
</tr>
<tr>
<td>rpm</td>
<td>Enter this keyword to display boot image information for all RPMs on the system.</td>
</tr>
</tbody>
</table>

Defaults

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.6.1.0 Introduced on C-Series and E-Series
Example

FTOS#show boot verification all
System image verification in progress...
System image verification:

<table>
<thead>
<tr>
<th>Type</th>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Error: Linecard 0 is not present.</td>
<td>Passed</td>
<td>Failed</td>
</tr>
<tr>
<td>Linecard 1</td>
<td>Passed</td>
<td>Failed</td>
</tr>
<tr>
<td>% Error: Linecard 3 is not present.</td>
<td>Passed</td>
<td>Failed</td>
</tr>
<tr>
<td>Linecard 4</td>
<td>Passed</td>
<td>Failed</td>
</tr>
<tr>
<td>% Error: Linecard 5 is not present.</td>
<td>Passed</td>
<td>Failed</td>
</tr>
<tr>
<td>Linecard 6</td>
<td>Passed</td>
<td>Failed</td>
</tr>
<tr>
<td>Linecard 7</td>
<td>Passed</td>
<td>Failed</td>
</tr>
<tr>
<td>RPM 1</td>
<td>Passed</td>
<td>Passed</td>
</tr>
</tbody>
</table>

Usage Information

The **show boot verification** output displays **Failed** in the following cases:

- the checksum of the file in bootflash is wrong.
- the file is non-existent.

Use the **show boot system all** command to identify the reason. In both the cases, a new file should be placed in bootflash.

show bootvar

Display the variable settings for the E-Series boot parameters.

Syntax

`show bootvar`

Command Modes

EXEC Privilege

Command History

- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command

Example

Command Output example: **show bootvar**

```
FTOS#show bootvar
PRIMARY IMAGE FILE =  ftp://box:password@10.31.1.205//home/5.3.1/5.3.1.0/FTOS-ED-RPM1-5.3.1.0.bin
SECONDARY IMAGE FILE =  variable does not exist
DEFAULT IMAGE FILE =  flash://FTOS-ED-5.3.1.0.bin
LOCAL CONFIG FILE =  variable does not exist
PRIMARY HOST CONFIG FILE =  variable does not exist
SECONDARY HOST CONFIG FILE =  variable does not exist
PRIMARY NETWORK CONFIG FILE =  variable does not exist
SECONDARY NETWORK CONFIG FILE =  variable does not exist
CURRENT IMAGE FILE =  ftp://box:password@10.31.1.205//home/5.3.1/5.3.1.0/FTOS-ED-RPM1-5.3.1.0.bin
CURRENT CONFIG FILE 1 =  flash://startup-config
CURRENT CONFIG FILE 2 =  variable does not exist
CONFIG LOAD PREFERENCE =  local first
BOOT INTERFACE GATEWAY IP ADDRESS =  variable does not exist
FTOS#
```
### show file

Display contents of a text file in the local filesystem.

**Syntax**

```
show file filesystem
```

**Parameters**

- `filesystem` Enter one of the following:
  - `flash`: for the internal Flash
  - `slot0`: for the external Flash

**Command Modes**

EXEC Privilege

**Command History**

- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command

**Example**

Command output example (Partial): `show file`

```
FTOS#show file flash://startup-config
!
boot system rpm0 primary ftp://test:server@10.16.1.144//home/images/
E1200_405-3.1.2b1.86.bin
boot system rpm0 secondary flash://FTOS-ED-6.1.1.0.bin
boot system rpm0 default ftp://@/\n!
redundancy auto-synchronize persistent-data
redundancy primary rpm0
!
hostname E1200-20
!
enable password 7 94849d8482d5c3
!
username test password 7 93e1e7e2ef
!
enable restricted 7 948a9d848cd5c3
!
protocol spanning-tree 0
bridge-priority 8192
rapid-root-failover enable
!
interface GigabitEthernet 0/0
  no ip address
  shutdown
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>boot config</code></td>
<td>Set the location of configuration files on local devices.</td>
</tr>
<tr>
<td><code>boot host</code></td>
<td>Set the location of configuration files from the remote host.</td>
</tr>
<tr>
<td><code>boot network</code></td>
<td>Set the location of configuration files from a remote network.</td>
</tr>
<tr>
<td><code>boot system</code></td>
<td>Set the location of Dell Networking OS image files.</td>
</tr>
<tr>
<td><code>boot system gateway</code></td>
<td>Specify the IP address of the default next-hop gateway for the management subnet.</td>
</tr>
<tr>
<td><code>format (C-Series and E-Series)</code></td>
<td>Erase all existing files and reformat a filesystem on the E-Series or C-Series platform.</td>
</tr>
<tr>
<td><code>format flash (S-Series)</code></td>
<td>Erase all existing files and reformat the filesystem in the internal flash memory on and S-Series.</td>
</tr>
<tr>
<td><code>show file-systems</code></td>
<td>Display 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

**Example**

Command Output example: `show file-system`

```
FTOS#show file-systems
Size(b) Free(b) Feature Type Flags Prefixes
63938560 51646464 dosFs2.0 MMC rw flash:
63938560 18092032 dosFs1.0 MMC rw slot0:
- - network rw ftp:
- - network rw tftp:
- - network rw scp:
```

**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>
</tbody>
</table>
|           |     • r = read access
|           |     • w = write access                                                      |
| Prefixes  | Displays the name of the storage location.                                  |

**Related Commands**

- `format (C-Series and E-Series)` Erase all existing files and reformat a filesystem.
- `format flash (S-Series)` Erase all existing files and reformat the filesystem in the internal flash memory.
- `show file` Display contents of a text file in the local filesystem.
- `show sfm` Display the current SFM status.
**show linecard**

View the current linecard status.

**Syntax**

```markdown
show linecard [number | all | boot-information]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter a number to view information on that linecard. Range: 0 to 6.</td>
</tr>
<tr>
<td>all</td>
<td>(OPTIONAL) Enter the keyword all to view a table with information on all present linecards.</td>
</tr>
<tr>
<td>boot-information</td>
<td>(OPTIONAL) Enter the keyword boot-information to view cache boot information of all line cards in table format.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

- **Version 7.5.1.0** Introduced on C-Series

**E-Series original Command**

**Example**

Command output example (E-Series): `show linecard boot-information`

```
FTOS#show linecard boot-information
-- Line cards --
Serial       Booted       Next         Cache         Boot
#  Status  CurType  number        from         boot         boot
flash
------------------------------------------------------------------------
0    -       
1    -       
2    -       
3  online  E48TF FX000032632  4.7.7.171  4.7.7.171 A: invalid  B: invalid
   A: 2.3.2.1 [b] B: 2.3.2.1
4    -       
5    -       
6    -       
FTOS#
```

**show os-version**

Display the release and software image version information of the image file specified or, optionally, the image loaded on the RPM (C-Series and E-Series only).

**Syntax**

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 the external Flash, enter slot0:// followed by the filename.  
- For a file on a TFTP server, enter tftp://hostip/filepath  
**Note:** ftp and tftp are the only S-Series options. |

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege
Command History

- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series

E-Series original Command

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

Example

Command output example (E-Series): `show os-version`

```
FTOS#show os-version
RELEASE IMAGE INFORMATION :
Platform          Version        Size           ReleaseTime
E-series:  EF          7.5.1.0    27676168    Aug 15 2007 10:06:21

TARGET IMAGE INFORMATION :
Type          Version                   Target    checksum
runtime          7.5.1.0        control processor      passed
runtime          7.5.1.0                 linecard      passed
boot flash       2.4.1.1        control processor      passed
boot flash       2.4.1.1                 linecard      passed
boot selector    2.4.1.1        control processor      passed
boot selector    2.4.1.1                 linecard      passed

FTOS#
```

Example

Command output example (C-Series): `show os-version`

```
FTOS#show os-version
RELEASE IMAGE INFORMATION :
Platform          Version        Size           ReleaseTime
C-series:  CB          7.5.1.0    23734363    Aug 18 2007 11:49:51

TARGET IMAGE INFORMATION :
Type          Version                   Target    checksum
runtime          7.5.1.0        control processor      passed
runtime          7.5.1.0                 linecard      passed
boot flash       2.7.0.1        control processor      passed
boot flash       1.0.0.40                 linecard      passed
boot selector    2.7.0.1        control processor      passed
boot selector    1.0.0.40                 linecard      passed

FPGA IMAGE INFORMATION :
Card          Version       Release Date
Primary RPM    4.1          May 02 2007
Secondary RPM  4.1          May 02 2007
LC0            3.2          May 02 2007
LC5            3.2          May 02 2007
LC6            2.2          May 02 2007

FTOS#
```

**show running-config**

Display the current configuration and display changes from the default values.

**Syntax**

```
show running-config [entity] [configured] [status]
```
Parameters

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

- **aaa** for the current AAA configuration
- **acl** for the current ACL configuration
- **arp** for the current static ARP configuration
- **as-path** for the current AS-path configuration
- **bgp** for the current BGP configuration
- **boot** for the current boot configuration
- **cam-profile** for the current CAM profile in the configuration.
- **class-map** for the current class-map configuration
- **community-list** for the current community-list 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
- **isis** for the current ISIS 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
- **management-address** for the current MAC address configuration
- **management-route** for the current Management port forwarding configuration
- **mroute** for the current Mroutes configuration
- **ntp** for the current NTP configuration
- **ospp** 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
- **redirect-list** for the current redirect-list configuration
- **redundancy** for the current RPM redundancy configuration
- **resolve** for the current DNS configuration
- **rip** for the current RIP configuration
- **route-map** for the current route map configuration
**Command Modes**

EXEC Privilege

---

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VLT option.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added hardware-monitor option</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Expanded to include last configuration change and start-up last updated (date and time) and who made the change</td>
</tr>
<tr>
<td>6.5.4.0</td>
<td>Added status option</td>
</tr>
</tbody>
</table>

---

**Example**

Command output example (partial): **show running-config**

```
FTOS#show running-config
Current Configuration ...
! Version 7.4.1.0
! Last configuration change at Tue Apr 10 17:43:38 2007 by admin
! Startup-config last updated at Thu Mar 29 02:35:08 2007 by default
!
boot system rpm0 primary flash:/FTOS-EF-7.4.1.0.bin
boot system rpm0 secondary flash:/FTOS-EF-6.3.1.2.bin
boot system rpm0 default flash:/FTOS-EF-6.5.1.8.bin
!
...
```

Command output example: **show running-config status**

```
FTOS#show running-config status

running-config checksum 0x84B9BF03
startup-config checksum 0x8803620F
FTOS#
```

---

**Usage Information**

The **status** option enables you to display the size and checksum of the running configuration and the startup configuration.
show sfm

View the current SFM status.

Syntax

```
show sfm [number [brief] | all]
```

Parameters

- `number`: Enter a number to view information on that SFM.
  Range: 0 to 8.
- `all` (OPTIONAL) Enter the keyword `all` to view a table with information on all present SFMs.
- `brief` (OPTIONAL) Enter the keyword `brief` to view a list with SFM status.

Note: The `brief` option is not available on C-Series.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command

E-Series Example

Command output example (Partial) on E-Series: `show sfm`

```
FTOS#show sfm
Switch Fabric State: up
   -- SFM card 0 --
      Status       : active
      Card Type    : SFM - Switch Fabric Module
      Up Time      : 37 min, 24 sec
      Temperature  : 49C
      Power Status : PEM0: absent or down    PEM1: up
      Serial Number: 0018102
      Part Number  : 7520012900 Rev 02
      Vendor Id    : 02
      Date Code    : 06182004
      Country Code : 01
```

show sfm Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Fabric State:</td>
<td>States that the Switch Fabric is up (8 SFMs are online and operating).</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the SFM's active status.</td>
</tr>
<tr>
<td>Card Type</td>
<td>States the type of SFM.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Displays the number of hours and minutes since the RPM's last reboot.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Displays the temperature of the RPM. Minor alarm status if temperature is over 65° C.</td>
</tr>
<tr>
<td>Power Status</td>
<td>Displays power status: absent, down, or up</td>
</tr>
<tr>
<td>Serial Num</td>
<td>Displays the line card serial number.</td>
</tr>
<tr>
<td>Part Num</td>
<td>Displays the line card part number.</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Displays an internal code, which specifies the manufacturing vendor.</td>
</tr>
</tbody>
</table>
show sfm Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Code</td>
<td>Displays the line card’s manufacturing date.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Displays the country of origin. 01 = USA</td>
</tr>
</tbody>
</table>

Command output example: `show sfm all`

```
FTOS#show sfm all
Switch Fabric State: up
  --  Switch Fabric Modules  --
  Slot  Status
  0   active
  1   active
  2   active
  3   active
  4   active
  5   active
  6   active
  7   active
  8   active
FTOS#
```

**show startup-config**

Display the startup configuration.

**Syntax**

```
show startup-config
```

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Expanded to include last configuration change and start-up last updated (date and time) and who made the change.</td>
</tr>
</tbody>
</table>

**Example**

Command output example (partial): `show startup-config`

```
FTOS#show startup-config

! Version 7.4.1.0
! Last configuration change at Thu Mar 29 02:16:07 2007 by default
! Startup-config last updated at Thu Mar 29 02:35:08 2007 by default
! boot system rpm0 primary flash://FTOS-EF-7.4.1.0.bin
boot system rpm0 secondary flash://FTOS-EF-6.3.1.2.bin
boot system rpm0 default flash://FTOS-EF-6.5.1.8.bin
!
```

**Related Commands**

- `show running-config` Display current (running) configuration.
show version

Display the current Dell Networking OS version information on the system.

Syntax

show version

Command Modes

EXEC Privilege

Command History

E-Series original Command

Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series

E-Series Example

Command output example on E-Series: show version

```
FTOS#show version
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: 5.3.1.0
Copyright (c) 1999-2004 by Force10 Networks, Inc.
Build Time: Sun May 9 00:57:03 PT 2004
Build Path: /local/local0/Release/5-4-1/SW/Bap/Diag
Force10 uptime is 1 days, 3 hours, 16 minutes
System image file is "/home/5.3.1/5.3.1.0/FTOS-ED-RPM1-5.3.1.0.bin"

Chassis Type: E1200
Control Processor: IBM PowerPC 405GP (Rev D) with 268435456 bytes of memory.
Route Processor 1: IBM PowerPC 405GP (Rev D) with 536870912 bytes of memory.
Route Processor 2: IBM PowerPC 405GP (Rev D) with 536870912 bytes of memory.
128K bytes of non-volatile configuration memory.

1 Route Processor Module
9 Switch Fabric Module
1 24-port GE line card with SFP optics (EE)
1 12-port GE Flex line card with SFP optics (EE)
1 2-port OC48c line card with SR optics (EC)
2 24-port GE line card with SX optics (EB)
1 2-port 10GE WAN PHY line card with 10Km (1310nm) optics (EE)
1 12-port GE Flex line card with SFP optics (EC)
1 2-port 10GE LAN PHY line card with 10Km (1310nm) optics (ED)
1 12-port OC12c/3c PoS line card with IR optics (EC)
1 24-port GE line card with SFP optics (ED)
1 1 FastEthernet/IEEE 802.3 interface(s)
120 GigabitEthernet/IEEE 802.3 interface(s)
14 SONET network interface(s)
4 Ten GigabitEthernet/IEEE 802.3 interface(s)
FTOS#
```

show version Command Fields

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

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis Type:</td>
<td>Chassis type (E1200, E600, E600i, E300, C7008/C300, C7004/C150)</td>
</tr>
<tr>
<td>Control Processor:...</td>
<td>Control processor information and amount of memory on processor.</td>
</tr>
<tr>
<td>Route Processor 1:...</td>
<td>E-Series route processor 1 information and the amount of memory on that processor.</td>
</tr>
<tr>
<td>Route Processor 2:...</td>
<td>E-Series route processor 2 information and the amount of memory on that processor.</td>
</tr>
<tr>
<td>128K bytes...</td>
<td>Amount and type of memory on system.</td>
</tr>
<tr>
<td>1 Route Processor...</td>
<td>Hardware configuration of the system, including the number and type of physical interfaces available.</td>
</tr>
</tbody>
</table>

S-Series Example

Command output example on an S50V: show version

FTOS#show version [[change Force10 to something else?]]
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: E7-8-1-13
Copyright (c) 1999-2008 by Force10 Networks, Inc.
Build Time: Mon Nov 24 18:59:27 2008
Build Path: /sites/sjc/work/sw/build/build2/Release/E7-8-1/SW/SRC
Force10 uptime is 1 minute(s)
System Type: S50V
Control Processor: MPC8451E with 252739584 bytes of memory.
32M bytes of boot flash memory.
1 48-port E/FE/GE with POE (SB)
48 GigabitEthernet/IEEE 802.3 interface(s)
4 Ten GigabitEthernet/IEEE 802.3 interface(s)
FTOS#

upgrade (E-Series version)

Upgrade the bootflash, boot selector, or system image on a processor.

Syntax

```
upgrade {bootflash-image | bootselector-image | system-image} {all | linecard [linecard-slot | rpm] {booted | file-url}}
```

Parameters

- **bootflash-image**: Enter the keyword `bootflash-image` to upgrade the bootflash image.
- **bootselector-image**: Enter the keyword `bootselector-image` to upgrade the boot selector image. Use with TAC supervision only.
- **system-image**: Enter the keyword `system-image` to upgrade the cache boot image.
- **all**: Enter the keyword `all` to upgrade the bootflash/boot selector image on all processors in the E-Series. This keyword does not upgrade the bootflash on the standby RPM.
- **linecard linecard-slot**: Enter the keyword `linecard` followed by the slot number to change the bootflash image on a specific line card.

E-Series Range: 0 to 13 on the E1200; 0 to 6 for the E600; 0 to 5 on the E300
Defaults
No configuration or default values

Command Modes
EXEC Privilege

Command History
Version 7.7.1.0 Removed alt-bootflash-image, alt-bootselector-image, alt-system-image options, rp1, rp2, and cp options.
E-Series original Command

Usage Information
A system message appears stating the Bootflash upgrade status. Reload the system to boot from the upgraded boot images.

Once the URL is specified, the same downloaded image can be used for upgrading an individual RPM, line cards, SFM FPGA, and system-image for cache-boot without specifying the file-url again using the command upgrade {bootflash-image | bootselector-image | system-image} {all | linecard linecard-slot | rpm}. After 20 minutes, the cached memory is released and returned for general use, but the URL is maintained and you do not have to specify it for subsequent upgrades.

Related Commands
upgrade fpga-image Upgrade the FPGA version in the specified E-Series SFM.
boot系统 Display configured boot image information

upgrade (C-Series version)
Upgrade the bootflash or boot selector image on a processor.

Syntax
upgrade {bootflash-image | bootselector-image | system-image} {all | linecard {number | all} | rpm} {booted | file-url | repair}

Parameters
bootflash-image Enter the keyword bootflash-image to upgrade the bootflash image.
bootselector-image Enter the keyword bootselector-image to upgrade the boot selector image. Use with TAC supervision only.
system-image Enter the keyword system-image to upgrade the system image. Use with TAC supervision only.
all Enter the keyword all to upgrade the bootflash or boot selector image on all processors. This keyword does not upgrade the bootflash on the standby RPM.

Enter the keyword all after the keyword linecard to upgrade the bootflash or boot selector image on all linecards.
Defaults
Dell Networking OS uses the boot flash image that was packed with it if no URL is specified.

Command Modes
EXEC Privilege

Command History
Version 7.7.1.0 Introduced system-image option
Version 7.5.1.0 Introduced on C-Series
E-Series original Command

Usage Information
A system message appears stating the Bootflash upgrade status. Reload the system to boot from the upgraded boot images.

Once the URL is specified, the same downloaded image can be used for upgrading an individual RPM, line cards, SFM FPGA, and system-image for cache-boot without specifying the file-url again using the command upgrade {bootflash-image | bootselector-image | system-image} {all | linecard linecard-slot | rpm}. After 20 minutes, the cached memory is released and returned for general use, but the URL is maintained and you do not have to specify it for subsequent upgrades.

Related Commands
upgrade fpga-image Upgrade the FPGA version in the specified E-Series SFM.
boot system Display configured boot image information
upgrade (S-Series management unit)

Upgrades the bootflash image or system image of the S-Series management unit.

Syntax

```
upgrade {boot | system} {ftp: | scp: | tftp:} file-url
```

Parameters

- `boot` Enter this keyword to change the boot image.
- `system` Enter this keyword to change the system image.
- `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.

Defaults

No configuration or default values

Command Modes

EXEC Privilege

Command History

- Version 7.7.1.0 Added support for TFTP and SCP.
- Version 7.6.1.0 Introduced on S-Series

Usage Information

You must reload Dell Networking OS after executing this command. Use the command `upgrade system stack-unit` (S-Series stack member) on page 242 to copy Dell Networking OS from the management unit to one or more stack members.

```
FTOS#upgrade system ?
ftp: Copy from remote file system (ftp://userid:password@hostip/filepath)
scp: Copy from remote file system (scp://userid:password@hostip/filepath)
tftp: Copy from remote file system (tftp://hostip/filepath)
```

Erasing Sseries ImageUpgrade Table of Contents, please wait

```

12946259 bytes successfully copied
```

FTOS#reload

upgrade fpga-image

This command only be used on systems with SFM3 modules (and only when required by the upgrade procedure in the release notes). Upgrade the FPGA version in the specified E-Series SFM3 and automatically initiate an automatic reset to complete the version upgrade.

Syntax

```
upgrade fpga-image {sfm} {all | id} [booted | flash:// | ftp: | slot0: | tftp]
```

FTOS#upgrade fpga-image sfm 0 ftp://userid:password@hostip/filepath
Parameters

| sfm     | Enter the keyword sfm to upgrade the FPGA on the SFMs. |
| rpm     | Enter the keyword rpm to upgrade all processors on the RPM. |
| all     | Enter the keyword all to upgrade the FPGA on all the SFMs. |
| id      | Enter the keyword id to upgrade the FPGA on all a specific SFM. |

Enter the path to the upgrade source. Entering <CR> updates the FPGA from the flash.

Defaults
No default values or behavior

Command Modes
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added rpm option</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added rpm option</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Example

Command example: **upgrade sfm autoreset**

FTOS#upgrade sfm 1 autoreset
SFM1: upgrade in progress
!!! !!! !!!
SFM1: upgrade complete
SFM1 is active. Resetting it might temporarily impact traffic.
Proceed with reset [confirm yes/no]: yes
FTOS#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sfm</td>
<td>Display the SFM status.</td>
</tr>
<tr>
<td>upgrade (E-Series version)</td>
<td>Upgrade the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

On E-Series ExaScale, you cannot upgrade SFMs using this command when Cache Boot is configured. If you attempt an upgrade, you must reload the chassis to recover.

**Upgrading the C-Series FPGA**

These commands are for upgrading the FPGA for C-Series RPMs and line cards.

- restore fpga-image
- upgrade fpga-image

**restore fpga-image**

Copy the backup C-Series FPGA image to the primary FPGA image.

**Syntax**

`restore fpga-image {rpm | linecard} number`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rpm</td>
<td>Enter rpm to upgrade an RPM FPGA.</td>
</tr>
<tr>
<td>linecard</td>
<td>Enter linecard to upgrade a line card FPGA.</td>
</tr>
<tr>
<td>number</td>
<td>Enter the line card or RPM slot number.</td>
</tr>
</tbody>
</table>

**C-Series** Line Card Range: 0-7, RPM Range: 0-1
### Defaults
None.

### Command Mode
EXEC Privilege

### Command History
<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Renamed keyword primary-fpga-flash to fpga-image.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

### Example
Command example: `restore fpga-image`

```
FTOS# restore fpga-image linecard 6
Current FPGA information in the system:
-------------------------------------------------------
Card     FPGA Name       Current Version   New Version
-------------------------------------------------------
LC6      48 Port 1G LCM POEPLUS FPGA     A: 0.1       restore

***********************************************************************
* Warning - Upgrading FPGA is inherently risky and should
* only be attempted when necessary. A failure at this upgrade may
* cause a board RMA. Please do not reset/powercycle or reload.
* Proceed with caution !
***********************************************************************

Restore fpga image for linecard 6 [yes/no]: y
FPGA restore in progress. Please do NOT power off the card.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upgrade result :
----------------
Linecard 6 FPGA restore successful.
FTOS#
```

### Usage Information
Reset the card using the **power-cycle** option after restoring the FPGA command.

### Related Commands
- `reset` - Reset a card.

### upgrade fpga-image
Upgrade the primary FPGA image.

#### Syntax
```
upgrade fpga-image {rpm {number | all} | linecard {number | all} | all} {booted | file-url}
```

#### Parameters
- `rpm number` - Enter rpm followed by the RPM slot number to upgrade an RPM FPGA
  - Range: 0-1
- `linecard number` - Enter linecard followed by the line card slot number to upgrade a
  - linecard FPGA.
  - Range: 0-7 on the C7008/C300, 0-3 on the C7004/C150
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enter the keyword <strong>all</strong> to upgrade all RPM and linecard FPGAs. Enter the keyword <strong>all</strong> after the keyword <strong>rpm</strong> to upgrade all FPGAs on all RPMs. Enter the keyword <strong>all</strong> after the keyword <strong>linecard</strong> to upgrade all FPGAs on all linecards.</td>
</tr>
<tr>
<td>system-fpga</td>
<td>(OPTIONAL) Enter <strong>system-fpga</strong> to upgrade only the system FPGA on a fiber linecard. Contact the Dell Networking TAC before using this keyword.</td>
</tr>
<tr>
<td>link-fpga</td>
<td>(OPTIONAL) Enter <strong>link-fpga</strong> to upgrade only the link FPGA on a fiber linecard. Contact the Dell Networking TAC before using this keyword.</td>
</tr>
<tr>
<td>booted</td>
<td>Upgrade the FPGA image using the currently running Dell Networking OS image.</td>
</tr>
<tr>
<td>file-url</td>
<td>Enter the following location keywords and information to upgrade the FPGA using an Dell Networking OS image other than the one currently running:</td>
</tr>
<tr>
<td></td>
<td>• To specify an Dell Networking OS image on the internal flash, enter <code>flash:// file-path/filename</code>.</td>
</tr>
<tr>
<td></td>
<td>• To specify an Dell Networking OS image on an FTP server, enter <code>ftp://user:password@hostip/filepath</code></td>
</tr>
<tr>
<td></td>
<td>• To specify an Dell Networking OS image on the external flash on the primary RPM, <code>slot0://file-path/filename</code></td>
</tr>
<tr>
<td></td>
<td>• To copy a file on a TFTP server, enter <code>tftp://hostip/filepath/filename</code></td>
</tr>
</tbody>
</table>

**Defaults**

None.

**Command Mode**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Renamed the <strong>primary-fpga-flash</strong> keyword to <strong>fpga-image</strong>. Added support for upgrading using a remote Dell Networking OS image.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for the <strong>all</strong> keyword</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>
Example Command example: **upgrade fpga-image**

FTOS# upgrade fpga-image linecard 6 booted

Current FPGA information in the system:

<table>
<thead>
<tr>
<th>Card</th>
<th>FPGA Name</th>
<th>Current Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>LC6</td>
<td>48 Port 1G LCM POEPLUS FPGA</td>
<td>A: 0.1</td>
<td>0.1</td>
</tr>
</tbody>
</table>

******************************************************************************
* Warning - Upgrading FPGA is inherently risky and should only be attempted when necessary. A failure at this upgrade may cause a board RMA. Please do not reset/powercycle or reload. *
* Proceed with caution !
******************************************************************************

Upgrade fpga image for linecard 6 [yes/no]: y

FPGA upgrade in progress. Please do NOT power off the card.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Upgrade result :
Linecard 6 FPGA upgrade successful.
FTOS#

Usage Information
Reset the card using the **power-cycle** option after restoring the FPGA command.

Related Commands
**reset**          Reset a line card or RPM.

**restore fpga-image**       This command copies the backup FPGA image to the primary FPGA image.

**upgrade poe-controller-firmware**

Upgrade the PoE controller on the line cards.

**Syntax**

**upgrade poe-controller-firmware linecard \{number\|all\} booted**

**Parameters**

<table>
<thead>
<tr>
<th><strong>linecard number</strong></th>
<th>Enter the keyword <strong>linecard</strong> followed by the line card slot number to upgrade the PoE controller. Range: 0-7 on the C7008/C300, 0-3 on the C7004/C150</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Enter the keyword <strong>all</strong> after the keyword <strong>linecard</strong> to upgrade all PoE controllers on all line cards.</td>
</tr>
<tr>
<td><strong>booted</strong></td>
<td>Upgrade the PoE controller using the currently running Dell Networking OS image.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Mode**

EXEC Privilege

**Command History**

Version 8.4.5.0    Introduced on C-Series
Example

Command example: **upgrade poe-controller-firmware**

```
FTOS#upgrade poe-controller-firmware linecard 6 booted

Current PoE-Controller information in the system:
-----------------------------------------------
Card Current Version New Version
-----------------------------------------------
LC6 2.39 2.39

**************************************************************************
* Warning - Upgrading PoE Controller should only be attempted     *
* when necessary. Linecard will be reset automatically after upgrade. *
* Please do not reset/powercycle or reload. Proceed with caution !    *
**************************************************************************

Upgrade PoE Controller image for linecard 6 [yes/no]: y

PoE Controller upgrade in progress. Please do NOT POWER-OFF the card.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upgrade result :
================
Linecard 6 PoE Controller upgrade successful. Resetting the linecard.
00:24:37: %RPM0-P:CP %CHMGR-5-CARD_RESET: line card 6 being reset
00:24:37: %RPM0-P:CP %IFMGR-1-DEL_PORT: Removed port: Gi 6/0-47
00:24:37: %RPM0-P:CP %CHMGR-2-CARD_DOWN: Line card 6 down - reset
FTOS#00:24:37: %RPM1-S:CP %IFMGR-1-DEL_PORT: Removed port: Gi 6/0-47
00:25:05: %RPM0-P:CP %CHMGR-5-CHECKIN: Checkin from line card 6 (type E48IB, 48 ports)
00:25:08: %RPM0-P:CP %CHMGR-5-LINECARDDUP: Line card 6 is up
FTOS#
```
BOOT_USER Mode

Overview

Most of the commands in this chapter are in Configuration mode, except for format, which is in the BOOT_ADMIN mode. The exception to this is that on the Dell Networking S50 platform. On the S50, the commands are accessed from the BOOT_USER mode. Command support on Dell Networking platforms is indicated by the characters that appear below each command heading:

- C = C-Series
- E = E-Series
- S = S-Series

To access the BOOT_USER mode, boot your Dell Networking platform. When the prompt, “Hit any key to break into BOOT_USER mode” appears, press a key.

Commands

- boot change
- boot messages
- boot selection
- boot zero
- default-gateway
- delete
- dir
- enable
- format
- ignore enable-password
- ignore startup-config
- interface management ethernet ip address
- interface management ethernet mac-address
- interface management ethernet port
- interface management port config
- reload
- rename
- restore factory-defaults
- save
- show boot selection
- show bootflash
- show bootvar
- show default-gateway
- show interface management ethernet

Note: You cannot use the Tab key to complete commands in this mode.

Note: The question mark (?) key to get help does not work in this mode. Instead, enter help.

**boot change**

Change the primary, secondary, or default Dell Networking OS boot configuration.

**Syntax**

```
boot change {primary | secondary | default}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Enter the keyword primary to configure the boot parameters used in the first attempt to boot Dell Networking OS.</td>
</tr>
<tr>
<td>secondary</td>
<td>Enter the keyword secondary to configure boot parameters used if the primary operating system boot selection is not available.</td>
</tr>
<tr>
<td>default</td>
<td>Enter the keyword default to configure boot parameters used if the secondary operating system boot parameter selection is not available. The default location should always be the internal flash device (flash:), and a verified image should be stored there.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

BOOT_USER

**Command History**

Version 7.8.1.0 Introduced on S-Series

**Usage Information**

After entering the `boot change` keywords and selecting among parameters, above, press Enter. The software prompts you to enter the following:

- The boot device (ftp, tftp, flash, slot0) (Note: tftp and flash are the only options available for the S-Series), image file name, IP address of the server containing the image, username and password (only for FTP)

Note: When you enter a new parameter that extends beyond 80 characters, you cannot use the Backspace key to correct any mistakes. If you make a mistake, you must re-enter the parameter.

Note: The IP address of the designated download port must be set before you execute this command. Otherwise, an error message will alert you that the configuration cannot proceed. See the command interface management ethernet ip address.

Figure 4-1 shows the first field after you enter `boot change primary`. At this point:

- Press Enter to accept the information already configured, or
- Change that information. To do so, press the . (period) key and enter new information. After you enter the information, press Enter.
Figure 4-1.  First Field in the boot change Command

BOOT_USER # boot change primary
'.' = clear field;  '=' = clear non-essential field

boot device : ftp

Figure 4-2 shows the completed command:

Figure 4-2.  Completed boot change Command Example

BOOT_USER # boot change primary
'. ' = clear field;  '-' = go to previous field

boot device : ftp
file name : tt/latestlabel
Server IP address : 10.16.1.209
username : amsterdam
password : *****

BOOT_USER #

In the runtime CLI of C-Series and E-Series, use the **boot system** command to change the boot image file and location.

To view the current boot configuration, use the **show bootvar** command.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>boot system</td>
<td>Set the location of Dell Networking OS image files.</td>
</tr>
<tr>
<td>boot zero</td>
<td>Remove the primary, secondary, or default boot image configuration.</td>
</tr>
<tr>
<td>show boot selection</td>
<td>Display the current Boot Flash image selected.</td>
</tr>
<tr>
<td>show bootvar</td>
<td>Display boot configuration information.</td>
</tr>
</tbody>
</table>

**boot messages**

Limit the number of messages seen during system boot-up.

**Syntax**

`boot messages {disable | enable}`

**Parameters**

- **disable**
  - Enter the keyword **disable** to display fewer messages during boot-up.
- **enable**
  - Enter the keyword **enable** to display all messages during boot-up.

**Defaults**

enable (that is, all messages are displayed during boot up)

**Command Modes**

BOOT_USER

**boot selection**

Specify the boot flash partition in the internal Flash from which to boot the system.

**Syntax**

`boot selection [a | b]`
Parameters

- **a**: Enter the keyword `a` to select the boot code in partition A.
- **b**: Enter the keyword `b` to select the boot code in partition B.

Defaults

None.

Command Modes

BOOT_USER

Usage Information

To view the current boot flash image, enter the `show boot selection` command.

Related Commands

- **boot change**: Change the primary, secondary or default boot image configuration
- **show boot selection**: Display the current Boot Flash image selected.

### boot zero

Erase the configured primary, secondary, or default boot image parameters. If all three parameters are erased, the S-Series switch will boot from its internal Flash.

**Syntax**

```
boot zero {primary | secondary | default}
```

**Parameters**

- **primary**: Enter the keyword `primary` to configure the boot parameters used in the first attempt to boot the system.
- **secondary**: Enter the keyword `secondary` to configure boot parameters used if the primary operating system boot selection is not available.
- **default**: Enter the keyword `default` to configure boot parameters used if the secondary operating system boot parameter selection is not available. The default parameters always reside on the internal flash device (flash:).

Defaults

Not configured.

Command Modes

BOOT_USER

Command History

- **Version 7.8.1.0**: Introduced on S-Series

Usage Information

This command reverses changes made with the `boot change` command.
**Figure 4-3. Completed boot zero Command Example**

```plaintext
BOOT_USER # boot zero primary
BOOT_USER # boot zero secondary
BOOT_USER # boot zero default
BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
No Operating System boot parameters specified!

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
No Operating System boot parameters specified!

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
No Operating System boot parameters specified!

BOOT_USER #
```

### default-gateway

Assign an IP address as the default gateway for the system.

**Syntax**

```
[no] default-gateway ip-address
```

**Parameters**

- `ip-address`: Enter the IP address of the gateway router in dotted decimal format (A.B.C.D).

**Defaults**

Not configured.

**Command Modes**

BOOT_USER

**Command History**

Version 7.8.1.0 Introduced on S-Series

**Usage Information**

Use the `show default-gateway` command to view the current default gateway.

**Related Commands**

- `show default-gateway`: Change the primary, secondary or default boot image configuration
- `show boot selection`: Display the current Boot Flash image selected.

### delete

Erase a file on the internal or external Flash.

**Syntax**

```
delete file-url
```

**Parameters**

- `file-url`: Enter the location keywords and information:
  - For a file on the internal Flash, enter `flash://` followed by the filename.
  - For a file on the external Flash, enter `slot0://` followed by the filename.
**dir**

Display files in a directory

**Syntax**

```
dir file-url
```

**Parameters**

- **file-url**: Enter the location keywords and information:
  - For a file on the internal Flash, enter `flash://` followed by the filename.
  - For a file on the external Flash, enter `slot0://` followed by the filename.

**Defaults**
Not configured.

**Command Modes**
BOOT_USER

**Usage Information**

The maximum number of files allowed on an MMC card (internal or external flash) is 100 files.

**Example**

Figure 4-4. dir Command Example

```plaintext
BOOT_USER # dir flash:
Displaying files in flash:
        size          date       time       name          
-------------------------- ------ ------- ------ ------------ 
  8681647    MAR-21-2004  11:08:50   E1200-3.1.a3.78.bin
   4905     MAR-17-2004  18:16:34     nimule
 1182431    FEB-29-2004  22:08:14     dohuk
  8007825  MAR-30-2004  12:49:14   E1200-3.1.0.309.bin
 1182431    FEB-24-2004  22:52:00     t1
  14729    MAR-14-2004  17:55:26     erbil
  1182431   MAR-10-2004  10:57:30     vW
   6858    MAR-07-2004  09:52:58        RPM0CP1
 1182431   MAR-22-2004  12:17:34        tunis
  781238    MAR-22-2004  12:23:14   E1200-3.1.0.316.bin
  8989646    MAR-17-2004  15:13:06   E1200-3.1.0.390.bin.dos2
  14517   MAR-30-2004  09:48:44    RPM0CPlog1
  14506   MAR-30-2004  09:49:34    RPM0CPlog2

BOOT_USER #
```
Usage Information

Only Dell Networking TAC staff use this command.

format

Format the internal or external flash memory.

Syntax

format file-url

Parameters

- **file-url**: Enter the location keywords and information:
  - For a file on the internal Flash, enter `flash://` followed by the filename.
  - For a file on the external Flash, enter `slot0://` followed by the filename.

Defaults

Not configured.

Command Modes

BOOT_ADMIN

Usage Information

The maximum number of files allowed on an MMC card (internal or external flash) is 100 files.

Related Commands

- **format (C-Series and E-Series)**: Erase all existing files and reformat a filesystem (EXEC Privilege mode).
- **show file**: Display contents of a text file in the local filesystem.
- **show file-systems**: Display information about the file systems on the system.

ignore enable-password

Reload the system software without the enable password configured. This command is hidden on the C-Series and E-Series, so it is not listed when you enter ? or help in this mode.

Syntax

ignore enable-password

Defaults

Not configured.

Command Modes

BOOT_USER

Command History

- Version 7.8.1.0: Introduced on S-Series

Usage Information

When you enter the **reload** command and the system reboots, you will not be prompted for a password to enter the EXEC Privilege mode (normally you are required to enter the enable command.)

If your console or Telnet session expires after you used the **ignore enable-password** command, you are prompted for an **enable** password when you re-establish the session.

Related Commands

- **reload**: Exit from this mode and reload Dell Networking OS.
- **show running-config**: Display the current configuration and the changes from the default values.
ignore startup-config

During a reload, do not load the startup-config file.

Syntax

ignore startup-config

Defaults

disabled

Command Modes

BOOT_USER

Command History

Version 7.8.1.0 Introduced on S-Series

Usage Information

This command might be used if a the user has authentication procedures in the startup-config other than the enable-password setting.

interface management ethernet ip address

Assign an IP address to the Management Ethernet interface.

Syntax

[no] interface management ethernet ip address ip-address mask

To delete the IP address on the C-Series and E-Series (not on S-Series), enter no interface management ethernet ip address.

Parameters

- **ip-address mask**: Enter the IP address in dotted decimal format (A.B.C.D) and the mask in /prefix-length format (/x).

Defaults

Not configured.

Command Modes

BOOT_USER

Command History

Version 7.8.1.0 Introduced on S-Series

Usage Information

In the runtime CLI of the C-Series and E-Series (not on S-Series), use the ip address command in the INTERFACE mode to change the Management interface’s IP address.

If there is a mac address programmed in the eeprom, the show interface management ethernet command gets the mac address from there and displays it. If there is no mac address programmed, the following is used by default - 00:10:18:00:00:01.

To view the current IP address configured on the Management interface, enter the show interfaces management ethernet command.

Related Commands

- **ip address**: Assign a primary and secondary IP address to the interface.
- **show default-gateway**: Display the IP address configured for the default gateway.
- **show interface management ethernet**: Display the IP address configured for the Management interface.
interface management ethernet mac-address

Syntax:  
interface management ethernet mac-address mac-address

Parameters:  

Defaults:  
Not configured.

Command Modes:  
BOOT_USER

Command History:  
Version 7.8.1.0 Introduced on S-Series

Usage Information:  
Use this command to assign a MAC address if Dell Networking OS cannot find a default MAC address.

Related Commands:  
show default-gateway Display the IP address configured for the default gateway.
show interface management ethernet Display the IP address configured for the Management interface.

interface management ethernet port

Syntax:  
interface management ethernet port portID

Parameters:  
portID: Enter an S-Series port ID as an integer.  
Range: 1 to 48

Defaults:  
Not configured.

Command Modes:  
BOOT_USER

Command History:  
Version 7.8.1.0 Introduced on S-Series

Usage Information:  
Assign any copper port to be the Management Ethernet interface.

Related Commands:  
show interface management ethernet Display the IP address configured for the Management interface.

interface management port config

Syntax:  
interface management port config {half-duplex | full-duplex | 10m | 100m | auto-negotiation | no auto-negotiation | show}

Configure speed, duplex, and negotiation settings for the management interface.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>half-duplex</td>
<td>Enter the keyword <strong>half-duplex</strong> to set the Management interface to half-duplex mode.</td>
</tr>
<tr>
<td>full-duplex</td>
<td>Enter the keyword <strong>full-duplex</strong> to set the Management interface to full-duplex mode.</td>
</tr>
<tr>
<td>10m</td>
<td>Enter the keyword <strong>10m</strong> to set the speed on the Management interface to 10 Mb/s.</td>
</tr>
<tr>
<td>100m</td>
<td>Enter the keyword <strong>100m</strong> to set the speed of the Management interface to 100 Mb/s.</td>
</tr>
<tr>
<td>auto-negotiation</td>
<td>Enter the keyword <strong>auto-negotiation</strong> to enable negotiation on the Management interface.</td>
</tr>
<tr>
<td>no auto-negotiation</td>
<td>Enter the keyword <strong>no auto-negotiation</strong> to disable auto-negotiation on the Management interface.</td>
</tr>
<tr>
<td>show</td>
<td>Enter the keyword <strong>show</strong> to display the settings on the Management interface.</td>
</tr>
</tbody>
</table>

### Defaults

- full duplex; auto-negotiation

### Command Modes

- **BOOT_USER**

### Usage Information

This command is only available in Boot Flash version 2.0.0.21 and higher.

### Related Commands

- **show default-gateway** Display the IP address configured for the default gateway.
- **show interface management ethernet** Display the IP address configured for the Management interface.

### reload

**Syntax**

```
reload
```

**Command Modes**

- **BOOT_USER**

**Command History**

- **Version 7.8.1.0** Introduced on S-Series

**Related Commands**

- **save** Save configurations created in BOOT_USER mode (BLI).

### rename

**Syntax**

```
rename file-url
```

**Description**

Rename a file.
Parameters

file-url

Enter the location keywords and information:

- For a file on the internal Flash, enter flash:// followed by the filename.
- For a file on the external Flash, enter slot0:// followed by the filename.

Defaults

None.

Command Modes

BOOT_USER

restore factory-defaults

Erase all NVRAM sectors, EEPROM sectors, and user boot configurations.

Syntax

restore factory-defaults

Command Modes

BOOT_USER

Command History

Version 7.8.1.0 Introduced on S-Series

save

Save configurations created in BOOT_USER mode (BLI).

Command History

Version 7.8.1.0 Introduced on S-Series

Usage Information

A basic difference between S-Series and other Dell Networking platforms is that, on the S-Series, Dell Networking OS does not save configurations into NVRAM while the user enters them in the BLI. Instead, the configurations are saved in a software cache and are written into NVRAM only on the execution of this save command or of the reload command.

Related Commands

reload  Exit from this mode and reload Dell Networking OS.

write  Save the running configuration to the startup configuration file.

show boot selection

Display the current Dell Networking OS boot image.

Syntax

show boot selection

Command Modes

BOOT_USER
Example

Figure 4-5. show boot selection Command Example

BOOT_USER # show boot selection

ROM BOOTSTRAP SELECTOR PARAMETERS:
---------------------------------------
Current ROM bootstrap selection set to Bootflash partition B.
Last ROM bootstrap occurred from Bootflash partition B.

BOOT_USER #

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot change</td>
<td>Change the primary, secondary or default boot image configuration</td>
</tr>
<tr>
<td>boot selection</td>
<td>Change the boot flash image on the internal Flash.</td>
</tr>
</tbody>
</table>

show bootflash

Syntax: show bootflash

Display information on the boot flash.

Command Modes: BOOT_USER

Example

Figure 4-6. show bootflash Command Example

BOOT_USER # show bootflash

GENERAL BOOTFLASH INFO
----------------------------
Bootflash Partition A:
Force10 Networks System Boot
Copyright 1999-2004 Force10 Networks, Inc.
ROM Header Version 1.0
Engineering CP_IMG_BOOT, BSP Release 2.0.0.19, Checksum 0x39303030
Created Mon Mar 20 10:56:53 US/Pacific 2004 by xxx on Unknown host

Bootflash Partition B:
Force10 Networks System Boot
Copyright 1999-2004 Force10 Networks, Inc.
ROM Header Version 1.0
Engineering CP_IMG_BOOT, BSP Release 2.0.0.19, Checksum 0x36313031
Created Mon Mar 6 18:15:10 2004 by xxx on hostname

Boot Selector Partition:
Force10 Networks System Boot
Copyright 1999-2004 Force10 Networks, Inc.
ROM Header Version 1.0
Official CP_IMG_BOOT_SELECTOR, BSP Release 2.0.0.15, Checksum 0x30314348
Created Mon Jan 21 17:15:47 US/Pacific 2004 by xxx on Unknown host

BOOT_USER #

show bootvar

Syntax: show bootvar

Display boot configuration information.

Command Modes: BOOT_USER
Figure 4-7. show bootvar Command Example

```
BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
--------------------------------------------
boot device : ftp
file name : tt/latestlabel
Management Ethernet IP address : 10.16.1.181/24
username : amsterdam
password : ******

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
----------------------------------------------
boot device : flash
file name : /E1200-3.1.1.3.bin

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
--------------------------------------------
boot device : flash
file name : /E1200-3.1.1.2.bin

BOOT_USER #
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot change</td>
<td>Change the primary, secondary or default boot image configuration.</td>
</tr>
<tr>
<td>boot zero</td>
<td>Erase the configured primary, secondary, or default boot image parameters.</td>
</tr>
</tbody>
</table>

show default-gateway

Display the IP address configured for the default gateway.

Syntax

```
show default-gateway
```

Command Mode

BOOT_USER

Example

Figure 4-8. show default-gateway Command Example

```
BOOT_USER # show default-gateway
Gateway IP address: 10.1.1.1
BOOT_USER #
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-gateway</td>
<td>Configure the IP address for the default gateway.</td>
</tr>
<tr>
<td>interface management ethernet ip address</td>
<td>Assign an IP address to the Management Ethernet interface.</td>
</tr>
</tbody>
</table>
show interface management ethernet

declare that the IP address configured for the Management interface.

Syntax
show interface management ethernet

Command Modes
BOOT_USER

Command History
Version 7.8.1.0 Introduced on S-Series

Example
Figure 4-9. show interface management ethernet Command Example

BOOT_USER # show interfaces management ethernet
Management ethernet IP address: 10.16.1.181/24
BOOT_USER #

On the S-Series, the output of this command includes the MAC address and port number of the assigned management port.

Example
Figure 4-10. show interface management ethernet Command Example

BOOT_USER # show interface management ethernet
Management ethernet IP address: 10.16.1.181/24
Management ethernet MAC address: 00:01:e8:43:13:16
Management ethernet port number: 1
BOOT_USER #

Related Commands
interface management ethernet ip address Assign an IP address to the Management Ethernet interface.

interface management port config Configure speed, duplex, and negotiation settings for the management interface.
Control and Monitoring

Overview

This chapter contains the following commands to configure and monitor the system, including Telnet, FTP, and TFTP as they apply to platforms C E S.

Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audible cut-off</td>
<td>send</td>
</tr>
<tr>
<td>banner exec</td>
<td>service timestamps</td>
</tr>
<tr>
<td>banner login</td>
<td>show alarms</td>
</tr>
<tr>
<td>banner motd</td>
<td>show chassis</td>
</tr>
<tr>
<td>cam-audit linecard</td>
<td>show command-history</td>
</tr>
<tr>
<td>clear alarms</td>
<td>show command-tree</td>
</tr>
<tr>
<td>clear command history</td>
<td>show console lp</td>
</tr>
<tr>
<td>clear line</td>
<td>show cpu-traffic-stats</td>
</tr>
<tr>
<td>configure</td>
<td>show debugging</td>
</tr>
<tr>
<td>debug cpu-traffic-stats</td>
<td>show environment (C-Series and E-Series)</td>
</tr>
<tr>
<td>debug ftpserver</td>
<td>show environment (S-Series)</td>
</tr>
<tr>
<td>disable</td>
<td>show inventory (C-Series and E-Series)</td>
</tr>
<tr>
<td>do</td>
<td>show inventory (S-Series)</td>
</tr>
<tr>
<td>enable</td>
<td>show linecard</td>
</tr>
<tr>
<td>enable xfp-power-updates</td>
<td>show linecard boot-information</td>
</tr>
<tr>
<td>end</td>
<td>show memory (C-Series and E-Series)</td>
</tr>
<tr>
<td>epoch</td>
<td>show memory (S-Series)</td>
</tr>
<tr>
<td>exec-banner</td>
<td>show processes cpu (C-Series and E-Series)</td>
</tr>
<tr>
<td>exec-timeout</td>
<td>show processes cpu (S-Series)</td>
</tr>
<tr>
<td>exit</td>
<td>show processes ipc flow-control</td>
</tr>
<tr>
<td>ftp-server tomdir</td>
<td>show processes memory (C-Series and E-Series)</td>
</tr>
<tr>
<td>ftp-server username</td>
<td>show processes memory (S-Series)</td>
</tr>
<tr>
<td>hostname</td>
<td>show rpm</td>
</tr>
<tr>
<td>ip ftp password</td>
<td>show software ifm</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip ftp source-interface</td>
<td>show switch links</td>
</tr>
<tr>
<td>ip ftp username</td>
<td>show system (S-Series)</td>
</tr>
<tr>
<td>ip telnet server enable</td>
<td>show tech-support (C-Series and E-Series)</td>
</tr>
<tr>
<td>ip telnet source-interface</td>
<td>show tech-support (S-Series)</td>
</tr>
<tr>
<td>ip tftp source-interface</td>
<td>ssh-peer-rpm</td>
</tr>
<tr>
<td>line</td>
<td>telnet</td>
</tr>
<tr>
<td>linecard</td>
<td>telnet-peer-rpm</td>
</tr>
<tr>
<td>module power-off</td>
<td>terminal length</td>
</tr>
<tr>
<td>motd-banner</td>
<td>terminal xml</td>
</tr>
<tr>
<td>ping</td>
<td>traceroute</td>
</tr>
<tr>
<td>power-off</td>
<td>undeflag all</td>
</tr>
<tr>
<td>power-on</td>
<td>upload trace-log</td>
</tr>
<tr>
<td>reload</td>
<td>virtual-ip</td>
</tr>
<tr>
<td>reset</td>
<td>write</td>
</tr>
<tr>
<td>rpm &lt;slot&gt; location-led</td>
<td>show tech-support(Series)</td>
</tr>
</tbody>
</table>

### audible cut-off

**E**

Turn off an audible alarm.

**Syntax**

```
audible cut-off
```

**Defaults**

Not configured.

**Command Modes**

EXEC Privilege

### banner exec

**C E S**

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

**Syntax**

```
banner exec c line c
```

**Parameters**

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

**Defaults**

No banner is displayed.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
</tbody>
</table>
### Usage Information

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

### Example

```
FTOS(config)#banner exec?
LINE c banner-text c where 'c' is a delimiting character
FTOS(config)#banner exec %
Enter TEXT message. End with the character '%'.
This is the banner%
FTOS(config)#end
FTOS#exit
4d21h5m: %RPM0-P:CP %SEC-5-LOGOUT: Exec session is terminated for user on line
console
This is the banner
Dell Networking OS con0 now available
Press RETURN to get started.
4d21h6m: %RPM0-P:CP %SEC-5-LOGIN_SUCCESS: Login successful for user on line
console
This is the banner
FTOS>
```

### Related Commands

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

### `banner login`

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

#### Syntax

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

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyboard-interactive</td>
<td>Enter this keyword to require a carriage return (CR) to get the message banner prompt.</td>
</tr>
<tr>
<td>c</td>
<td>Enter a delineator character to specify the limits of the text banner. In Figure 5-1, the % character is the delineator character.</td>
</tr>
</tbody>
</table>
| line                 | Enter a text string for your text banner message ending the message with your delineator. In the example in Figure 5-1, 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`
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.

### Related Commands

- **banner exec**
  Sets a banner to be displayed when you enter EXEC Privilege mode.

- **banner motd**
  Sets a Message of the Day banner.

### Example

**Figure 5-1. Command Example: banner login**

```
FTOS(conf)#banner login
keyboard-interactive Press enter key to get prompt
LINE  c banner-text c, where 'c' is a delimiting character
FTOS(conf)#no banner login
keyboard-interactive Prompt will be displayed by default
<cr>
FTOS(conf)#banner login keyboard-interactive
Enter TEXT message. End with the character '%'.
This is the banner%
FTOS(conf)#end
FTOS#exit

13d21h9m: %RPM0-P:CP %SEC-5-LOGOUT: Exec session is terminated for user on line console
This is the banner
Dell Networking OS con0 now available
Press RETURN to get started.
13d21h10m: %RPM0-P:CP %SEC-5-LOGIN_SUCCESS: Login successful for user on line console
This is the banner
FTOS>
```

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

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

---

### cam-audit linecard

**Syntax**

```
cam-audit linecard all ipv4-fib interval time-in-minutes
```

**Parameters**

- **`all`**
  Enter the keyword `all` to enable CAM audit on all line cards.
- **`ipv4-fib`**
  Enter the keyword `ipv4-fib` to designate the CAM audit on the IPv4 forwarding entries.
- **`interval time-in-minutes`**
  Enter the keyword `interval` followed by the frequency in minutes of the CAM audit.
  Range: 5 to 1440 minutes (24 hours)
  Default: 60 minutes

---

### clear alarms

**Syntax**

```
clear alarms
```

**Command Modes**

- EXEC Privilege

---

Enables periodic audits of software and hardware copies of the IPv4 forwarding table.
clear command history

Clear the command history log.

Syntax

`clear command history`

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series original Command</td>
</tr>
</tbody>
</table>

Related Commands

`show command-history` Display 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 | aux 0 | console 0 | vty number}`

Parameters

`line-number` Enter a number for one of the 12 terminal lines on the system.

Range: 0 to 11.

`aux 0` Enter the keywords `aux 0` to reset the Auxiliary port.

Note: This option is supported on E-Series only.

`console 0` Enter the keyword `console 0` to reset the Console port.

`vty number` Enter the keyword vty followed by a number to clear a Terminal line.

Range: 0 to 9

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series original Command</td>
</tr>
</tbody>
</table>
configure

Enter the CONFIGURATION mode from the EXEC Privilege mode.

Syntax

configure [terminal]

Parameters

terminal (OPTIONAL) Enter the keyword terminal to specify that you are configuring from the terminal.

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

Example

Figure 5-2. Command Example: configure

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

**disable**

Return to the EXEC mode.

**Syntax**

```
disable [level]
```

**Parameters**

- **level** (OPTIONAL) Enter a number for a privilege level of the Dell Networking OS.
  - Range: 0 to 15.
  - Default: 1

**Defaults**

1

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

**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**

No default behavior

**Command Modes**

CONFIGURATION

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

- enable
- disable
- exit
- config

### Example

**Figure 5-3. Command Example: do**

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

### enable

**Syntax**

```
enable [level]
```

**Parameters**

- `level` *(OPTIONAL)* Enter a number for a privilege level of Dell Networking OS.
  
  Range: 0 to 15.

**Defaults**

- `15`

**Command Modes**

- EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Users entering the 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** — Configure a password for the enable command and to access a privilege level.
enable xfp-power-updates

Enable XFP power updates for SNMP.

**Syntax**

```
enable xfp-power-updates interval seconds
```

To disable XFP power updates, use the **no enable xfp-power-updates** command.

**Parameters**

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

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The chassis MIB contain the entry chSysXfpRecvPower in the chSysPortTable table. Periodically, IFA polls the XFP power for each of the ports, and sends the values to IFM where it is cached. The default interval for the polling is 300 seconds (5 minutes). Use this command to enable the polling and to configure the polling frequency.

**end**

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

**Syntax**

```
end
```

**Command Modes**

CONFIGURATION, SPANNING TREE, MULTIPLE SPANNING TREE, LINE, INTERFACE, TRACE-LIST, VRRP, ACCESS-LIST, PREFIX-LIST, AS-PATH ACL, COMMUNITY-LIST, ROUTER OSPF, ROUTER RIP, ROUTER ISIS, ROUTER BGP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Return to the lower command mode.</td>
</tr>
</tbody>
</table>
## epoch

Set the epoch scheduling time for the chassis.

### Syntax

```
epoch \{2.4 | 3.2 | 10.4\}
```

### Parameters

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>2.4</code></td>
<td>Enter the keyword <code>2.4</code> to set the epoch to 2.4 micro-seconds and lower the latency. This option is available on the E600i and E1200i E-Series ExaScale systems only.</td>
</tr>
<tr>
<td><code>3.2</code></td>
<td>Enter the keyword <code>3.2</code> to set the epoch to 3.2 micro-seconds and lower the latency. This option is available on the E600/E600i and E1200/E1200i only. ExaScale does not support this setting with Dell Networking OS 8.3.1.0 and later.</td>
</tr>
<tr>
<td><code>10.4</code></td>
<td>Enter the keyword <code>10.4</code> to set the epoch to 10.4 micro-seconds. This is the default setting and is available on the E300, E600/E600i, and E1200.</td>
</tr>
</tbody>
</table>

### Defaults

```
10.4
```

### Command Modes

```
CONFIGURATION
```

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added 2.4 micro-seconds option. ExaScale supports only 10.4 micro-seconds and 2.4 micro-seconds with Dell Networking OS 8.3.1.0 and later.</td>
</tr>
<tr>
<td>8.1.1.2</td>
<td>Introduced on E-Series ExaScale E600i</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale E1200i</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Support for E300 introduced (10.4 only)</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Values changed as described above</td>
</tr>
</tbody>
</table>

### Usage Information

You save the configuration and reload the chassis for the changes to the `epoch` command setting to take affect.

When using 10 SFMs in an ExaScale chassis, the 10.4 and 2.4 settings are both line rate. Additionally, the 2.4 setting has a lower latency.

When using 9 SFMs in an ExaScale chassis, the 10.4 setting is line rate; the 2.4 setting reduces throughput. Dell Networking recommends using the 10.4 setting when the system has 9 SFMs.

Using 8 SFMs in an ExaScale chassis reduces throughput at any epoch setting.

**Note:** The E300 supports only the 10.4 epoch setting. The E-Series TeraScale E600/E600i and the E1200/E1200i systems support the 10.4 and the 3.2 epoch settings.

**Note:** For E-Series ExaScale, the 2.4 setting is supported on Dell Networking OS version 8.3.1.0 and later. The 10.4 setting is supported on all ExaScale Dell Networking OS versions. The 3.2 setting is only supported on Dell Networking OS versions 8.2.1.0 and earlier.
exec-banner

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

Syntax

exec-banner

Defaults

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

Command Modes

LINE

Command History

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- E-Series original Command

Usage

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

Related Commands

- `banner exec` Configure a banner to display when entering the EXEC mode.
- `line` Enable and configure console and virtual terminal lines to the system.

exec-timeout

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

Syntax

exec-timeout minutes [seconds]

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

Parameters

- `minutes` Enter the number of minutes of inactivity on the system before disconnecting the current session.
  - Range: 0 to 35791
  - Default: 10 minutes for console line; 30 minutes for VTY line.
  - (OPTIONAL) Enter the number of seconds
  - Range: 0 to 2147483
  - Default: 0 seconds

Defaults

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

Command Modes

LINE

Command History

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- E-Series original Command

Usage

To remove the time interval, enter `exec-timeout 0 0`. 
Figure 5-4. Dell Networking OS time-out display

Dell Networking OS 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, TRACE-LIST, PROTOCOL GVRP, SPANNING TREE, MULTIPLE SPANNING TREE, MAC ACCESS LIST, ACCESS-LIST, AS-PATH ACL, COMMUNITY-LIST, PREFIX-LIST, ROUTER OSPF, ROUTER RIP, ROUTER ISIS, ROUTER BGP

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>E-Series original Command</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

end Return to the EXEC Privilege command mode.

ftp-server enable

Enable FTP server functions on the system.

Syntax ftp-server enable

Defaults Disabled.

Command Modes CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>E-Series original Command</td>
<td></td>
</tr>
</tbody>
</table>
Example

Figure 5-5. Example of Logging on to an FTP Server

```
morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 Dell Networking OS (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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ftp-server topdir</code></td>
<td>Set the directory to be used for incoming FTP connections to the E-Series.</td>
</tr>
<tr>
<td><code>ftp-server username</code></td>
<td>Set a username and password for incoming FTP connections to the E-Series.</td>
</tr>
</tbody>
</table>

```
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

**Command History**

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series

**Usage Information**

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

**Related Commands**

- `ftp-server username` Set a username and password for incoming FTP connections to the E-Series.
**ftp-server username**

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

**Syntax**

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

**Parameters**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>E-Series original Command</td>
<td></td>
</tr>
</tbody>
</table>

**hostname**

Set the host name of the system.

**Syntax**

```
hostname name
```

**Parameters**

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

**Defaults**

FTOS

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>E-Series original Command</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

**Usage Information**

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

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

**Related Commands**

- `copy` Copy files.
- `ip ftp username` Set the user name for 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 an 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port 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:
    - **C-Series and S-Series**: 1-128
    - **E-Series**: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale
  - For SONET interface types, enter the keyword `sonet` followed by the slot/port information.
  - 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.

**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 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.2.1.0** Increased number of VLANs on ExaScale to 4094 (was 2094)
- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Support added for S-Series
- **Version 7.5.1.0** Introduced on C-Series

**Related Commands**

- `copy` Copy 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series original Command</td>
</tr>
</tbody>
</table>

**Usage Information**

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

**Related Commands**

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

---

**ip telnet server enable**

Enable the Telnet server on the switch.

**Syntax**

```
ip telnet server enable
```

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

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ip ssh server` Enable 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**

<table>
<thead>
<tr>
<th><strong>interface</strong></th>
<th>Enter the following keywords and slot/port or number information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For an 100/1000 Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For Loopback interfaces, enter the keyword <code>loopback</code> followed by a number from zero (0) to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For the SONET interfaces, enter the keyword <code>sonet</code> followed by slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>C-Series and S-Series: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale</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 VLAN interface, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Defaults**

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

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Increased number of VLANs on ExaScale to 4094 (was 2094)</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

telnet  Telnet 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 an 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port 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:
      - **C-Series** and **S-Series**: 1-128
      - **E-Series**: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale
    - For the SONET interfaces, enter the keyword `sonet` followed by 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.
    - 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8.4.6.0    | Added support for the keyword `fortyGigE`.
| 8.2.1.0    | Increased number of VLANs on ExaScale to 4094 (was 2094) |
| 8.1.1.0    | Introduced on E-Series ExaScale       |
| 7.6.1.0    | Support added for S-Series            |
| 7.5.1.0    | Introduced on C-Series                |

E-Series original Command

line

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

Syntax

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

Parameters

- **aux 0**
  - Enter the keyword `aux 0` to configure the auxiliary terminal connection.
  - **Note:** This option is supported on E-Series only.

- **console 0**
  - Enter the keyword `console 0` to configure the console port.
  - The console option for the S-Series 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**Usage Information**
You cannot delete a terminal connection.

**Related Commands**
- *access-class* Restrict incoming connections to a particular IP address in an IP access control list (ACL).
- *password* Specify a password for users on terminal lines.
- *show linecard* Display the line card(s) status.

### linecard

Pre-configure a line card in a currently empty slot of the system or a different line card type for the slot.

**Syntax**

```
linecard number card-type
```

**Parameters**

- *number* Enter the number of the slot.
  - **C-Series** Range: 0-7
  - **E-Series** Range: 0 to 13 on a E1200/E1200i, 0 to 6 on a E600/E6001, and 0 to 5 on a E300.

- *card-type* Enter the line card ID (see the Supported Hardware section in the Release Notes).

**Defaults**
Not configured

**Command Modes**
CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.2</td>
<td>Introduced on E-Series ExaScale E600i</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale E1200i</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command
Figure 5-6. Command Example: show linecard on C-Series

FTOS#show linecard 0
-- Line card 0 --
Status : online
Next Boot : online
Required Type : E48VB - 48-port GE 10/100/1000Base-T line card with RJ45 interfaces and PoE (CB)
Current Type : E48VB - 48-port GE 10/100/1000Base-T line card with RJ45 interfaces and PoE (CB)
Hardware Rev : 2.0
Num Ports : 48
Up Time : 1 min, 56 sec
Dell Networking OS Version : 8-4-2-399
Jumbo Capable : yes
POE Capable : yes
Boot Flash : A: 1.0.0.40 B: 2.6.0.2 [booted]
FPGA Flash : A: 3.2
Memory Size : 268435456 bytes
Temperature : 39C
Power Status : AC
Voltage : ok
Serial Number : FX000008104
Part Number : 7520029400 Rev 03
Vendor Id : 04
Date Code : 01082007
Country Code : 01
Piece Part ID : US-0YK2JY-76991-1BA-8104
PPID Revision : 002
Service Tag : SRVCTG2
Expr Svc Code : 626 351 582 90
Auto Reboot : enabled
FTOS#

Usage Information
Use this command only for empty slots or a slot where you have hot-swapped a different line card type. Before inserting a card of a different type into the pre-configured slot, execute the no linecard number command. The following screenshot shows the current supported C-Series line cards, along with their “card types” (card-type IDs).
Figure 5-7. Command Example: show linecard on E-Series

FTOS#show linecard 0
-- Line card 0 --
Status : online
Next Boot : online
Required Type : E48VB - 48-port GE 10/100/1000Base-T line card with RJ45 interfaces and PoE (CB)
Current Type : E48VB - 48-port GE 10/100/1000Base-T line card with RJ45 interfaces and PoE (CB)
Hardware Rev : 2.0
Num Ports : 48
Up Time : 1 min, 56 sec
Dell Networking OS Version : 8-4-2-399
Jumbo Capable : yes
POE Capable : yes
Boot Flash : A: 1.0.0.40 B: 2.6.0.2 [booted]
FPGA Flash : A: 3.2
Memory Size : 268435456 bytes
Temperature : 39C
Power Status : AC
Voltage : ok
Serial Number : FX000008104
Part Number : 7520029400 Rev 03
Vendor Id : 04
Date Code : 01082007
Country Code : 01
Piece Part ID : US-0YK2JY-76991-1BA-8104
PPID Revision : 002
Service Tag : SRVCTG2
Expr Svc Code : 626 351 582 90
Auto Reboot : enabled
FTOS#

Note: It is advisable to shut down interfaces on a line card that you are hot-swapping.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show linecard</td>
<td>Display the line card(s) status.</td>
</tr>
</tbody>
</table>
module power-off

Turn off power to a line card at next reboot.

Syntax

module power-off linecard number

Parameters

<table>
<thead>
<tr>
<th>linecard number</th>
<th>Enter the keyword line card followed by the line card slot number</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-Series</td>
<td>Range: 0-7</td>
</tr>
<tr>
<td>E-Series</td>
<td>Range: 0 to 13 on an E1200/1200i, 0 to 6 on an E600/E600i, and 0 to 5 on an E300.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.2</td>
<td>E-Series ExaScale E600i</td>
<td></td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale E1200i</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>E-Series C-Series</td>
<td></td>
</tr>
</tbody>
</table>

motd-banner

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

Syntax

motd-banner

Defaults

Enabled on all lines.

Command Modes

LINE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
<td></td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>E-Series S-Series</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>E-Series C-Series</td>
<td></td>
</tr>
</tbody>
</table>

ping

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

Syntax

ping [vrf <id>] [host | ip-address | ipv6-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] [o-interface (ip src-ipv4-address) | interface]
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(OPTIONAL) <strong>E-Series Only</strong>: Enter the VRF Instance name of the device to which you are testing connectivity.</td>
</tr>
<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>
<tr>
<td>ipv6-address</td>
<td>(OPTIONAL) <strong>E-Series only</strong> Enter the IPv6 address, in the X:X::X format, to which you are testing connectivity.</td>
</tr>
<tr>
<td>Note:</td>
<td>The :: notation specifies successive hexadecimal fields of zeros</td>
</tr>
<tr>
<td>count</td>
<td>Enter the number of echo packets to be sent.</td>
</tr>
<tr>
<td></td>
<td><strong>number</strong>: 1 - 2147483647</td>
</tr>
<tr>
<td></td>
<td><strong>Continuous</strong>: transmit echo request continuously</td>
</tr>
<tr>
<td></td>
<td>Default: 5</td>
</tr>
<tr>
<td>datagram size</td>
<td>Enter the ICMP datagram size.</td>
</tr>
<tr>
<td></td>
<td>Range: 36 - 15360 bytes</td>
</tr>
<tr>
<td></td>
<td>Default: 100</td>
</tr>
<tr>
<td>timeout</td>
<td>Enter the interval to wait for an echo reply before timing out.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 - 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 2 seconds</td>
</tr>
<tr>
<td>source</td>
<td>Enter the IPv4 or IPv6 source ip address or the source interface. For IPv6 addresses, you may enter global addresses only.</td>
</tr>
<tr>
<td></td>
<td>• Enter the IP address in A.B.C.D format</td>
</tr>
<tr>
<td></td>
<td>• For an 100/1000 Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <strong>port-channel</strong> followed by a number:</td>
</tr>
<tr>
<td></td>
<td><strong>C-Series</strong> and <strong>S-Series</strong>: Range: 1-128</td>
</tr>
<tr>
<td></td>
<td><strong>E-Series</strong>: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• <strong>E-Series only</strong>: For the SONET interfaces, enter the keyword <strong>sonet</strong> followed by slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <strong>TenGigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <strong>fortyGigE</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN interface, enter the keyword <strong>vlan</strong> followed by a number from 1 to 4094.</td>
</tr>
<tr>
<td>tos</td>
<td>(IPv4 only) Enter the type of service required.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-255</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>df-bit</td>
<td>(IPv4 only) Enter Y or N for the “don't fragment” bit in IPv4 header</td>
</tr>
<tr>
<td></td>
<td>N: Do not set the “don't fragment” bit</td>
</tr>
<tr>
<td></td>
<td>Y: Do set “don't fragment” bit</td>
</tr>
</tbody>
</table>
|               | Default is No. Adam so
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
</table>
| `validate-reply` | (IPv4 only) Enter Y or N for reply validation.  
  N: Do not validate reply data  
  Y: Do validate reply data  
  Default is No. |
| `pattern pattern` | (IPv4 only) Enter the IPv4 data pattern.  
  Range: 0-FFFF  
  Default: 0xABC0 |
| `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` | (IPv4 only) Enter the outgoing interface for multicast packets.  
  - Enter the IP address in A.B.C.D format  
  - For an 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.  
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.  
  - For a Port Channel, enter the keyword `port-channel` followed by a number:  
    - **C-Series and S-Series**: 1-128  
    - **E-Series**: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale  
    - **E-Series only**: For the SONET interfaces, enter the keyword `sonet` followed by slot/port information.  
    - 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. |

**Defaults**

See parameters above.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

- **Version 8.4.6.0**: Added support for the keyword `fortyGigE`.
- **Version 8.4.1.0**: IPv6 pinging available on management interface.
- **Version 8.3.1.0**: Introduced extended ping options.
- **Version 8.2.1.0**: Introduced on E-Series ExaScale (IPv6)
- **Version 8.1.1.0**: Introduced on E-Series ExaScale (IPv4)
- **Version 7.9.1.0**: Introduced VRF
- **Version 7.6.1.0**: Introduced on S-Series
- **Version 7.5.1.0**: Introduced support for C-Series
- **Version 7.4.1.0**: Added support for IPv6 address on E-Series
Usage Information

When you enter the ping command without specifying an IP/IPv6 address (Extended Ping), you are prompted for a target IP/IPv6 address, a repeat count, a datagram size (up to 1500 bytes), a timeout in seconds, and for Extended Commands. See Appendix , for information on the ICMP message codes that return from a ping command.

Figure 5-8. Command Example: ping (IPv4)

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#

Figure 5-9. Command Example: ping (IPv6)

FTOS#ping 100::1
Type Ctrl-C to abort.
Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max = 0/0/0 (ms)
FTOS#

power-off

Turn off power to a selected line card or the standby (extra) Switch Fabric Module (SFM).

Syntax
power-off {linecard number | sfm sfm-slot-id}

Parameters

- **linecard number**: Enter the keyword linecard and a number for the line card slot number.
  - C-Series Range: 0 to 7
  - E-Series Range: 0 to 13 on a E1200/E1200i, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

- **sfm sfm-slot-id**: Enter the keyword sfm by the slot number of the SFM to which you want to turn off power.
  - Note: This option is supported on E-Series only.

Defaults

Disabled

Command Modes

EXEC Privilege

Command History

- Version 8.1.1.2 Introduced on E-Series ExaScale E600i
- Version 8.1.1.0 Introduced on E-Series ExaScale E1200i
- Version 7.5.1.0 Introduced on C-Series

E-Series original Command
### power-on

**Syntax**
```
power-on (linecard number | sfm sfm-slot-id)
```

**Parameters**
- **linecard number**: Enter the keyword `linecard` and a number for the line card slot number.
  - C-Series Range: 0-7
  - E-Series Range: 0 to 13 on a E1200i/E1200i, 0 to 6 on a E600i/E600i, and 0 to 5 on an E300.
- **sfm standby**: Enter the keyword `sfm` followed by the slot number of the SFM to power on.
  - **Note**: This option is supported on E-Series only.

**Defaults**
Disabled

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.1.1.2 Introduced on E-Series ExaScale E600i
- Version 8.1.1.0 Introduced on E-Series ExaScale E1200i
- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command

### reload

**Syntax**
```
reload
```

**Command Modes**
EXEC Privilege

**Command History**
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command

**Usage Information**
If there is a change in the configuration, Dell Networking OS will prompt you to save the new configuration. Or you can save your running configuration with the `copy running-config` command.

### Related Commands
- **reset**: Reset a line card, RPM, a standby SFM (EtherScale only), or a failed SFM (TeraScale and ExaScale).
- **reset stack-unit**: Reset any designated stack member except the management unit
reset

Reset a line card, RPM, a standby SFM (EtherScale only), or a failed SFM (TeraScale only).

Syntax

```
reset {linecard number [hard | power-cycle] | rpm number [hard | power-cycle ] | sfm slot number | standby}
```

Parameters

- **linecard number**: Enter the keyword `linecard` and a number for the line card slot number. (Optional) Add the keyword `hard` or `power-cycle` (power-cycle is C-Series only) to power cycle the line card.
  - **C-Series**: Range: 0-7
  - **E-Series**: Range: 0 to 13 on E1200/E1200i, 0 to 6 on E600/E600i, and 0 to 5 on E300
- **hard**: Enter the keyword `hard` to power cycle the line card.
- **power-cycle**: Enter the keyword `power-cycle` after upgrading a C-Series FPGA to cause the FPGA to be reprogrammed based on the contents of the FPGA PROM.
  - **Note**: This option is supported on C-Series only.
- **rpm number**: Enter the keyword `rpm` followed by a number for the RPM slot number. (Optional) Add the keyword `hard` or `power-cycle` (C-Series only) to power cycle the RPM.
  - Range: 0 to 1
- **sfm standby**: Enter the keyword `sfm standby` to reset the standby SFM.
  - **Note**: This option is supported on E-Series EtherScale only.
- **sfm slot number**: Enter the keyword `sfm` followed by the failed or powered-off SFM slot number.
  - **Note**: Supported on E-Series only

Defaults

Disabled.

Command Modes

EXEC Privilege

Command History

- **Version 7.5.1.0**: Introduced on C-Series
- **E-Series original Command**

Usage Information

The command `reset` without any options is a soft reset, which means Dell Networking OS boots the line card from its runtime image. The `hard` option reloads the Dell Networking OS image on the line card. Use the `power-cycle` after upgrading an FPGA.

When a soft reset is issued on a line card (`reset linecard number`), Dell Networking OS boots the line card from its runtime image. Only when you enter `reset linecard number hard` is the software image reloaded on the line card.

Related Commands

- `reload`: Reboots the system.
- `restore fpga-image`: Copy the backup C-Series FPGA image to the primary FPGA image.

rpm <slot> location-led

Toggle the location LED on/off on the E-Series ExaScale RPM (LC-EH-RPM).

Syntax

```
rpm slot number location-led [on | off]
```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| rpm slot number | Enter the slot number
  E1200i: 0-13
  E600i: 0-6 |
| on | Toggles the LED on the RPM on or off. |

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The LED setting is not saved through power cycles.</td>
<td></td>
</tr>
</tbody>
</table>

**send**

Send messages to one or all terminal line users.

**Syntax**

`send [ ] | [ ] | [ ] | [ ] | [ ]`

**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
- `aux` Enter the keyword `aux` to send a message to an Auxiliary line.
  **Note:** This option is supported on E-Series only.
- `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**

No default behavior or values

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>Version 6.5.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages can contain an unlimited number of lines, however each line is limited to 255 characters. To move to the next line, use the &lt;CR&gt;. To send the message use CTR-Z, to abort a message use CTR-C.</td>
<td></td>
</tr>
</tbody>
</table>
**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.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series original Command

**Usage Information**

If you do not specify parameters and enter `service timestamps`, it appears as `service timestamps debug uptime` in the running-configuration.

Use the `show running-config` command to view the current options set for the service timestamps command.

**show alarms**

View alarms for the RPM, SFMs, line cards and fan trays.

**Syntax**

```
show alarms [threshold]
```

**Parameters**

- `threshold` (OPTIONAL) Enter the keyword threshold to display the temperature thresholds set for the line cards, RPM, and SFMs.

**Command Modes**

EXEC

EXEC Privilege
Command History

| Version 8.1.1.0 | Introduced on E-Series ExaScale |
| Version 7.6.1.0 | Introduced on S-Series |
| Version 7.5.1.0 | Introduced on C-Series |

E-Series original Command

**Figure 5-10. Command Example: show alarms on E-Series**

```
FTOS# show alarms
-- Minor Alarms --
Alarm Type                            Duration
-----------------------------------------------------
RPM 0 PEM A failed or rmvd            7 hr, 37 min
SFM 0 PEM A failed or rmvd            7 hr, 37 min
SFM 1 PEM A failed or rmvd            7 hr, 37 min
SFM 2 PEM A failed or rmvd            7 hr, 37 min
SFM 3 PEM A failed or rmvd            7 hr, 37 min
SFM 4 PEM A failed or rmvd            7 hr, 37 min
SFM 5 PEM A failed or rmvd            7 hr, 37 min
SFM 6 PEM A failed or rmvd            7 hr, 37 min
SFM 7 PEM A failed or rmvd            7 hr, 36 min
line card 1 PEM A failed or rmvd      7 hr, 36 min
line card 4 PEM A failed or rmvd      7 hr, 36 min
only 8 SFMs in chassis                7 hr, 35 min
-- Major Alarms --                    Duration
-----------------------------------------------------
No major alarms
```

show chassis

View the configuration and status of modules in the system. Use this command to determine the chassis mode.

**Syntax**

```
show chassis [brief]
```

**Parameters**

- **brief** (OPTIONAL) Enter the keyword `brief` to view a summary of the show chassis output.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

| Version 8.1.1.0 | Introduced on E-Series ExaScale |
| Version 7.5.1.0 | Introduced on C-Series |

E-Series original Command
Figure 5-11. Command Example: show chassis brief on C-Series

FTOS#show chassis
-- Manufacturing Info --
Chassis Type : C150
Chassis Mode : 1.0
Chassis MAC : 00:01:e8:51:a7:e3
Serial Number : TY000002776
Part Number : 7520036800
Vendor Id : 04
Date Code : 01082008
Country Code : 01
Product Rev : 03
Piece Part ID : US-021R1D-76991-1ba-2776
PPID Revision : 001
Service Tag : srvctg1
Expr Svc Code : 626 351 582 89
FTOS#

Figure 5-12. Command Example: show chassis brief on E-Series

FTOS#show chassis brief
-- Manufacturing Info --
Chassis Type : E1200
Chassis Mode : TeraScale
Chassis Epoch : 10.4 micro-seconds
Chassis MAC : 00:01:e8:55:55:55
Serial Number : FX000003180
Part Number : 7520004200
Vendor Id : 04
Date Code : 01082008
Country Code : 01
Product Rev : 01
Piece Part ID : US-0RVY43-76991-82b-0456
PPID Revision : 1b2
Service Tag : svctgCH
Expr Svc Code : 628 458 864 65
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 8.1.1.0 Introduced on E-Series ExaScale
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series and E-Series

Usage Information

One trace log message is generated for each command. No password information is saved to this file. A command-history trace log is saved to a file upon an RPM failover. This file can be analyzed by the Dell Networking TAC to help identify the root cause of an RPM failover.

Example

Figure 5-13. Command Example: show command-history

FTOS#show command-history
[11/20 15:47:22]: CMD-(CLI):[service password-encryption] by default from console
[11/20 15:47:22]: CMD-(CLI):[service password-encryption hosttos] by default from console
  - Repeated 3 times.
[11/20 15:47:23]: CMD-(CLI):[service timestamps log datetime] by default from console
[11/20 15:47:23]: CMD-(CLI):[hostname FTOS] by default from console
[11/20 15:47:23]: CMD-(CLI):[enable password 7 ******] by default from console
[11/20 15:47:23]: CMD-(CLI):[username admin password 7 ******] by default from console
[11/20 15:47:23]: CMD-(CLI):[protocol spanning-tree rstp] by default from console
[11/20 15:47:23]: CMD-(CLI):[no disable] by default from console
[11/20 15:47:23]: CMD-(CLI):[interface gigabitethernet 0/1] by default from console
[11/20 15:47:23]: CMD-(CLI):[ip address 1.1.1.1 /24] by default from console
[11/20 15:47:23]: CMD-(CLI):[ip access-group abc in] by default from console
[11/20 15:47:23]: CMD-(CLI):[no shutdown] by default from console
[11/20 15:47:23]: CMD-(CLI):[interface gigabitethernet 0/2] by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address] by default from console
[11/20 15:47:23]: CMD-(CLI):[interface gigabitethernet 0/3] by default from console
[11/20 15:47:23]: CMD-(CLI):[ip address 5.5.5.1 /24] by default from console
[11/20 15:47:23]: CMD-(CLI):[no shutdown] by default from console
[11/20 15:47:23]: CMD-(CLI):[interface gigabitethernet 0/5] by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address] by default from console
[11/20 21:17:35]: CMD-(CLI):[line console 0] by default from console
[11/20 21:17:36]: CMD-(CLI):[exec-timeout 0] by default from console
FTOS#
Related Commands

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

---

**show command-tree**

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

**Syntax**

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

**Parameters**

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

**Defaults**

None

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- **Version 8.2.1.0** Introduced

**Usage Information**

Reload the system to reset the command-tree counters.

**Example**

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

  enable                        command usage:3
         <0-15>                       option usage: 0
  exit                               command usage:1
  show command-tree              command usage:9
         count                          option usage: 3
  show version                      command usage:1
!
Global configuration mode:

  aaa authentication enable            command usage:1
     WORD                               option usage: 1
     default                            option usage: 0
     enable                             option usage: 0
     line                               option usage: 0
     none                               option usage: 0
     radius                             option usage: 1
     tacacs+                            option usage: 0
```

---

**show console lp**

View the buffered boot-up log of a line card.

**Syntax**

```
show console lp number
```

---
show cpu-traffic-stats

View the CPU traffic statistics.

Syntax

show cpu-traffic-stats [port number | all | cp | linecard {all | slot#} | rp1 | rp2]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>(OPTIONAL) Enter the port number to display traffic statistics on that port only. Range: 1 to 1568</td>
</tr>
<tr>
<td>all</td>
<td>(OPTIONAL) Enter the keyword all to display traffic statistics on all the interfaces receiving traffic, sorted based on traffic.</td>
</tr>
<tr>
<td>cp</td>
<td>(OPTIONAL) Enter the keyword cp to display traffic statistics on the specified CPU. Note: This option is supported on E-Series only.</td>
</tr>
<tr>
<td>linecard</td>
<td>(OPTIONAL) Enter the keyword linecard followed by either all or the slot number to display traffic statistics on the designated line card. Note: This option is supported on C-Series only.</td>
</tr>
<tr>
<td>rp1</td>
<td>(OPTIONAL) Enter the keyword rp1 to display traffic statistics on the RP1. Note: This option is supported on E-Series only.</td>
</tr>
<tr>
<td>rp2</td>
<td>(OPTIONAL) Enter the keyword rp2 to display traffic statistics on the RP2. Note: This option is supported on E-Series only.</td>
</tr>
</tbody>
</table>

Defaults

all

Command Modes

EXEC

Command History

Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
Version 6.2.1.1 Introduced on E-Series

Usage Information

Caution: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.
E-Series Example

**Figure 5-14. Command Example: show cpu-traffic-stats on the E-Series**

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

Processor : RP1
------------
Received 62% traffic on GigabitEthernet 8/2   Total packets:500
   LLC:0, SNAP:0, IP:500, ARP:0, other:0
   Unicast:500, Multicast:0, Broadcast:0

Received 37% traffic on GigabitEthernet 8/1   Total packets:300
   LLC:0, SNAP:0, IP:300, ARP:0, other:0
   Unicast:300, Multicast:0, Broadcast:0

Processor : RP2
------------
No CPU traffic statistics.
```  

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug cpu-traffic-stats</code></td>
<td>Enable CPU traffic statistics for debugging</td>
</tr>
</tbody>
</table>

**show debugging**

View a list of all enabled debugging processes.

**Syntax**

```
show debugging
```

**Command Mode**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command
show environment (C-Series and E-Series)

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

**Syntax**

```
show environment [all | fan | linecard | linecard-voltage | PEM | RPM | SFM]
```

**Parameters**

- **all**
  - Enter the keyword **all** to view all components.

- **fan**
  - Enter the keyword **fan** to view information on the fans. The output of this command is chassis dependent. See Figure 5-12, Figure 5-13, and Figure 5-14 for a comparison of output.

- **linecard**
  - Enter the keyword **linecard** to view only information on line cards

- **linecard-voltage**
  - Enter the keyword **linecard-voltage** to view line card voltage information.

- **PEM**
  - Enter the keyword **PEM** to view only information on power entry modules.

- **RPM**
  - Enter the keyword **RPM** to view only information on RPMs.

- **SFM**
  - Enter the keyword **SFM** to view only information on SFMs.

  **Note:** This option is supported on E-Series only.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.8.1.0 Added temperature information for C-Series fans (Figure 5-18)
- Version 7.5.1.0 Introduced on C-Series

**Usage Information**

Fan speed is controlled by temperatures measured at the sensor located on the fan itself. The fan temperatures shown with this command may not accurately reflect the temperature and fan speed. Refer to your hardware installation guide for fan speed and temperature information.
Examples

Figure 5-16. Command Example: show environment for the E1200

FTOS#show environment
-- Fan Status --
Tray Status Temp Volt Speed PEM0 PEM1 Fan1 Fan2 Fan3
------------------------------------------------------------------
0 up < 50C 12-16V low/2100-2700 RPM up up up up up
1 up < 50C 12-16V low/2100-2700 RPM up up up up up
2 up < 50C 12-16V low/2100-2700 RPM up up up up up
3 up < 50C 12-16V low/2100-2700 RPM up up up up up
4 up < 50C 16-20V med/2700-3200 RPM up up up up up
5 up < 50C 12-16V low/2100-2700 RPM up up up up up
-- Power Entry Modules --
Bay Status
------------------------------------------------------------------
0 absent or down
1 up
-- Line Card Environment Status --
Slot Status Temp PEM0 PEM1 Voltage
------------------------------------------------------------------
0 not present
1 not present
2 not present
3 not present
4 not present
5 not present
6 not present
7 not present
8 not present
9 not present
10 not present
11 booting 53C down up ok
12 not present
13 not present
-- RPM Environment Status --
Slot Status Temp PEM0 PEM1 Voltage
------------------------------------------------------------------
0 active 48C down up ok
1 not present
-- SFM Environment Status --
Slot Status Temp PEM0 PEM1
------------------------------------------------------------------
0 active 49C up up
1 active 47C up up
2 active 46C up up
3 active 48C up up
4 active 52C up up
5 active 50C up up
6 active 47C up up
7 active 48C up up
8 active 47C up up
FTOS#

Figure 5-17. Command Example: show environment fan on the E600

FTOS#show environment fan
-- Fan Status --
Status Temp Fan1 Fan2 Fan3 Serial Num Version
------------------------------------------------------------------
up 29C 6000 RPM 7500 RPM 7500 RPM 0.0
FTOS#
show environment (S-Series)

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

Syntax

```
show environment [all | fan | stack-unit unit-id | pem]
```

Parameters

- `all`: Enter the keyword `all` to view all components.
- `fan`: Enter the keyword `fan` to view information on the fans. The output of this command is chassis dependent.
- `stack-unit unit-id`: Enter the keyword `stack-unit` followed by the `unit-id` to display information on a specific stack member. Range: 0 to 1.
- `pem`: Enter the keyword `pem` to view only information on power entry modules.

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 7.8.1.0** The output of the `show environment fan` command for S-Series is changed to display fan speeds instead of just showing the fan status as up or down.
- **Version 7.6.1.0** Introduced for S-Series. S-Series options and output differ from the C-Series/E-Series version.

Usage Information

Figure 5-19 shows the output of the `show environment fan` command as it appears prior to Dell Networking OS 7.8.1.0.

```
FTOS#show env fan

-- Fan Status --

Tray 0

+---------------------+-----------------+---------------------+
<table>
<thead>
<tr>
<th>FanNumber</th>
<th>Speed</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4170</td>
<td>up</td>
</tr>
<tr>
<td>1</td>
<td>4140</td>
<td>up</td>
</tr>
<tr>
<td>2</td>
<td>3870</td>
<td>up</td>
</tr>
<tr>
<td>3</td>
<td>4140</td>
<td>up</td>
</tr>
<tr>
<td>4</td>
<td>3870</td>
<td>up</td>
</tr>
<tr>
<td>5</td>
<td>3810</td>
<td>up</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>--------</td>
</tr>
</tbody>
</table>

FTOS#
```
Example  Figure 5-19. Command Example: show environment all on the S-Series

```
FTOS#show environment all
-- Fan Status --
--------------------------------------------------------------------------------
Unit  TrayStatus Fan0 Fan1 Fan2 Fan3 Fan4 Fan5
  0     up    up    up    up    up    up    up
-- Power Supplies --
Unit   Bay Status       Type
--------------------------------------------------------------------------------
  0     0     up            AC
  0     1     absent
-- Unit Environment Status --
Unit  Status        Temp   Voltage
--------------------------------------------------------------------------------
  0*    online        50C    ok
  * Management Unit
-- Fan Status --
Unit  Status   Speed Fan1 Fan2 Fan3 Fan4 Fan5 Fan6    Serial Num    Version
--------------------------------------------------------------------------------
  1      up        high up    up    up    up    up 1234  1
```

Example  Figure 5-20. Command Example: show environment fan on the S-Series

```
FTOS#show environment fan
-- Fan Status --
--------------------------------------------------------------------------------
Unit  TrayStatus Fan0 Fan1 Fan2 Fan3 Fan4 Fan5
  0     up    up    up    up    up    up    up
```

Example  Figure 5-21. Command Example: show environment pem on the S-Series

```
FTOS#show environment pem
-- Power Supplies --
Unit   Bay Status       Type
--------------------------------------------------------------------------------
  0     0     up            AC
  0     1     absent
```

Example  Figure 5-22. Command Example: show environment stack-unit on the S-Series

```
FTOS#show environment stack-unit 0
-- Unit Environment Status --
Unit  Status        Temp   Voltage
--------------------------------------------------------------------------------
  0*    online        49C    ok
  * Management Unit
```
show inventory (C-Series and E-Series)

Display the chassis type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.

**Syntax**

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

**Parameters**

- `media slot` (OPTIONAL) Enter the keyword `media` followed by the slot number.
  - C-Series Range: 0-7
  - E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.8.1.0 Output expanded to include SFP+ media in C-Series.
- Version 7.7.1.0 Vendor field removed from output of `show inventory media`.
- Version 7.5.1.0 Introduced on C-Series and expanded to include transceiver media
- Version 6.2.1.0 Expanded to include Software Protocol Configured field on E-Series
- Version 5.3.1.0 Introduced on E-Series

**Usage Information**

The `show inventory media` command provides some details about installed pluggable media (SFP, XFP), as shown in Figure 5-25. Use the `show interfaces` command to get more details about installed pluggable media.

The display output might include a double asterisk (**) next to the SFMs, for example:

```
   ... 0   CC-E-SFM **   0004875       7490007411   A
   1   CC-E-SFM **   0004889       7490007411   A
   ...```

The double asterisk generally indicates the SFM’s frequency capabilities, indicating either that they are operating at 125 MHz or that the frequency capability, which is stored in an EPROM, cannot be determined.

If there are no fiber ports in the line card, then just the header under show inventory media will be displayed. If there are fiber ports but no optics inserted, then the output will display “Media not present or accessible.”

C7008 Example
### FTOS#sh inventory

**Chassis Type**: C150  
**Chassis Mode**: 1.0  
**Software Version**: E8-4-2-399

<table>
<thead>
<tr>
<th>Slot Item</th>
<th>Serial Number</th>
<th>Part Number</th>
<th>Rev</th>
<th>Piece Part ID</th>
<th>Rev</th>
<th>Svc Tag</th>
<th>Exprs Svc Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>C150</td>
<td>TY000002776</td>
<td>7520036800</td>
<td>03</td>
<td>US-021R1D-76991-1BA-2776 001 SRVCTG1 626 351 582 89</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>FX000008104</td>
<td>7520029400</td>
<td>03</td>
<td>US-0YK2JY-76991-1BA-8104 002 SRVCTG2 626 351 582 90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>FX000001094</td>
<td>7520029401</td>
<td>01</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>FX000002945</td>
<td>7520030304</td>
<td>02</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>FX000013637</td>
<td>7520030400</td>
<td>02</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>FX000037575</td>
<td>7520029307</td>
<td>02</td>
<td>US-074VKT-76991-1BA-7575 002 SRVCTG9 626 351 582 97</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>FX000026033</td>
<td>7520033800</td>
<td>03</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* - standby

---

### E-Series Example

**FTOS#show inventory**  
**Chassis Type**: EI200  
**Chassis Mode**: TeraScale  
**Software Version**: E8-4-2-399

<table>
<thead>
<tr>
<th>Slot Item</th>
<th>Serial Number</th>
<th>Part Number</th>
<th>Rev</th>
<th>Piece Part ID</th>
<th>Rev</th>
<th>Svc Tag</th>
<th>Exprs Svc Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>EI200</td>
<td>FX000033180</td>
<td>752004200</td>
<td>01</td>
<td>US-ORVY43-76991-82B-0456 1B2 SVCTGCH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>FX000033136</td>
<td>7520016601</td>
<td>01</td>
<td>US-0YK2JY-76991-1BA-1361 001 SRVCTG3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>FX000031361</td>
<td>7520016600</td>
<td>01</td>
<td>US-0YK2JY-76991-1BA-1360 001 SRVCTG3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* - standby

---

### Figure 5-24. Example output of show inventory for E-Series

**Chassis Type**: EI200  
**Chassis Mode**: TeraScale  
**Software Version**: E8-4-2-399

<table>
<thead>
<tr>
<th>Slot Item</th>
<th>Serial Number</th>
<th>Part Number</th>
<th>Rev</th>
<th>Piece Part ID</th>
<th>Rev</th>
<th>Svc Tag</th>
<th>Exprs Svc Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>EI200</td>
<td>FX000008104</td>
<td>7520029400</td>
<td>03</td>
<td>US-0YK2JY-76991-1BA-8104 002 SRVCTG2 626 351 582 90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>FX000001094</td>
<td>7520029401</td>
<td>01</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>FX000002945</td>
<td>7520030304</td>
<td>02</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>FX000013637</td>
<td>7520030400</td>
<td>02</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>FX000037575</td>
<td>7520029307</td>
<td>02</td>
<td>US-074VKT-76991-1BA-7575 002 SRVCTG9 626 351 582 97</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>FX000026033</td>
<td>7520033800</td>
<td>03</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* - standby

---

### Figure 5-23. Example output of show inventory for C7008 (C-Series)

**Chassis Type**: C150  
**Chassis Mode**: 1.0  
**Software Version**: E8-4-2-399

<table>
<thead>
<tr>
<th>Slot Item</th>
<th>Serial Number</th>
<th>Part Number</th>
<th>Rev</th>
<th>Piece Part ID</th>
<th>Rev</th>
<th>Svc Tag</th>
<th>Exprs Svc Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>C150</td>
<td>TY000002776</td>
<td>7520036800</td>
<td>03</td>
<td>US-021R1D-76991-1BA-2776 001 SRVCTG1 626 351 582 89</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>FX000008104</td>
<td>7520029400</td>
<td>03</td>
<td>US-0YK2JY-76991-1BA-8104 002 SRVCTG2 626 351 582 90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>FX000001094</td>
<td>7520029401</td>
<td>01</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>FX000002945</td>
<td>7520030304</td>
<td>02</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>FX000013637</td>
<td>7520030400</td>
<td>02</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>FX000037575</td>
<td>7520029307</td>
<td>02</td>
<td>US-074VKT-76991-1BA-7575 002 SRVCTG9 626 351 582 97</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>FX000026033</td>
<td>7520033800</td>
<td>03</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* - standby
show inventory (S-Series)

Display the S-Series switch type, components (including media), Dell Networking OS 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

- No default behavior or values

Command Modes

- CONFIGURATION

Command History

- Version 7.6.1.0: Introduced this version of the command for S-Series. S-Series output differs from E-Series.

Usage

- If there are no fiber ports in the unit, then just the header under `show inventory media` will be displayed. If there are fiber ports but no optics inserted, then the output will display “Media not present or accessible.”
Example Figure 5-27. Example output of show inventory for S-Series

FTOS#show inventory
System Type : S50N
System Mode : 1.0
Software Version : E8-4-2-399

* 2  S50-01-GE-48T-AC  DL257430183  7590005600  B  CN-0RVY43-28298-82B-0456 1B2  SVCTGCH  628 458 864 65
2  S50-01-12G-2S      N/A            N/A          N/A  N/A                      N/A  N/A      N/A
2  S50-PWR-AC         N/A            N/A          N/A  N/A                      N/A  N/A      N/A
2  S50-FAN            N/A            N/A          N/A  N/A                      N/A  N/A      N/A

* - Management Unit

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Display the line card(s) status.</td>
</tr>
<tr>
<td>show linecard [number [brief]</td>
<td>Display the physical status and operational status of an installed transceiver. The output also displays the transceiver’s serial number.</td>
</tr>
<tr>
<td>show interfaces transceiver</td>
<td>Display the interface configuration.</td>
</tr>
</tbody>
</table>

show linecard

Syntax

show linecard [number [brief] | all]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>(OPTIONAL) Enter a slot number to view information on the line card in that slot. C-Series Range: 0-7 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.</td>
</tr>
<tr>
<td>all</td>
<td>(OPTIONAL) Enter the keyword all to view a table with information on all present line cards.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword brief to view an abbreviated list of line card information.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command
Figure 5-28. Command Example: show linecard on E-Series

FTOS#show linecard 0
-- Line card 0 --
Status : online
Next Boot : online
Required Type : E48TF - 48-port 10/100/1000Base-T line card with RJ-45 interfaces (EF)
Current Type : E48TF - 48-port 10/100/1000Base-T line card with RJ-45 interfaces (EF)
Hardware Rev : Base - 1.1 PP0 - 1.1 PP1 - 1.1
Num Ports : 48
Up Time : 2 min, 41 sec
Dell Networking OS Version : 8-4-2-399
Jumbo Capable : yes
Boot Flash : A: 2.3.2.1 [booted] B: 2.3.2.1
Memory Size : 268435456 bytes
Temperature : 44C
Power Status : PEM0: absent or down PEM1: up
Voltage : ok
Serial Number : FX000031361
Part Number : 7520016601 Rev 01
Vendor Id : 04
Date Code : 02312005
Country Code : 01
Piece Part ID : US-0YK2JY-76991-1BA-1361
PPID Revision : 001
Service Tag : SRVCTG3
Expr Svc Code : 626 351 582 91
Auto Reboot : enabled

FTOS#
```
FTOS#show linecard 11

-- Line card 11 --
Status        : online
Next Boot     : online
Required Type : E48PF - 48-port GE line card with SFP optics (EF)
Current Type  : E48PF - 48-port GE line card with SFP optics (EF)
Hardware Rev  : Base - 1.0  PP0 - n/a  PP1 - n/a
Num Ports     : 48
Up Time       : 12 hr, 37 min
Dell Networking OS Version : 6.2.1.x
Jumbo Capable : yes
Boot Flash    : A: 2.0.3.4 B: 2.0.3.4 [booted]
Memory Size   : 268435456 bytes
Temperature   : 49C
Power Status  : PEM0: absent or down  PEM1: up
Voltage       : ok
Serial Number :
Part Number    :
Vendor Id      :
Date Code      :
Country Code   :
Piece Part ID  : US-0YK2JY-76991-1BA-8104
PPID Revision  : 002
Service Tag    : SRVCTG2
Expr Svc Code  : 626 351 582 90
Auto Reboot    : enabled

FTOS#
```
Table 5-1 list the definitions of the fields shown in Figure 5-28.

**Table 5-1. Descriptions for show linecard output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line card</td>
<td>Displays the line card slot number (only listed in show linecard all command output).</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the line card’s status.</td>
</tr>
<tr>
<td>Next Boot</td>
<td>Displays whether the line card is to be brought online at the next system reload.</td>
</tr>
<tr>
<td>Required Type</td>
<td>Displays the line card type configured for the slot.</td>
</tr>
<tr>
<td></td>
<td>The Required Type and Current Type must match. Use the linecard command to reconfigure the line card type if they do not match.</td>
</tr>
<tr>
<td>Current Type</td>
<td>Displays the line card type installed in the slot.</td>
</tr>
<tr>
<td></td>
<td>The Required Type and Current Type must match. Use the linecard command to reconfigure the line card type if they do not match.</td>
</tr>
<tr>
<td>Hardware Rev</td>
<td>Displays the chip set revision.</td>
</tr>
<tr>
<td>Num Ports</td>
<td>Displays the number of ports in the line card.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Displays the number of hours and minutes the card is online.</td>
</tr>
<tr>
<td>Dell Networking OS Version</td>
<td>Displays the operating software version.</td>
</tr>
<tr>
<td>Jumbo Capable</td>
<td>Displays Yes or No indicating if the line card can support Jumbo frames.</td>
</tr>
<tr>
<td></td>
<td>This field does not state whether the chassis is operating in EtherScale or TeraScale mode.</td>
</tr>
<tr>
<td>Boot Flash Ver</td>
<td>Displays the two possible Bootflash versions. The [Booted] keyword next to the version states which version was used at system boot.</td>
</tr>
<tr>
<td>Memory Size</td>
<td>List the memory of the line card processor.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Displays the temperature of the line card. Minor alarm status if temperature is over 65° C.</td>
</tr>
<tr>
<td>Power Status</td>
<td>Lists the type of power modules used in the chassis:</td>
</tr>
<tr>
<td></td>
<td>• AC = AC power supply</td>
</tr>
<tr>
<td></td>
<td>• DC = DC Power Entry Module (PEM)</td>
</tr>
<tr>
<td>Voltage</td>
<td>Displays OK if the line voltage is within range.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Displays the line card serial number.</td>
</tr>
<tr>
<td>Part Num</td>
<td>Displays the line card part number.</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Displays an internal code, which specifies the manufacturing vendor.</td>
</tr>
<tr>
<td>Date Code</td>
<td>Displays the line card’s manufacturing date.</td>
</tr>
</tbody>
</table>
Figure 5-30. Command Example: show linecard brief

FTOS#show linecard 11 brief

-- Line card 11 --
Status : online
Next Boot: online
Required Type: E48PF - 48-port GE line card with SFP optics (EF)
Current Type: E48PF - 48-port GE line card with SFP optics (EF)
Hardware Rev: Base - 1.0  PP0 - n/a  PP1 - n/a
Num Ports: 48
Up Time: 11 hr, 24 min
Dell Networking OS Version: 6.1.1.0
Jumbo Capable: yes
FTOS#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linecard</td>
<td>Pre-configure a line card in a currently empty slot of the system or a different line card type for the slot.</td>
</tr>
<tr>
<td>show interfaces linecard</td>
<td>Display information on all interfaces on a specific line card.</td>
</tr>
<tr>
<td>show chassis</td>
<td>View information on all elements of the system.</td>
</tr>
<tr>
<td>show rpm</td>
<td>View information on the RPM.</td>
</tr>
<tr>
<td>show sfm</td>
<td>View information on the SFM.</td>
</tr>
</tbody>
</table>

show linecard boot-information

View the line card status and boot information.

Syntax

show linecard boot-information

Command Modes

EXEC
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>6.5.1.4</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

Example

Figure 5-31. Command Example: show linecard boot-information

FTOS#show linecard boot-information

-- Line cards --

<table>
<thead>
<tr>
<th>#</th>
<th>Status</th>
<th>CurType</th>
<th>Serial</th>
<th>Booted</th>
<th>Next Boot</th>
<th>Cache</th>
<th>Boot flash</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>online</td>
<td>E48PF</td>
<td>012345</td>
<td>6.5.1.4</td>
<td>6.5.1.4</td>
<td>A: invalid</td>
<td>B: 6.5.1.4</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>online</td>
<td>E48TF</td>
<td>0031318</td>
<td>6.5.1.4</td>
<td>6.5.1.4</td>
<td>A: invalid</td>
<td>B: 6.5.1.4</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

FTOS#
Table 5-2 defines the fields in Figure 5-31.

**Table 5-2. Descriptions for show linecard boot-information output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Displays the line card slot numbers, beginning with slot 0. The number of slots listed is dependent on your chassis: E-Series: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates if a line card is online, offline, or booting. If a line card is not detected in the slot, a hyphen ( - ) is displayed.</td>
</tr>
<tr>
<td>CurType</td>
<td>Displays the line card identification number, for example EXW4PF.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Displays the line card serial number.</td>
</tr>
<tr>
<td>Booted from</td>
<td>Indicates whether the line card cache booted or system booted. In addition, the image with which the line card booted is also displayed. If the line card cache booted, then the output is A: or B: followed by the image in the flash partition (A: 6.5.1.4 or B: 6.5.1.4). If the line card system booted, then display is the current Dell Networking OS version number (6.5.1.4).</td>
</tr>
<tr>
<td>Next boot</td>
<td>Indicates if the next line card boot is a cache boot or system boot and which image will be used in the boot.</td>
</tr>
<tr>
<td>Cache boot</td>
<td>Displays the system image in cache boot flash partition A: and B: for the line card. If the cache boot does not contain a valid image, “invalid” is displayed.</td>
</tr>
<tr>
<td>Boot flash</td>
<td>Displays the two possible Boot flash versions. The [b] next to the version number is the current boot flash, that is the image used in the last boot.</td>
</tr>
</tbody>
</table>

The display area of this command uses the maximum 80 character length. If your display area is not set to 80 characters, the display will wrap.

**Usage Information**

**Related Commands**

- `show linecard` View the line card status
- `upgrade (E-Series version)` Upgrade the boot flash, boot selector, or system image
- `download alt-boot-image` Download an alternate boot image to the chassis
- `download alt-full-image` Download an alternate Dell Networking OS image to the chassis
- `download alt-system-image` Download an alternate system image to the chassis

**show memory (C-Series and E-Series)**

View current memory usage on the system.

**Syntax**

```
show memory [cp | lp slot-number | rp1 | rp2]
```
The output for show memory displays the memory usage of LP part (sysdlp) of the system. The Sysdlp is an aggregate task that handles all the tasks running on C-Series’ and E-Series' LP.

In Dell Networking OS Release 7.4.1.0 and higher, the total counter size (for all 3 CPUs) in show memory (C-Series and E-Series) and show processes memory (C-Series and E-Series) will differ based on which Dell Networking OS processes are counted.

- In the show memory (C-Series and E-Series) display output, the memory size is equal to the size of the application processes.
- In the show processes memory (C-Series and E-Series) display output, the memory size is equal to the size of the application processes plus the size of the system processes.

### E-Series Example

**Figure 5-32. Command Example: show memory on E-Series**

```
FTOS#show memory
  Statistics On  CP Processor
  Total(b)   Used(b)   Free(b)   Lowest(b)   Largest(b)
  452689184   64837834   387851350   387805590   371426976
  Statistics On RP1 Processor
  Total(b)   Used(b)   Free(b)   Lowest(b)   Largest(b)
  629145600   4079544   625066056   625066056            0
  Statistics On RP2 Processor
  Total(b)   Used(b)   Free(b)   Lowest(b)   Largest(b)
  510209568   47294716   462914852   462617968   446275376
FTOS#
```
Table 5-3 defines the fields displayed in Figure 5-32.

### Table 5-3. Descriptions for show memory output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowest</td>
<td>Displays the memory usage the system went to in the lifetime of the system. Indirectly, it indicates the maximum usage in the lifetime of the system: Total minus Lowest.</td>
</tr>
<tr>
<td>Largest</td>
<td>The current largest available. This relates to block size and is not related to the amount of memory on the system.</td>
</tr>
</tbody>
</table>

### show memory (S-Series)

View current memory usage on the S-Series switch.

**Syntax**

```
show memory [stack-unit 0-7]
```

**Parameters**

- `stack-unit 0-7` (OPTIONAL) Enter the keyword `stack-unit` followed by the stack unit ID of the S-Series stack member to display memory information on the designated stack member.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 7.6.1.0 Introduced this version of the command for the S-Series

**Usage Information**

The output for show memory 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 S-Series’ CPU.

**Example**

```
Figure 5-33. Command Example: show memory on S-Series

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 (C-Series and E-Series)

View CPU usage information based on processes running in the system.

**Syntax**

```
show processes cpu [cp | rp1 | rp2] [lp [linecard-number | 1-99] | all | summary]
```

**Parameters**

- `cp` (OPTIONAL) Enter the keyword `cp` to view CPU usage of the Control Processor.
- `rp1` (OPTIONAL) Enter the keyword `rp1` to view CPU usage of the Route Processor 1.

**Note:** This option is supported on the E-Series only.
**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on C-Series</th>
<th>Modified: Added the lp all option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.4.1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Modified: The granularity of the output for rp1 and rp2 is changed. The output is now at the process level, so process-specific statistics are displayed.</td>
<td></td>
</tr>
</tbody>
</table>

**Example 1**

Figure 5-34. Command Example: show processes cpu (Partial)

```
FTOS#show processes cpu
CPU Statistics On CP Processor
----------------------------------------
CPU utilization for five seconds: 4%/2%; one minute: 2%; 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>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xd02e4e8</td>
<td>1498633</td>
<td>89918</td>
<td>16666</td>
<td>3.00%</td>
<td>2.67%</td>
<td>2.67%</td>
<td>0</td>
<td>KP</td>
</tr>
<tr>
<td>0xd9d4c70</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>tLogTask</td>
</tr>
<tr>
<td>0xd9cd200</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>soc_dpc</td>
</tr>
<tr>
<td>0xd9bf588</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>TEARL</td>
</tr>
<tr>
<td>0xd9bf2f8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>tBCMlink</td>
</tr>
<tr>
<td>0xd9bb0e0</td>
<td>700</td>
<td>42</td>
<td>16666</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>tBcmTask</td>
</tr>
<tr>
<td>0xd9998d0</td>
<td>106683</td>
<td>6401</td>
<td>16666</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>tNetTask</td>
</tr>
<tr>
<td>0xd368a0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>tWdbTask</td>
</tr>
<tr>
<td>0xd3329b0</td>
<td>166</td>
<td>10</td>
<td>16600</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>tWdtTask</td>
</tr>
<tr>
<td>0xd32a8c8</td>
<td>102500</td>
<td>6150</td>
<td>16666</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>tme</td>
</tr>
<tr>
<td>0xd161d8</td>
<td>120500</td>
<td>723</td>
<td>16666</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ipc</td>
</tr>
<tr>
<td>0xd1680c8</td>
<td>33</td>
<td>2</td>
<td>16500</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>irc</td>
</tr>
<tr>
<td>0xd156008</td>
<td>116</td>
<td>7</td>
<td>16571</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>RpmAvailMgr</td>
</tr>
<tr>
<td>0xd153ab0</td>
<td>216</td>
<td>13</td>
<td>16615</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ev</td>
</tr>
</tbody>
</table>
```

- more -
Example 2  
Figure 5-35. Command Example: show processes cpu rp1

FTOS#show processes cpu rp1
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime(ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>S5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000007c</td>
<td>60</td>
<td>6</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ospf</td>
</tr>
<tr>
<td>0x00000077</td>
<td>460</td>
<td>46</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>dsm</td>
</tr>
<tr>
<td>0x00000074</td>
<td>100</td>
<td>10</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ipmi</td>
</tr>
<tr>
<td>0x0000006e</td>
<td>100</td>
<td>10</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>rip</td>
</tr>
<tr>
<td>0x0000006b</td>
<td>120</td>
<td>12</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>acl</td>
</tr>
<tr>
<td>0x00000064</td>
<td>690</td>
<td>69</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>sysdi</td>
</tr>
<tr>
<td>0x00000062</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>
<td>sysmon</td>
</tr>
<tr>
<td>0x00000024</td>
<td>980</td>
<td>88</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>sshd</td>
</tr>
<tr>
<td>0x00000022</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>init</td>
</tr>
<tr>
<td>0x00000020</td>
<td>2580</td>
<td>258</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>mount_mfs</td>
</tr>
</tbody>
</table>

Example 3  
Figure 5-36. Command Example: show processes cpu rp2

FTOS#show processes cpu rp2
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime(ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>S5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000090</td>
<td>140</td>
<td>14</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>vrrp</td>
</tr>
<tr>
<td>0x0000008d</td>
<td>120</td>
<td>12</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>frrp</td>
</tr>
<tr>
<td>0x00000088</td>
<td>360</td>
<td>36</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>xstp</td>
</tr>
<tr>
<td>0x00000084</td>
<td>60</td>
<td>6</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>span</td>
</tr>
<tr>
<td>0x00000083</td>
<td>180</td>
<td>18</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>pim</td>
</tr>
<tr>
<td>0x00000080</td>
<td>80</td>
<td>8</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>igmp</td>
</tr>
<tr>
<td>0x0000007b</td>
<td>130</td>
<td>13</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ipm2</td>
</tr>
<tr>
<td>0x00000078</td>
<td>700</td>
<td>70</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>mrtm</td>
</tr>
<tr>
<td>0x00000074</td>
<td>100</td>
<td>10</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>l2mgr</td>
</tr>
<tr>
<td>0x00000070</td>
<td>80</td>
<td>8</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>l2pm</td>
</tr>
<tr>
<td>0x0000006c</td>
<td>80</td>
<td>8</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>arpm</td>
</tr>
<tr>
<td>0x00000068</td>
<td>60</td>
<td>6</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>acl2</td>
</tr>
<tr>
<td>0x00000064</td>
<td>750</td>
<td>75</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>sysd2</td>
</tr>
<tr>
<td>0x00000062</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>sysmon</td>
</tr>
<tr>
<td>0x0000006c</td>
<td>880</td>
<td>88</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>sshd</td>
</tr>
<tr>
<td>0x00000022</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>init</td>
</tr>
<tr>
<td>0x00000020</td>
<td>2250</td>
<td>225</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>mount_mfs</td>
</tr>
<tr>
<td>0x0000001d</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>mount_mfs</td>
</tr>
<tr>
<td>0x00000006</td>
<td>100</td>
<td>10</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>sh</td>
</tr>
<tr>
<td>0x00000005</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>aiodoned</td>
</tr>
<tr>
<td>0x00000004</td>
<td>960</td>
<td>96</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>loflush</td>
</tr>
<tr>
<td>0x00000003</td>
<td>140</td>
<td>14</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>reaper</td>
</tr>
<tr>
<td>0x00000002</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>pagedaemon</td>
</tr>
<tr>
<td>0x00000001</td>
<td>160</td>
<td>16</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>init</td>
</tr>
<tr>
<td>0x00000000</td>
<td>700</td>
<td>70</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>swapper</td>
</tr>
</tbody>
</table>

Usage Information
The CPU utilization for the last five seconds as shown in Figure 5-34 is 4%/2%. The first number (4%) is the CPU utilization for the last five seconds. The second number (2%) indicates the percent of CPU time spent at the interrupt level.
show processes cpu (S-Series)

Display CPU usage information based on processes running in an S-Series.

Syntax

```
show processes cpu [management-unit 1-99 [details] | stack-unit 0-7 | summary | ipc | memory [stack-unit 0-7]]
```

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 0-7` (OPTIONAL) Enter the keyword `stack-unit` followed by the stack member ID (Range 0 to 7).
  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.
- `summary` (OPTIONAL) Enter the keyword `summary` to view a summary view of CPU usage for all members of the stack. See Example 1.
- `ipc` (OPTIONAL) Enter the keyword `ipc` to display inter-process communication statistics.
- `memory` (OPTIONAL) Enter the keyword `memory` to display memory statistics. See Example 4.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 7.7.1.0 Modified: Added management-unit [details] keywords.
- Version 7.6.1.0 Introduced for S-Series

Example 1

**Figure 5-37. Command Example: show processes cpu summary on S-Series**

FTOS#show processes cpu summary

```
CPU utilization 5Sec 1Min 5Min
-------------------------------------------
Unit0 0% 0% 0%
-------------------------------------------
CPU utilization 5Sec 1Min 5Min
-------------------------------------------
Unit1* 1% 0% 0%
Unit2 0% 0% 0%
Unit3 0% 0% 0%

* Mgmt Unit
```
### Example 2

**Figure 5-38. Command Example: show processes cpu management-unit on S-Series**

```plaintext
FTOS#show processes cpu management-unit 0

CPU utilization for five seconds: 1%/0%; one minute: 10%; five minutes: 2%

<table>
<thead>
<tr>
<th>PID</th>
<th>Process</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>272</td>
<td>topoDPC</td>
<td>20</td>
<td>2</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>270</td>
<td>bcmNHOP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>269</td>
<td>bcmDISC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>268</td>
<td>bcmATP-RX</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>267</td>
<td>bcmATP-TX</td>
<td>30</td>
<td>3</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>266</td>
<td>bcmSTACK</td>
<td>380</td>
<td>38</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>265</td>
<td>bcmRX</td>
<td>30</td>
<td>3</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>264</td>
<td>bcmLINK.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>263</td>
<td>bcmXGS3AsyncTX</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>262</td>
<td>bcmTX</td>
<td>160</td>
<td>16</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>260</td>
<td>bcmCNTR.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>253</td>
<td>bcmDPC</td>
<td>10690</td>
<td>1069</td>
<td>10000</td>
<td>0</td>
<td>10</td>
<td>2.97</td>
<td>0</td>
</tr>
<tr>
<td>251</td>
<td>sysd</td>
<td>2380</td>
<td>238</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0.50</td>
<td>0</td>
</tr>
<tr>
<td>58</td>
<td>kfldintr</td>
<td>30</td>
<td>3</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>36</td>
<td>sh</td>
<td>50</td>
<td>5</td>
<td>10000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

!-------- output truncated -------------!
```
**Example 3**  
**Figure 5-39. Command Example: show processes cpu stack-unit on S-Series**

```
FTOS#show processes cpu stack-unit 0

CPU Statistics On Unit0 Processor

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime(ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>8260</td>
<td>826</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.22%</td>
<td>0</td>
<td>sysd</td>
</tr>
<tr>
<td>116</td>
<td>70</td>
<td>7</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>xstp</td>
</tr>
<tr>
<td>109</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>
<td>span</td>
</tr>
<tr>
<td>108</td>
<td>60</td>
<td>6</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>span</td>
</tr>
<tr>
<td>103</td>
<td>70</td>
<td>7</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>igmp</td>
</tr>
<tr>
<td>100</td>
<td>70</td>
<td>7</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>mrtm</td>
</tr>
<tr>
<td>96</td>
<td>70</td>
<td>7</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>12mgr</td>
</tr>
<tr>
<td>92</td>
<td>100</td>
<td>10</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>12pm</td>
</tr>
<tr>
<td>86</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>
<td>arpm</td>
</tr>
<tr>
<td>83</td>
<td>40</td>
<td>4</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ospf</td>
</tr>
<tr>
<td>80</td>
<td>100</td>
<td>10</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>dsm</td>
</tr>
<tr>
<td>74</td>
<td>60</td>
<td>6</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>rtm</td>
</tr>
<tr>
<td>70</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>
<td>rip</td>
</tr>
<tr>
<td>68</td>
<td>120</td>
<td>12</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ism</td>
</tr>
<tr>
<td>64</td>
<td>70</td>
<td>7</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>acl</td>
</tr>
<tr>
<td>63</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>
<td>bcmLINK.1</td>
</tr>
<tr>
<td>62</td>
<td>290</td>
<td>29</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>bcmCNTR.1</td>
</tr>
<tr>
<td>61</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>
<td>bcmRX</td>
</tr>
<tr>
<td>60</td>
<td>40</td>
<td>4</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>bcmLINK.0</td>
</tr>
<tr>
<td>59</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>bcmXGS3AsynctX</td>
</tr>
<tr>
<td>58</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>bcmTX</td>
</tr>
<tr>
<td>57</td>
<td>340</td>
<td>34</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>bcmCNTR.0</td>
</tr>
<tr>
<td>55</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>bcmDPC</td>
</tr>
<tr>
<td>117</td>
<td>60</td>
<td>6</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>frpr</td>
</tr>
<tr>
<td>28</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>inetd</td>
</tr>
<tr>
<td>21</td>
<td>450</td>
<td>45</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>mount_mfs</td>
</tr>
<tr>
<td>18</td>
<td>130</td>
<td>13</td>
<td>10000</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>mount_mfs</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>syslogd</td>
</tr>
<tr>
<td>6</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>
<td>sh</td>
</tr>
<tr>
<td>5</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>
<td>aioldoned</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>ioflush</td>
</tr>
<tr>
<td>3</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>
<td>reaper</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>pagedaemon</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>init</td>
</tr>
<tr>
<td>0</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>
<td>swapper</td>
</tr>
</tbody>
</table>
```
### Example 4

**Figure 5-40. Command Example: show processes memory on S-Series**

```
FTOS#show processes memory
Memory Statistics On Unit 0 Processor (bytes)
------------------------------------------
start
Total      :   160231424, MaxUsed    :   130596864 [09/19/2007 03:11:17]
CurrentUsed:   130560000, CurrentFree:    29671424
SharedUsed :   14261872, SharedFree :   6709672
PID   Process        ResSize       Size       Allocs       Frees        Max       Current
124 KernLrnAgMv    140410880           0           0           0           0           0           0
117 xstp           5677056       217088       87650       0             0             0             0
116 xstp           7587592       1536000      551812       49692       518684           0           0
109 span           5709824       221184       55386       0             53586           0           0
108 pim            5869568       720896       12300       0             12300           0           0
103 igmp           553216       327680       18236       16564       18236           0           0
100 mrtm           6098586       516096       72846       0             72846           0           0
96 12mgr           6107136       491520     254858       115948       170238           0           0
92 12pm            5607424       221184       667578       579470       120966           0           0
86 arpm            533472       208896       54528       16564       54528           0           0
83 ospf            4210688       475136       0             0             0           0           0
80 dsm             6057984       552960       22838       0             22838           0           0
74 rtm             6311936       577536       574972       298152       376024           0           0
70 rip              5001216       249856       528           0             528           0           0
68 ipml            5292032       339696       67224       67224           0           0           0
64 acl             5607424       544768       140866       66256           0           0           0
62 bcmCNTR.1 140410880           0           0           0           0           0           0
61 bcmRX           140410880           0           0           0           0           0           0
60 bcmLINK.0 140410880           0           0           0           0           0           0
59 bcmXGS3AsyncTX 140410880           0           0           0           0           0           0
58 bcmFX           140410880           0           0           0           0           0           0
57 bcmCNTR.0 140410880           0           0           0           0           0           0
55 bcmDPC          140410880           0           0           0           0           0           0
52 sysd           44650496       22876160       393086       1358248       2589172           0           0
28 inetd        22642688       1953792           0           0           0           0           0
21 mount_mfs      22642688       1953792           0           0           0           0           0
!----output truncated ------------------!
```

### Example 5

**Figure 5-41. Command Example: show processes memory stack-unit on S-Series**

```
FTOS#show processes memory stack-unit 0
Memory Statistics On Unit 0 Processor (bytes)
------------------------------------------
start
Total      :   160231424, MaxUsed    :   130596864 [09/19/2007 03:11:17]
CurrentUsed:   130560000, CurrentFree:    29671424
SharedUsed :   14261872, SharedFree :   6709672
PID   Process        ResSize       Size       Allocs       Frees        Max       Current
124 KernLrnAgMv    140410880           0           0           0           0           0           0
117 xstp           5677056       217088       87650       0             0             0             0
116 xstp           7587592       1536000      551812       49692       518684           0           0
109 span           5709824       221184       55386       0             53586           0           0
108 pim            5869568       720896       12300       0             12300           0           0
103 igmp           553216       327680       18236       16564       18236           0           0
100 mrtm           6098586       516096       72846       0             72846           0           0
96 12mgr           6107136       491520     254858       115948       170238           0           0
92 12pm            5607424       221184       667578       579470       120966           0           0
86 arpm            533472       208896       54528       16564       54528           0           0
83 ospf            4210688       475136       0             0             0           0           0
80 dsm             6057984       552960       22838       0             22838           0           0
74 rtm             6311936       577536       574972       298152       376024           0           0
70 rip              5001216       249856       528           0             528           0           0
68 ipml            5292032       339696       67224       67224           0           0           0
!----output truncated ------------------!
```

### Related Commands

- `show hardware layer2 acl`: Display Layer 2 ACL data for the selected stack member and stack member port-pipe.
- `show hardware layer3`: Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.
- `show hardware stack-unit`: Display the data plane or management plane input and output statistics of the designated component of the designated stack member.
show processes ipc flow-control

Display the Single Window Protocol Queue (SWPQ) statistics.

Syntax

show processes ipc flow-control [cp | rp1 | rp2 | lp linecard-number]

Parameters

- **cp**: (OPTIONAL) Enter the keyword `cp` to view the Control Processor’s SWPQ statistics.
- **rp1**: (OPTIONAL) Enter the keyword `rp1` to view the Control Processor’s SWPQ statistics on Route Processor 1.*
- **rp2**: (OPTIONAL) Enter the keyword `rp2` to view the Control Processor’s SWPQ statistics on Route Processor 2.*
- **lp linecard-number**: (OPTIONAL) Enter the keyword `lp` followed by the line card number to view the Control Processor’s SWPQ statistics on the specified line card.*

* In the S-Series, this command supports only the `cp` keyword, not the `rp1`, `rp2`, and `lp` options. See Figure 5-46.

Defaults

No default values or behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series and E-Series
### Example 1  Figure 5-42. Command Example: show processes ipc flow-control from C-Series

```
FTOS# show processes ipc flow-control cp

Q Statistics on CP Processor
TxProcess  RxProcess  Cur   High  Time  Retr  Mag    Ack  Aval  Max
Len    Mark   Out    ies    Sent   Rcvd Retra Retra
ACL0     RTM0    0      0     0      0     0       0    10    10
ACL0     DIFFSERV0    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
ACL0     ACL20     0      1     0      2     2       2    50    50
CFG0    CFGDATASYNC0    0      2     0      7     7       7    255   255
DHCP0    ACL0     0      1     0      9     9       9    25    25
DHCP0    IPMGR0    0      0     0      0     0       0    25    25
RTM0     ARPMGR0    0      1     0      1     1       1    136   136
ACL20    IGMP0    0      0     0      0     0       0    50    50
ARPMGR0    IFMGR0    0      2     0      4     4       4    25    25
ACL20    PIM0     0      0     0      0     0       0    50    50
MACMGR0  ACL0     0      1     0      1     1       1    25    25
TCLASSMGR0    ARPMGR0    0      0     0      0     0       0    100   100
IFMGR0    IPMGR2    0      6     0      44     44      44    8     8

!--------------------------output truncated ---------------------------------!
```

### Example 2  Figure 5-43. Command Example: show processes ipc flow-control rp from E-Series

```
FTOS# show processes ipc flow-control cp

Q Statistics on CP Processor
TxProcess  RxProcess  Cur   High  Time  Retr  Mag    Ack  Aval  Max
Len    Mark   Out    ies    Sent   Rcvd Retra Retra
DHCP0    ACL0     0      1     0      6     6       6    25    25
DHCP0    IPMGR0    0      0     0      0     0       0    25    25
IFMGR0    FEFD0    0      3     0      27    27      27    8     8
IFMGR0    IPMGR0    0      6     0      44     44      44    8     8
IFMGR0    SNMP0    0      1     0      16    16      16    8     8
IFMGR0    SFL_CP0    0      4     0      31    31      31    8     8
IFMGR0    EVENTTERMLOG0    0      1     0      6     6       6    8     8
IFMGR0    PORTMIRRO0    0      0     0      0     0       0    8     8
IFMGR0    DHCP0    0      1     0      6     6       6    8     8
IFMGR0    TCLASSMGR0    0      2     0      13    13      13    8     8
IFMGR0    VRRP0     0      3     0      25    25      25    8     8
IFMGR0    MRTM0     0      2     0      21    21      21    8     8
TCLASSMGR0    ARPMGR0    0      0     0      0     0       0    100   100
IFMGR0    IPMGR2    0      6     0      44     44      44    8     8

!--------------------------output truncated ---------------------------------!
```
Table 5-4 list the definitions of the fields shown in Figure 5-42 and Figure 5-43.

Table 5-4. Description of show processes ipc flow-control cp output

<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>
<tr>
<td>Retr /Available Retra</td>
<td>Number of retries left</td>
</tr>
<tr>
<td>Total/ Max Retra</td>
<td>Number of retries allowed</td>
</tr>
</tbody>
</table>

Example 2

Figure 5-44. Command Example: show processes ipc flow-control rp

FTOS# show processes ipc flow-control rp2

```
[qid] Source->Dest       Cur High #of #of  #msg   #msg Retr total
Len Mark to Retr Sent   Ackd
--------------------------------------------------------------------
[1] unknown2->unknown2   0    0   0   0    0      0    3    3
[2] l2pm0->spanMgr0      0    2   0   0    2298   2298 25   25
[3] fvrp0->macMGr0        0    0   0   0    0      0    25   25
[4] l2pm0->fvrp0          0    2   0   0    1905   1905 25   25
[5] fvrp0->l2pm0          0    0   0   0    0      0    25   25
[6] stp0->l2pm0           0    0   0   0    0      0    25   25
[7] spanMgr0->macMGr0     0    0   0   0    0      0    25   25
[8] spanMgr0->lpMGr0      0    0   0   0    0      0    25   25
```

Example 3

Figure 5-45. Command Example: show processes ipc flow-control lp

FTOS#show processes ipc flow-control lp 10

```
Q Statistics on LP 10
TxProcess RxProcess Cur Len High Mark Time Retries Msg Sent Ack Rcvd Aval Retra Max Retra
ACL_AGENT10    PIM0          0    0    0    0    0    0    20    20
ACL_AGENT10    PIM0          0    0    0    0    0    0    20    20
FRRPAGT10      FRRP0         0    0    0    0    0    0    30    30
LPDMACAGENT10  IPMGR0       0    1    0    0    1    1    8     8
FTOS#
```
Example 4  Figure 5-46. Command Example: show processes ipc flow-control on S-Series

```
FTOS#show processes ipc flow-control
Q Statistics on CP Processor

<table>
<thead>
<tr>
<th>TxProcess</th>
<th>RxProcess</th>
<th>Cur Len</th>
<th>High Mark</th>
<th>Time Out</th>
<th>Retr ies</th>
<th>Mag Sent</th>
<th>Ack Rcvd</th>
<th>Aval Retra Max Retra</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL0</td>
<td>RTM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 10 10</td>
</tr>
<tr>
<td>ACL0</td>
<td>DIFFSERV0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 10 10</td>
</tr>
<tr>
<td>ACL0</td>
<td>IGP0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 10 10</td>
</tr>
<tr>
<td>ACL0</td>
<td>PIM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 10 10</td>
</tr>
<tr>
<td>LACP0</td>
<td>IFMGR0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 25 25</td>
</tr>
<tr>
<td>RTM0</td>
<td>ARPMAK0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 136 136</td>
</tr>
<tr>
<td>MACMGR0</td>
<td>ACL0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 25 25</td>
</tr>
<tr>
<td>ARPMGR0</td>
<td>RTM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 100 100</td>
</tr>
<tr>
<td>DHCP0</td>
<td>ACL0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1 25 25</td>
</tr>
<tr>
<td>DHCP0</td>
<td>IFMGR0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 25 25</td>
</tr>
<tr>
<td>L2PM0</td>
<td>SPANMGR0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>14</td>
<td>14</td>
<td>14 25 25</td>
</tr>
<tr>
<td>ARPMAK0</td>
<td>FIBAGT0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1 100 100</td>
</tr>
<tr>
<td>SPANMGR0</td>
<td>MACMGR0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 25 25</td>
</tr>
<tr>
<td>SPANMGR0</td>
<td>IFMGR0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 25 25</td>
</tr>
<tr>
<td>MACMGR0</td>
<td>L2PM0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 25 25</td>
</tr>
<tr>
<td>STP0</td>
<td>L2PM0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>5 25 25</td>
</tr>
<tr>
<td>RTM0</td>
<td>FIBAGT0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4 255 255</td>
</tr>
<tr>
<td>L2PM0</td>
<td>STP0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>13</td>
<td>13 25 25</td>
</tr>
<tr>
<td>ACL_AGENT0</td>
<td>PIM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 20 20</td>
</tr>
<tr>
<td>ACL_AGENT0</td>
<td>FRRP0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 20 20</td>
</tr>
<tr>
<td>FRRP0</td>
<td>L2PM0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>13</td>
<td>13 25 25</td>
</tr>
<tr>
<td>L2PM0</td>
<td>FRRP0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 25 25</td>
</tr>
<tr>
<td>ACL0</td>
<td>ACL_AGENT0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>7</td>
<td>7 90 90</td>
</tr>
<tr>
<td>ACL0</td>
<td>MACAGENT0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 90 90</td>
</tr>
<tr>
<td>IFMGR0</td>
<td>EVENTTERM0LOGO</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1 8 8</td>
</tr>
<tr>
<td>IFMGR0</td>
<td>SNMP0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1 8 8</td>
</tr>
<tr>
<td>IFMGR0</td>
<td>IFMGR0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>9</td>
<td>9 8 8</td>
</tr>
<tr>
<td>IFMGR0</td>
<td>DIFFSERV0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3 8 8</td>
</tr>
<tr>
<td>DIFFSERV0</td>
<td>ACL_AGENT0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 100 100</td>
</tr>
</tbody>
</table>

!---------------output truncated --------------------------!
```

Usage Information

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 5-46, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

show processes memory (C-Series and E-Series)

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

Syntax

```
show processes memory [cp | lp slot-number | lp all | lp summary] [rp1 | rp2]
```

```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp</td>
<td>(OPTIONAL) Enter the keyword cp to view memory usage of the Control Processor.</td>
</tr>
</tbody>
</table>
| lp slot-number | (OPTIONAL) Enter the keyword lp and the slot number to view information on the line-card processor in that slot.  
C-Series Range: 0-7  
E-Series Range: 0 to 13 on a E1200/E1200i, 0 to 6 on a E6000/E6000i, and 0 to 5 on a E300. |
| lp all | (OPTIONAL) Enter the keyword lp all to view CP memory usage on all active line cards. |
| lp summary | (OPTIONAL) Enter the keyword lp summary to view a summary of the line card CP memory usage. |
| rp1 | (OPTIONAL) Enter the keyword rp1 to view memory usage of the Route Processor 1.  
Note: This option is supported on the E-Series only. |
| rp2 | (OPTIONAL) Enter the keyword rp2 to view memory usage of the Route Processor 2.  
Note: This option is supported on the E-Series only. |

Command Modes

- EXEC
- EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.2</td>
<td>Introduced on E-Series ExaScale E600i</td>
<td></td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale E1200i</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
<td></td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added lp all and lp summary options</td>
<td></td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>For rp1 and rp2 only, the output displays memory consumption of all the processes including a summary (see Figure 5-48 and Figure 5-49).</td>
<td></td>
</tr>
</tbody>
</table>

Usage Information

The output for show process memory 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 C-Series’ and E-Series' CP.

In Dell Networking OS Release 7.4.1.0 and higher, the total counter size (for all 3 CPUs) in show memory and show processes memory will differ based on which Dell Networking OS processes are counted.

- In the show memory (C-Series and E-Series) display output, the memory size is equal to the size of the application processes.
- In the show processes memory (C-Series and E-Series) display output, the memory size is equal to the size of the application processes plus the size of the system processes.
### Example Figure 5-47. Command Example: show processes memory (partial)

FTOS#show processes memory
Memory Statistics On CP Processor (bytes)

<table>
<thead>
<tr>
<th>TaskName</th>
<th>TotalAllocated</th>
<th>TotalFreed</th>
<th>MaxHeld</th>
<th>CurrentHolding</th>
</tr>
</thead>
<tbody>
<tr>
<td>tRootTask</td>
<td>39083408</td>
<td>1395840</td>
<td>38143920</td>
<td>37687568</td>
</tr>
<tr>
<td>tARL</td>
<td>64</td>
<td>0</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>tBcmTask</td>
<td>256</td>
<td>0</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>tPortmapd</td>
<td>18560</td>
<td>0</td>
<td>18560</td>
<td>18560</td>
</tr>
<tr>
<td>tShell</td>
<td>3440</td>
<td>0</td>
<td>3440</td>
<td>3440</td>
</tr>
<tr>
<td>tPingTmo0</td>
<td>0</td>
<td>1088</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tExcTask</td>
<td>0</td>
<td>592864</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tme</td>
<td>4002494</td>
<td>192</td>
<td>4002302</td>
<td>4002302</td>
</tr>
<tr>
<td>ipc</td>
<td>3460</td>
<td>0</td>
<td>3460</td>
<td>3460</td>
</tr>
<tr>
<td>irc</td>
<td>943436</td>
<td>0</td>
<td>943436</td>
<td>943436</td>
</tr>
<tr>
<td>RpmAvailMgr</td>
<td>9376</td>
<td>32</td>
<td>9344</td>
<td>9344</td>
</tr>
<tr>
<td>ev</td>
<td>133188</td>
<td>0</td>
<td>133188</td>
<td>133188</td>
</tr>
<tr>
<td>evterm</td>
<td>26752</td>
<td>0</td>
<td>26752</td>
<td>26752</td>
</tr>
<tr>
<td>evhdlr</td>
<td>2528</td>
<td>8064</td>
<td>2528</td>
<td>0</td>
</tr>
<tr>
<td>dlm</td>
<td>7556256</td>
<td>7366960</td>
<td>1239104</td>
<td>189296</td>
</tr>
<tr>
<td>dla</td>
<td>416</td>
<td>0</td>
<td>416</td>
<td>416</td>
</tr>
<tr>
<td>tsm</td>
<td>15136</td>
<td>0</td>
<td>15136</td>
<td>15136</td>
</tr>
<tr>
<td>fmg</td>
<td>766560</td>
<td>0</td>
<td>766560</td>
<td>766560</td>
</tr>
<tr>
<td>sysProc</td>
<td>40208</td>
<td>0</td>
<td>40208</td>
<td>40208</td>
</tr>
</tbody>
</table>

### Example Figure 5-48. Command Example: show processes memory rp1

FTOS#show processes memory rp1

<table>
<thead>
<tr>
<th>PID</th>
<th>Process</th>
<th>ResSize</th>
<th>Size</th>
<th>Allocs</th>
<th>Frees</th>
<th>Max</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>124</td>
<td>ospf</td>
<td>3215360</td>
<td>425984</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>119</td>
<td>dsm</td>
<td>7749632</td>
<td>1859584</td>
<td>797026</td>
<td>0</td>
<td>797026</td>
<td>797026</td>
</tr>
<tr>
<td>114</td>
<td>ipmi</td>
<td>3821568</td>
<td>229376</td>
<td>297324</td>
<td>0</td>
<td>297324</td>
<td>297324</td>
</tr>
<tr>
<td>112</td>
<td>rtm</td>
<td>4722688</td>
<td>421888</td>
<td>925008</td>
<td>0</td>
<td>925008</td>
<td>925008</td>
</tr>
<tr>
<td>107</td>
<td>rip</td>
<td>3731456</td>
<td>253952</td>
<td>198216</td>
<td>0</td>
<td>198216</td>
<td>198216</td>
</tr>
<tr>
<td>104</td>
<td>acl</td>
<td>4734976</td>
<td>430080</td>
<td>1127524</td>
<td>0</td>
<td>1127524</td>
<td>1127524</td>
</tr>
<tr>
<td>100</td>
<td>sysdl1</td>
<td>11636736</td>
<td>2019328</td>
<td>965798</td>
<td>0</td>
<td>965798</td>
<td>965798</td>
</tr>
<tr>
<td>98</td>
<td>asyom</td>
<td>528384</td>
<td>94208</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>36</td>
<td>sshd</td>
<td>1286144</td>
<td>430080</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>34</td>
<td>inetsd</td>
<td>663552</td>
<td>98304</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>32</td>
<td>mount_mfs</td>
<td>4239796</td>
<td>2514944</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>mount_mfs</td>
<td>364544</td>
<td>2449048</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>ash</td>
<td>446444</td>
<td>737280</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>aiomoned</td>
<td>76529664</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>ioflush</td>
<td>76529664</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>reaper</td>
<td>76529664</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>pagedaemon</td>
<td>76529664</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>init</td>
<td>139264</td>
<td>2375680</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>swapper</td>
<td>76529664</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Example

**Figure 5-49. Command Example: show processes memory rp2**

```plaintext
FTOS#show processes memory rp2
CurrentUsed : 149417984, CurrentFree : 804282368
SharedUsed : 7847200, SharedFree : 13124344

<table>
<thead>
<tr>
<th>PID</th>
<th>Process</th>
<th>ResSize</th>
<th>Size</th>
<th>Allocs</th>
<th>Frees</th>
<th>Max</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>145</td>
<td>vrrp</td>
<td>3870720</td>
<td>266240</td>
<td>297324</td>
<td>0</td>
<td>297324</td>
<td>297324</td>
</tr>
<tr>
<td>141</td>
<td>fvrp</td>
<td>4472832</td>
<td>204800</td>
<td>797010</td>
<td>0</td>
<td>797010</td>
<td>797010</td>
</tr>
<tr>
<td>138</td>
<td>xstp</td>
<td>10764288</td>
<td>7155712</td>
<td>367534</td>
<td>0</td>
<td>367534</td>
<td>367534</td>
</tr>
<tr>
<td>133</td>
<td>span</td>
<td>4136960</td>
<td>167936</td>
<td>565810</td>
<td>0</td>
<td>565810</td>
<td>565810</td>
</tr>
<tr>
<td>132</td>
<td>pim</td>
<td>6664192</td>
<td>516096</td>
<td>2812528</td>
<td>0</td>
<td>2812528</td>
<td>2812528</td>
</tr>
<tr>
<td>128</td>
<td>lpm2</td>
<td>4112384</td>
<td>344064</td>
<td>627684</td>
<td>0</td>
<td>627684</td>
<td>627684</td>
</tr>
<tr>
<td>124</td>
<td>lpm2</td>
<td>3923968</td>
<td>237568</td>
<td>363396</td>
<td>0</td>
<td>363396</td>
<td>363396</td>
</tr>
<tr>
<td>120</td>
<td>mtm</td>
<td>25567232</td>
<td>593920</td>
<td>697790</td>
<td>0</td>
<td>697790</td>
<td>697790</td>
</tr>
<tr>
<td>116</td>
<td>l2mgr</td>
<td>4579328</td>
<td>20192</td>
<td>830098</td>
<td>0</td>
<td>830098</td>
<td>830098</td>
</tr>
<tr>
<td>112</td>
<td>l2pm</td>
<td>3874816</td>
<td>225280</td>
<td>367446</td>
<td>32948</td>
<td>367446</td>
<td>334498</td>
</tr>
<tr>
<td>108</td>
<td>arpm</td>
<td>3702784</td>
<td>208962</td>
<td>268420</td>
<td>0</td>
<td>268420</td>
<td>268420</td>
</tr>
<tr>
<td>104</td>
<td>acl2</td>
<td>3485696</td>
<td>94208</td>
<td>132144</td>
<td>0</td>
<td>132144</td>
<td>132144</td>
</tr>
<tr>
<td>100</td>
<td>sysd2</td>
<td>11657216</td>
<td>1679360</td>
<td>998834</td>
<td>0</td>
<td>998834</td>
<td>998834</td>
</tr>
<tr>
<td>98</td>
<td>sysmon</td>
<td>528384</td>
<td>94208</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>36</td>
<td>sshd</td>
<td>1286144</td>
<td>430080</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>34</td>
<td>inetd</td>
<td>663552</td>
<td>98304</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>32</td>
<td>mount_mfs</td>
<td>41791488</td>
<td>2514944</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>mount_mfs</td>
<td>364544</td>
<td>2449408</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>sh</td>
<td>446464</td>
<td>737280</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>aiodoned</td>
<td>76967936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>ioflush</td>
<td>76967936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>reaper</td>
<td>76967936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>pagedaemon</td>
<td>76967936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>init</td>
<td>139264</td>
<td>2375680</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>swapper</td>
<td>76967936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Table 5-5 defines the fields that appear in the show processes memory output.**

**Table 5-5. Descriptions of show processes memory rp1/rp2 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>
<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 processes memory (S-Series)

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

Syntax

```
show processes memory {management-unit | stack unit {0–7 | all | summary}}
```

Parameters

- `management-unit` Enter the keyword `management-unit` for CPU memory usage of the stack management unit.
- `stack unit 0–7` 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Modified: Added management-unit option</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

Usage Information

The output for show process memory 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 S-Series’ CP.

For S-Series, the output of `show memory` and this command will differ based on which Dell Networking OS 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 5-50. Command Example: show processes memory on S-Series

FTOS#show processes memory stack-unit 0
Total: 268435456, MaxUsed: 2420244, CurrentUsed: 2420244, CurrentFree: 266015212

TaskName       TotalAllocated  TotalFreed  MaxHeld  CurrentHolding
  tme           435406         397536      54434    37870
  ipc           16652          0          16652     16652
  timerMgr      33216          0          33216     33216
  sysAdmTsk     33216          0          33216     33216
  tFib4         1943960        0          1943960   1943960
  aclAgent      90770          16564       74206    74206
  ifagt_1       21318          16564       21318    4754
  dsagt         6504           0          6504      6504
  MacAgent      269778         0          269778    269778
```
Example

Figure 5-51. Command Example: show processes memory management-unit

FTOS#show processes management-unit

CurrentUsed: 98840768, CurrentFree: 53088256
SharedUsed: 13007848, SharedFree: 7963696

<table>
<thead>
<tr>
<th>PID</th>
<th>Process</th>
<th>ResSize</th>
<th>Size</th>
<th>Allocs</th>
<th>Frees</th>
<th>Max</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>337</td>
<td>KernLrnAgMv</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>331</td>
<td>vrrp</td>
<td>5189632</td>
<td>249856</td>
<td>50572</td>
<td>0</td>
<td>50572</td>
<td>50572</td>
</tr>
<tr>
<td>323</td>
<td>frpr</td>
<td>5206016</td>
<td>241664</td>
<td>369238</td>
<td>0</td>
<td>369238</td>
<td>369238</td>
</tr>
<tr>
<td>322</td>
<td>xstp</td>
<td>7430144</td>
<td>2928640</td>
<td>38228</td>
<td>0</td>
<td>38228</td>
<td>38228</td>
</tr>
<tr>
<td>321</td>
<td>pim</td>
<td>5267456</td>
<td>823296</td>
<td>62168</td>
<td>0</td>
<td>62168</td>
<td>62168</td>
</tr>
<tr>
<td>314</td>
<td>igmp</td>
<td>4960256</td>
<td>380928</td>
<td>18588</td>
<td>16564</td>
<td>18588</td>
<td>2024</td>
</tr>
<tr>
<td>313</td>
<td>mrtm</td>
<td>6742016</td>
<td>1130496</td>
<td>72758</td>
<td>0</td>
<td>72758</td>
<td>72758</td>
</tr>
<tr>
<td>308</td>
<td>l2mgr</td>
<td>5607424</td>
<td>552960</td>
<td>735214</td>
<td>380972</td>
<td>619266</td>
<td>354242</td>
</tr>
<tr>
<td>311</td>
<td>12pm</td>
<td>5001216</td>
<td>1429522</td>
<td>1176044</td>
<td>286606</td>
<td>253478</td>
<td></td>
</tr>
<tr>
<td>298</td>
<td>arpm</td>
<td>4628480</td>
<td>217088</td>
<td>71092</td>
<td>33128</td>
<td>71092</td>
<td>37964</td>
</tr>
<tr>
<td>294</td>
<td>ospf</td>
<td>5468160</td>
<td>503808</td>
<td>724204</td>
<td>662560</td>
<td>78208</td>
<td>61644</td>
</tr>
<tr>
<td>288</td>
<td>dsm</td>
<td>6778880</td>
<td>1159168</td>
<td>39490</td>
<td>16564</td>
<td>39490</td>
<td>22926</td>
</tr>
<tr>
<td>287</td>
<td>rtm</td>
<td>513920</td>
<td>442280</td>
<td>198768</td>
<td>376024</td>
<td>243512</td>
<td></td>
</tr>
<tr>
<td>284</td>
<td>rip</td>
<td>4562944</td>
<td>258048</td>
<td>528</td>
<td>0</td>
<td>528</td>
<td>528</td>
</tr>
<tr>
<td>281</td>
<td>lacp</td>
<td>4673536</td>
<td>266240</td>
<td>221060</td>
<td>0</td>
<td>221060</td>
<td>221060</td>
</tr>
<tr>
<td>287</td>
<td>ipml</td>
<td>4837376</td>
<td>380928</td>
<td>83788</td>
<td>0</td>
<td>83788</td>
<td>83788</td>
</tr>
<tr>
<td>273</td>
<td>acl</td>
<td>5005312</td>
<td>239564</td>
<td>149076</td>
<td>123616</td>
<td>90488</td>
<td></td>
</tr>
<tr>
<td>272</td>
<td>topoDPC</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>271</td>
<td>bcmNHOP</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>270</td>
<td>bcmDISC</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>269</td>
<td>bcmATP-RX</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>268</td>
<td>bcmATP-TX</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>267</td>
<td>bcmSTACK</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>266</td>
<td>bcmRX</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>265</td>
<td>bcmLINK.0</td>
<td>117927936</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

!--------- output truncated ---------!

Table 5-6 defines the fields that appear in the show processes memory output.

Table 5-6. 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>
<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 processes switch-utilization

Show switch fabric utilization.

Syntax

show processes switch-utilization

Command Mode

EXEC
EXEC Privilege

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale
E-Series original Command

Example

Figure 5-52. Command Example: show processes switch-utilization

FTOS#show processes switch-utilization

Switch fabric utilization 5Sec 1Min 5Min
----------------------------------------
                                           3%  3%  3%

Usage Information

An asterisk ( * ) in the output indicates a legacy card that is not support by the show processes switch-utilization command.

show rpm

Show the current RPM status.

Syntax

show rpm [number [brief] | all]

Parameters

number  (OPTIONAL) Enter either zero (0) or 1 for the RPM.
all     (OPTIONAL) Enter the keyword all to view a table with information on all present RPMs.
brief   (OPTIONAL) Enter the keyword brief to view an abbreviated list of RPM information.

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.5.1.0 Introduced on C-Series
E-Series original Command
show rpm 0
-- RPM card 0 --
Status : active
Next Boot : online
Card Type : RPM - Route Processor Module (LC-EF-RPM)
Hardware Rev : 2.2i
Num Ports : 1
Up Time : 4 min, 37 sec
Last Restart : reset by user
Dell Networking OS Version : 8-4-2-399
Jumbo Capable : yes
CP Boot Flash : A: 2.4.2.2 [booted] B: 2.4.2.2
RP1 Boot Flash: A: 2.4.2.2 B: 2.4.2.2 [booted]
RP2 Boot Flash: A: 2.4.2.2 B: 2.4.2.2 [booted]
CP Mem Size : 536870912 bytes
RP1 Mem Size : 1073741824 bytes
RP2 Mem Size : 1073741824 bytes
MMC Mem Size : 511680512 bytes
External MMC : n/a
Temperature : 46C
Power Status : PEM0: absent or down PEM1: up
Voltage : ok
Serial Number : FX000040917
Part Number : 7520017200 Rev 01
Vendor Id : 04
Date Code : 02072005
Country Code : 01
Piece Part ID : US-0RVY43-76991-82B-0456
PPID Revision : 1B2
Service Tag : SVCTGCH
Expr Svc Code : 628 458 864 65
FTOS#
### Figure 5-54. Command Example: show rpm on C-Series

FTOS#show rpm 0
-- RPM card 0 --
Status : active
Next Boot : online
Card Type : RPM - Route Processor Module (LC-CB-RPM)
Hardware Rev : 2.0
Num Ports : 1
Up Time : 1 min, 58 sec
Last Restart : reset by user
Dell Networking OS Version : 8-4-2-399
Jumbo Capable : yes
CP Boot Flash : A: 2.7.1.1 [booted] B: 2.7.1.1
CP FPGA Flash : A: 5.0
CP Mem Size : 1073741824 bytes
MMC Mem Size : 511467520 bytes
External MMC : n/a
Temperature : 43C
Power Status : AC
Voltage : ok
Serial Number : FX000037575
Part Number : 7520029307 Rev 02
Vendor Id : Y
Date Code : 01342008
Country Code : 01
Piece Part ID : US-0T4VKT-76991-1BA-7575
PPID Revision : 002
Service Tag : SRVCTG9
Expr Svc Code : 626 351 582 97

### Table 5-7. Descriptions of show rpm output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays the RPM’s status.</td>
</tr>
<tr>
<td>Next Boot</td>
<td>Displays whether the RPM is to be brought online at the next system reload.</td>
</tr>
<tr>
<td>Card Type</td>
<td>Displays the RPM catalog number.</td>
</tr>
<tr>
<td>Hardware Rev</td>
<td>Displays the E-Series chipset hardware revision level: 1.0 (non-Jumbo); 1.5</td>
</tr>
<tr>
<td></td>
<td>(Jumbo-enabled); 2.0 (or above is TeraScale).</td>
</tr>
<tr>
<td>Num Ports</td>
<td>Displays the number of active ports.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Displays the number of hours and minutes since the RPM’s last reboot.</td>
</tr>
</tbody>
</table>
### Table 5-7. Descriptions of show rpm output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Last Restart    | States the reason for the last RPM reboot. C-Series possible values:  
• “normal power-cycle” (**reset power-cycle** command)  
• “reset by master” (peer RPM reset by master RPM)  
• “over temperature shutdown”  
• “power supply failed”  
E-Series possible values:  
• “normal power-cycle” (insufficient power, normal power cycle)  
• “reset by user” (automatic failover, software reload of both RPMs, or master RPM resetting peer)  
• “force-failover” (**redundancy force-failover** command) |
| Dell Networking OS Version | Displays the operating software version. |
| Jumbo Capable    | Displays a Yes or No indicating if the RPM is capable of sending and receiving Jumbo frames. This field does not indicate if the chassis is in Jumbo mode; for that determination, use the **show chassis brief** command. |
| CP Boot Flash    | Displays the two possible Boot Flash versions for the Control Processor. The [Booted] keyword next to the version states which version was used at system boot. |
| RP1 Boot Flash   | Displays the two possible Boot Flash versions for the Routing Processor 1. The [Booted] keyword next to the version states which version was used at system boot. |
| RP2 Boot Flash   | Displays the two possible Boot Flash versions for the Routing Processor 2. The [Booted] keyword next to the version states which version was used at system boot. |
| CP Mem Size      | Displays the memory of the Control Processor. |
| RP1 Mem Size     | Displays the memory of the Routing Processor 1. |
| PR2 Mem Size     | Displays the memory of the Routing Processor 2. |
| Temperature      | Displays the temperature of the RPM. Minor alarm status if temperature is over 65° C. |
| Power Status     | Lists the status of the power modules in the chassis. |
| Voltage          | Displays the power rails for the line card. |
| Serial Num       | Displays the line card serial number. |
| Part Num         | Displays the line card part number. |
| Vendor ID        | Displays an internal code, which specifies the manufacturing vendor. |
| Date Code        | Displays the line card’s manufacturing date. |
| Country Code     | Displays the country of origin.  
01 = USA |

**Related Commands**

- **show chassis** View information on all elements of the system.
- **show linecard** View information on a line card.
- **show sfm** View information on the SFM.
**show software ifm**

Display interface management (IFM) data.

**Syntax**

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clients</td>
<td>Enter the keyword <code>clients</code> to display IFM client information.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword <code>summary</code> to display brief information about IFM clients.</td>
</tr>
<tr>
<td>ifagt number</td>
<td>Enter the keyword <code>ifagt</code> 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 <code>ifcb</code> 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 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code>.</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>C-Series and S-Series: Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For a 10G Ethernet interface, enter the keyword <code>TenGigabitEthernet</code>.</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>C-Series options also include:</td>
</tr>
<tr>
<td></td>
<td>• <code>fastethernet</code> for a Fast Ethernet interface</td>
</tr>
<tr>
<td></td>
<td>• <code>loopback</code> for a Loopback interface</td>
</tr>
<tr>
<td></td>
<td>• <code>managementethernet</code> for a Management Ethernet interface</td>
</tr>
<tr>
<td></td>
<td>• <code>null</code> for a Null interface</td>
</tr>
<tr>
<td></td>
<td>• <code>vlan</code> for a VLAN interface (Range: 1 to 4094, 1 to 2094 for ExaScale)</td>
</tr>
<tr>
<td>stack-unit</td>
<td>Enter the keyword <code>stack-unit</code> followed by the stack member number to display IFM information for that unit.</td>
</tr>
<tr>
<td>unit-ID</td>
<td>Range: 0 to 1</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is only available on S-Series.</td>
</tr>
<tr>
<td>trace-flags</td>
<td>Enter the keyword <code>trace-flags</code> to display IFM information for internal trace flags.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Mode**

EXEC

EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 7.6.1.0** Introduced for C-Series and S-Series
show switch links

View the switch fabric backplane or internal status.

Syntax

show switch links {backplane | internal}

Parameters

backplane

Enter the keyword backplane to view a table with information on the link status of the switch fabric backplane for both SFMs.

internal

Enter the keyword internal to view a table with information on the internal status of the switch fabric modules.

Defaults

None

Command Modes

EXEC

Command History

Version 7.5.1.0 Introduced on C-Series
Figure 5-56. Command Example: show switch links backplane

FTOS# show switch links backplane

Switch fabric backplane link status:

<table>
<thead>
<tr>
<th>LC SlotID</th>
<th>SFM0 Links Status</th>
<th>SFM1 Links Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port0</td>
<td>Port1</td>
<td>Port2</td>
</tr>
<tr>
<td>0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>1</td>
<td>not present</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>not present</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>not present</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>not present</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>not present</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>7</td>
<td>not present</td>
<td></td>
</tr>
</tbody>
</table>

up - Both ends of the link are up
down - Both ends of the link are down
down / up - SFM side down and LC side up

Figure 5-57 shows the output from the show system brief command.
Figure 5-58 shows the output from the show system stack-unit command.

show system (S-Series)

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 7.

Command Modes

EXEC
EXEC Privilege

Command History

Version 7.8.1.0 Modified output: Boot Flash field will display code level for boot code 2.8.1.1 and newer, while older boot codes are displayed as "Present".

Version 7.7.1.0 Modified output: Added Master Priority field.

Version 7.6.1.0 Introduced for S-Series switches

Usage

Figure 5-57 shows the output from the show system brief command.
Figure 5-58 shows the output from the show system stack-unit command.
Example Figure 5-57. Command Example: show system brief

FTOS#show system brief

Stack MAC : 0:1:e8:d6:4:70

-- Stack Info --
Unit  UnitType    Status         ReqTyp      CurTyp      Version     Ports
-------------------------------------------------------------------------------
 0   Member      not present
 1   Standby     online         S50V        S50V        7.7.1.0     52
 2   Mgmt        online         S50V        S50V        7.7.1.0     52
 3   Member      not present
 4   Member      not present
 5   Member      not present
 6   Member      not present
 7   Member      not present

-- Module Info --
Unit  Module No   Status        Module Type        Ports
-------------------------------------------------------------------------------
 1   0           online        S50-01-10GE-2P      2
 1   1           online        S50-01-24G-2S       1
 2   0           online        S50-01-10GE-2P      2
 2   1           online        S50-01-24G-2S       1

-- Power Supplies --
Unit   Bay   Status       Type
-------------------------------------------------------------------------------
 1     0     up            AC
 1     1     absent
 2     0     up            AC
 2     1     absent

-- Fan Status --
Unit   TrayStatus Fan0   Fan1   Fan2   Fan3   Fan4   Fan5
-------------------------------------------------------------------------------
 1     up      up      up      up      up      up      up
 2     up      up      up      up      up      up      up

FTOS#
Example

**Figure 5-58. Command Example: show system stack-unit 2**

FTOS#show system stack-unit 2
-- Unit 2 --
Unit Type : Management Unit
Status : online
Next Boot : online
Required Type : S50N - 48-port E/FE/GE (SB)
Current Type : S50N - 48-port E/FE/GE (SB)
Master priority : 0
Hardware Rev : 2.0
Num Ports : 52
Up Time : 5 min, 18 sec
Dell Networking OS Version : 8-4-2-399
Jumbo Capable : yes
POE Capable : no
Boot Flash : 2.8.1.2
Memory Size : 268435456 bytes
Temperature : 52C
Voltage : ok
Serial Number : DL257430183
Part Number : 7590005600 Rev B
Vendor Id : 07
Date Code : 12172007
Country Code : 01
Piece Part ID : CN-0RVY43-28298-82B-0456
PPID Revision : 1B2
Service Tag : SVCTGCH
Expr Svc Code : 628 458 864 65
Auto Reboot : enabled
Burned In MAC : 00:01:e8:50:5c:a6
No Of MACs : 3
-- Module 0 --
Status : not present
-- Module 1 --
Status : online
Module Type : S50-01-12G-2S - 2-port 12G Stacking (SB)
Num Ports : 2
Hot Pluggable : no
-- Power Supplies --
Unit Bay Status Type
---------------------------------------------------------------------------
2 0 up AC
2 1 absent
-- Fan Status --
Unit TrayStatus Speed Fan0 Fan1 Fan2 Fan3 Fan4 Fan5
---------------------------------------------------------------------------
2 up low up up up up up
FTOS#
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>Display the Dell Networking OS version.</td>
</tr>
<tr>
<td>show processes memory (S-Series)</td>
<td>Display memory usage based on running processes.</td>
</tr>
<tr>
<td>show system stack-ports</td>
<td>Display information about the stack ports on all switches in the S-Series stack.</td>
</tr>
<tr>
<td>show hardware stack-unit</td>
<td>Display the data plane and management plane input and output statistics of a particular stack member.</td>
</tr>
<tr>
<td>stack-unit priority</td>
<td>Configure the ability of an S-Series switch to become the management unit of a stack.</td>
</tr>
</tbody>
</table>

**show tech-support (C-Series and E-Series)**

Display, or save to a file, a collection of data from other show commands, the information necessary for Dell Networking technical support to perform troubleshooting.

**Syntax**

```
show tech-support [linecard 0-6 | page] | {display | except | find | grep | no-more | save}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linecard 0-6</td>
<td>(OPTIONAL) Enter the keyword <code>linecard</code> followed by the linecard number to view information relating to a specific linecard.</td>
</tr>
<tr>
<td>page</td>
<td>(OPTIONAL) Enter the keyword <code>page</code> 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>
<tr>
<td>display, except, find, grep, no-more</td>
<td>If you use the pipe command (`</td>
</tr>
<tr>
<td>save</td>
<td>Enter the <code>save</code> keyword (following the pipe) to save the command output. <code>flash</code>: Save to local flash drive (flash://filename (max 20 chars) ) <code>slot0</code>: Save to local file system (slot0://filename (max 20 chars) )</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td></td>
<td>Introduced <code>save</code> to file options</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td></td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.5.4.0</td>
<td></td>
<td>Show clock included in display on E-Series</td>
</tr>
</tbody>
</table>
C-Series Example

Figure 5-59. Command Example: show tech-support (partial) on C-Series

FTOS#show tech-support page

------------------------------------------------------------------------ show version ------------------------------------------
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: Dell Networking OS 7.5.1.0
Copyright (c) 1999-2007 by Force10 Networks, Inc.
Build Time: Tue Sep 12 15:39:17 IST 2006
Build Path: /sites/maa/work/sw//C-SERIES/SW/SRC
Force10 uptime is 18 minutes

System image file is "/work/sw/IMAGES/Chassis/C300-ODC-2/FTOS-CS.bin"

Chassis Type: C300
Control Processor: IBM PowerPC 750FX (Rev D2.2) with 1073741824 bytes of memory.
128K bytes of non-volatile configuration memory.
1 Route Processor/Switch Fabric Module
2 48-port GE 10/100/1000Base-T line card with RJ45 interface (CB)
1 FastEthernet/IEEE 802.3 interface(s)
96 GigabitEthernet/IEEE 802.3 interface(s)

------------------------------------------------------------------------ show HA information --------------------------
-- RPM Status --
------------------------------------------------------------------------
RPM Slot ID: 0
RPM Redundancy Role: Primary
RPM State: Active
RPM SW Version: CS-1-1-317
Link to Peer: Down
Peer RPM: not present

-- RPM Redundancy Configuration --
------------------------------------------------------------------------
Primary RPM: rpm0
Auto Data Sync: Full
Failover Type: Hot Failover
Auto reboot RPM: Disabled
Auto failover limit: 3 times in 60 minutes

...more----
Figure 5-60. Command Example: show tech-support save (partial) on E-Series

FTOS#show tech-support ?
linecard Line card
page Page through output
| Pipe through a command
<cr>
FTOS#show tech-support linecard 3 |

Usage Information
Without the linecard or page 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 should 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-profile
- show cam-ipv4flow
- show chassis
- show clock
- show environment
- show file-system
- show interface
show tech-support (S-Series)

Display a collection of data from other show commands, necessary for Dell Force10 technical support to perform troubleshooting on S-Series switches.

Syntax

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

Parameters

- `stack-unit` (OPTIONAL) Enter the keyword `stack-unit` to view CPU memory usage for the stack member designated by `unit-id`. Range: 0 to 7
- `page` (OPTIONAL) Enter the keyword `page` to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press the ENTER key to view the next line of text.

Command Modes

EXEC Privilege

Command History

- Version 7.8.1.0 Introduced save to file options
- Version 7.6.1.0 Expanded to support S-Series switches
Figure 5-61. Command Example: show tech-support save (partial) on S-Series

FTOS#show tech-support ?
page Page through output
stack-unit Unit Number
| Pipe through a command
<cr>
FTOS#show tech-support stack-unit 1 ?
| 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:
1 drw- 16384 Jan 01 1980 00:00:00 +00:00 .
2 drwx 1536 Jul 13 1996 02:38:06 +00:00 ..
3 d--- 512 Nov 20 2007 15:46:44 +00:00 ADMIN_DIR
4 -rw- 7124 Jul 13 1996 02:33:04 +00:00 startup-config
5 -rw- 3303 Feb 14 2008 22:01:16 +00:00 startup-config.oldChassis
6 -rw- 6561 May 17 1996 04:10:54 +00:00 startup-config.bak
7 -rw- 6539 May 29 1996 10:35:42 +00:00 test.cfg
8 -rw- 276 Jul 15 1996 23:11:14 +00:00 LauraSave

flash: 3104256 bytes total (3072512 bytes free)
FTOS#
Figure 5-62. Command Example: show tech-support (partial) on S-Series

```
FTOS#show tech-support stack-unit 0
```

```
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>show version</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Force10 Networks Real Time Operating System Software</td>
<td></td>
</tr>
<tr>
<td>Force10 Operating System Version: 1.0</td>
<td></td>
</tr>
<tr>
<td>Force10 Application Software Version: Dell Networking OS 7.6.1.0</td>
<td></td>
</tr>
<tr>
<td>Copyright (c) 1999-2007 by Force10 Networks, Inc.</td>
<td></td>
</tr>
<tr>
<td>Build Time: Tue Sep 12 15:39:17 IST 2006</td>
<td></td>
</tr>
<tr>
<td>Build Path: /sites/maa/work/sw/purushothaman/cser-latest/depot/main/Dev/Cyclone/Force10 uptime is 18 minutes</td>
<td></td>
</tr>
</tbody>
</table>

System Type: S50N
Control Processor: MPC8451E with 255545344 bytes of memory.
32M bytes of Boot-Flash memory.

1 48-port E/FE/GE (SB)
48 GigabitEthernet/IEEE 802.3 interface(s)
4 Ten GigabitEthernet/IEEE 802.3 interface(s)

```
```
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>show clock</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>12:03:01.695 UTC Wed Nov 21 2007</td>
<td></td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Current Configuration</td>
<td></td>
</tr>
<tr>
<td>! Version E_MAIN4.7.5.414</td>
<td></td>
</tr>
<tr>
<td>! Last configuration change at Wed Nov 21 11:42:19 2007 by default</td>
<td></td>
</tr>
<tr>
<td>! service timestamps log datetime</td>
<td></td>
</tr>
<tr>
<td>! hostname FTOS</td>
<td></td>
</tr>
<tr>
<td>! enable password 7 xxxxxxxx</td>
<td></td>
</tr>
<tr>
<td>! username admin password 7 xxxxxxxx</td>
<td></td>
</tr>
<tr>
<td>! enable restricted 7 xxxxxxxx</td>
<td></td>
</tr>
<tr>
<td>! interface GigabitEthernet 0/1</td>
<td></td>
</tr>
<tr>
<td>! no ip address</td>
<td></td>
</tr>
<tr>
<td>! shutdown</td>
<td></td>
</tr>
<tr>
<td>! interface GigabitEthernet 0/2</td>
<td></td>
</tr>
<tr>
<td>! no ip address</td>
<td></td>
</tr>
<tr>
<td>! shutdown</td>
<td></td>
</tr>
<tr>
<td>!--------------------------</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
```

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 should 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>Display the Dell Networking OS version.</td>
</tr>
<tr>
<td>show system (S-Series)</td>
<td>Display the current switch status.</td>
</tr>
<tr>
<td>show environment (S-Series)</td>
<td>Display system component status.</td>
</tr>
<tr>
<td>show processes memory (S-Series)</td>
<td>Display memory usage based on running processes.</td>
</tr>
</tbody>
</table>

**ssh-peer-rpm**

Open an SSH connection to the peer RPM.

**Syntax**

```
ssh-peer-rpm [-l username]
```

**Parameters**

- `-l username` (OPTIONAL) Enter the keyword `-l` followed by your user name.
  Default: The user name associated with the terminal

**Defaults**

Not configured.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

This command is not available when the peer RPMs are running different Dell Networking OS releases.

**telnet**

Connect through Telnet to a server. The Telnet client and server in Dell Networking OS support IPv4 and IPv6 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 | ipv6-address prefix-length | vrf vrf instance name} [l 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>ipv6-address</td>
<td>Enter the IPv6 address in the <code>X:X:X:X::X</code> format followed by the prefix length in the <code>X</code> format. Range: <code>/0</code> to <code>/128</code></td>
</tr>
<tr>
<td>prefix-length</td>
<td></td>
</tr>
<tr>
<td>vrf instance</td>
<td>(Optional) E-Series Only: Enter the keyword <code>vrf</code> followed by the VRF Instance name.</td>
</tr>
<tr>
<td>source-interface</td>
<td>(OPTIONAL) Enter the keywords <code>/source-interface</code> followed by the interface information to include the interface’s IP address. Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a 100/1000 Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Loopback interface, enter the keyword <code>loopback</code> followed by a number from zero (0) to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For the Null interface, enter the keyword <code>null</code> followed by 0.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>• C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For SONET interface types, enter the keyword <code>sonet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN interface, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

### Defaults
Not configured.

### Command Modes
- EXEC
- EXEC Privilege
Telnet to link-local addresses is not supported.

**telnet-peer-rpm**

Open a Telnet connection to the peer RPM.

**Syntax**

```
telnet-peer-rpm
```

**Defaults**

Not configured.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.6.0: Added support for the keyword **fortyGigE**.
- Version 8.2.1.0: Introduced on E-Series ExaScale (IPv6).
  - Increased number of VLANs on ExaScale to 4094 (was 2094)
- Version 8.1.1.0: Introduced on E-Series ExaScale (IPv4)
- Version 7.9.1.0: Introduced VRF.
- Version 7.6.1.0: Introduced on S-Series
- Version 7.5.1.0: Introduced on C-Series and added support for IPv6 address on E-Series only

**Usage Information**

Opening a telnet connection from the Standby RPM to an Active RPM follows the authentication procedure configured in the chassis. However, opening a telnet connection from the Active RPM into the Standby RPM requires local authentication.

Configuring an ACL on a VTY line will block a Telnet session using the **telnet-peer-rpm** command in the standby to active RPM direction only. Such an ACL will not block an internal Telnet session in the active RPM to standby RPM direction.
terminal length

Configure the number of lines displayed on the terminal screen.

**Syntax**

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

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

**Parameters**

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

**Defaults**

24 lines

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>E-Series original Command</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Information**

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

View a packet’s path to a specific device.

**Syntax**

```
traceroute {host | vrf instance | ip-address | ipv6-address}
```

**Parameters**

- `host`: Enter the name of device.
- `vrf instance`: (Optional) E-Series Only: Enter the keyword `vrf` followed by the VRF Instance name.
- `ip-address`: Enter the IP address of the device in dotted decimal format.
- `ipv6-address`: Enter the IPv6 address, in the `x:x:x::x` format, to which you are testing connectivity. **Note:** The :: notation specifies successive hexadecimal fields of zeros

**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 8.4.1.0 IPv6 trace routing available on management interface.
- Version 8.2.1.0 Introduced on E-Series ExaScale with IPv6
- Version 8.1.1.0 Introduced on E-Series ExaScale (IPv4 only)
- Version 7.9.1.0 Introduced VRF.
- Version 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 7.4.1.0 Added support for IPv6 address on E-Series
- E-Series original Command

**Usage Information**

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.

For the source IP address option, you may enter IPv6 global addresses only (link-local addresses are not supported).

For IPv6, you are prompted for a minimum hop count (default is 1) and a maximum hop count (default is 64).
Example  Figure 5-63. Command Example: traceroute (IPv4)

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

<table>
<thead>
<tr>
<th>TTL</th>
<th>Hostname</th>
<th>Probe1</th>
<th>Probe2</th>
<th>Probe3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.11.199.190</td>
<td>001.000 ms</td>
<td>001.000 ms</td>
<td>002.000 ms</td>
</tr>
<tr>
<td>2</td>
<td>gwegress-sjc-02.force10networks.com (10.11.30.126)</td>
<td>005.000 ms</td>
<td>001.000 ms</td>
<td>001.000 ms</td>
</tr>
<tr>
<td>3</td>
<td>fw-sjc-01.force10networks.com (10.11.127.254)</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
</tr>
<tr>
<td>4</td>
<td><a href="http://www.force10networks.com">www.force10networks.com</a> (10.11.84.18)</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
</tr>
</tbody>
</table>

FTOS#

Example  Figure 5-64. Command Example: traceroute (IPv6)

FTOS#traceroute 100::1

Type Ctrl-C to abort.

Tracing the route to 100::1, 64 hops max, 60 byte packets

<table>
<thead>
<tr>
<th>Hops</th>
<th>Hostname</th>
<th>Probe1</th>
<th>Probe2</th>
<th>Probe3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100::1</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
</tr>
</tbody>
</table>

FTOS#traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b

Type Ctrl-C to abort.

Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b, 64 hops max, 60 byte packets

<table>
<thead>
<tr>
<th>Hops</th>
<th>Hostname</th>
<th>Probe1</th>
<th>Probe2</th>
<th>Probe3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3ffe:501:ffff:100:201:e8ff:fe00:4c8b</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
<td>000.000 ms</td>
</tr>
</tbody>
</table>

FTOS#

Related Commands

ping  Test connectivity to a device.
**undebug all**

Disable all debug operations on the system.

**Syntax**

`undebug all`

**Defaults**

No default behavior or values

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

**upload trace-log**

Upload trace log files from the three CPUs (cp, rp1, and rp2)

**Syntax**

`upload trace-log {cp {cmd-history | hw-trace | sw-trace}}| rp1 {cmd-history | hw-trace | sw-trace}}| rp2 {cmd-history | hw-trace | sw-trace}}`

**Parameters**

- `cp | rp1 | rp2` Enter the keyword `cp | rp1 | rp2` to upload the trace log from that CPU.
- `cmd-history` (OPTIONAL) Enter the keyword `cmd-history` to upload the CPU’s command history.
- `hw-trace` (OPTIONAL) Enter the keyword `hw-trace` to upload the CPU’s hardware trace.
- `sw-trace` (OPTIONAL) Enter the keyword `sw-trace` to upload the CPU’s software trace.

**Defaults**

No default behavior or values

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series and expanded to support command history, hardware trace, and software trace logs</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The log information is uploaded to flash:/TRACE_LOG_DIR
virtual-ip

Configure a virtual IP address for the active management interface. Virtual addresses can be configured both for IPv4 and IPv6 independently.

Syntax

```
virtual-ip {ipv4-address | ipv6-address}
```

Parameters

- **ipv4-address**
- **ipv6-address**

Enter the IPv4 address (A.B.C.D) or IPv6 address (X::X::X::) of the active management interface.

Defaults

No default behavior or values

Command Modes

CONFIGURATION

Command History

- **Version 8.4.1.0**
  - Added support for IPv6 addressing.
- **Version 8.1.1.0**
  - Introduced on E-Series ExaScale
- **Version 7.5.1.0**
  - Introduced on C-Series

Usage Information

Both IPv4 and IPv6 virtual address can be configured simultaneously, but only one of each. Each time this command is issued it will replace the previously configured address of the same family, IPv4 or IPv6. The `no virtual-ip` command now takes an address/prefix-length argument, so that the desired address only is removed. If `no virtual-ip` is entered without any specified address, then both IPv4 and IPv6 virtual addresses are removed.

Example

```
Figure 5-65. Command Example: virtual ip (IPv4 and IPv6)

FTOS#virtual-ip 10.11.197.99/16
FTOS#virtual-ip fdaa:bbbb:cccc:1004::60/64
```

write

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

Syntax

```
write {memory | terminal}
```

Parameters

- **memory**
- **terminal**

  - 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.
  - 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

- **Version 8.1.1.0**
  - Introduced on E-Series ExaScale
- **Version 7.6.1.0**
  - Introduced on S-Series
- **Version 7.5.1.0**
  - Introduced on C-Series

E-Series original Command
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>save</td>
<td>Save configurations created in BOOT_USER mode (BLI).</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" (for example, you used a specific file during the **boot config** command) the running-config is not saved to that file; use the **copy** command to save any running-configuration changes to that local file.
802.1ag

Overview

802.1ag is available only on platform: S

Commands

This chapter contains the following commands:

- `ccm disable`
- `ccm transmit-interval`
- `clear ethernet cfm traceroute-cache`
- `database hold-time`
- `disable`
- `domain`
- `ethernet cfm`
- `ethernet cfm mep`
- `ethernet cfm mip`
- `mep cross-check`
- `mep cross-check enable`
- `mep cross-check start-delay`
- `ping ethernet`
- `show ethernet cfm domain`
- `show ethernet cfm maintenance-points local`
- `show ethernet cfm maintenance-points remote`
- `show ethernet cfm mipbd`
- `show ethernet cfm statistics`
- `show ethernet cfm port-statistics`
- `show ethernet cfm traceroute-cache`
- `service`
- `traceroute cache hold-time`
- `traceroute cache size`
- `traceroute ethernet`
ccm disable

Syntax  ccm disable

Enter no ccm disable to enable CCM.

Defaults  Disabled

Command Modes  ECFM DOMAIN

Command History

- Version 8.3.7.0  Introduced on the S4810.
- Version 8.3.6.0  Introduced on the S-Series

ccm transmit-interval

Syntax  ccm transmit-interval seconds

Parameters

- seconds: Enter a transmit interval.
  Range: 1,10,60,600

Defaults  10 seconds

Command Modes  ECFM DOMAIN

Command History

- Version 8.3.7.0  Introduced on the S4810.
- Version 8.3.1.0  Introduced on S-Series

clear ethernet cfm traceroute-cache

Syntax  clear ethernet cfm traceroute-cache

Defaults  None

Command Modes  EXEC Privilege

Command History

- Version 8.3.7.0  Introduced on the S4810.
- Version 8.3.1.0  Introduced on S-Series

database hold-time

Syntax  database hold-time

Parameters

Set the amount of time that data from a missing MEP is kept in the Continuity Check Database.
Syntax: **database hold-time minutes**

Parameters:

- **minutes**: Enter a hold-time.
  - Range: 100-65535 minutes

Defaults: 100 minutes

Command Modes: ECFM DOMAIN

Command History:
- Version 8.3.7.0 Introduced on the S4810.
- Version 8.3.1.0 Introduced on S-Series

---

**disable**

Disable Ethernet CFM without stopping the CFM process.

Syntax: **disable**

Defaults: Disabled

Command Modes: ETHERNET CFM

Command History:
- Version 8.3.7.0 Introduced on the S4810.
- Version 8.3.1.0 Introduced on S-Series

---

**domain**

Create maintenance domain.

Syntax: **domain name md-level number**

Parameters:

- **name**: Name the maintenance domain.
- **md-level number**: Enter a maintenance domain level.
  - Range: 0-7

Defaults: None

Command Modes: ETHERNET CFM

Command History:
- Version 8.3.7.0 Introduced on the S4810.
- Version 8.3.1.0 Introduced on S-Series

---

**ethernet cfm**

Spawn the CFM process. No CFM configuration is allowed until the CFM process is spawned.
**Syntax**

```
eternet cfm
```

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

---

**ethernet cfm mep**

Create an MEP.

**Syntax**

```
eternet cfm mep \{up-mep | down-mep\} domain \{name | level\} ma-name name mepid mep-id
```

**Parameters**

- **[up-mep | down-mep]** Specify whether the MEP is up or down facing.
  - **Up-MEP**: monitors the forwarding path internal to an bridge on the customer or provider edge; on Dell Networking systems the internal forwarding path is effectively the switch fabric and forwarding engine.
  - **Down-MEP**: monitors the forwarding path external another bridge.
- **domain [name | level]** Enter this keyword followed by the domain name or domain level.
- **ma-name name** Enter this keyword followed by the name of the maintenance association.
- **mepid mep-id** Enter an MEP ID.
  - Range: 1-8191

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

---

**ethernet cfm mip**

Create an MIP.

**Syntax**

```
eternet cfm mip domain \{name | level\} ma-name name
```

**Parameters**

- **domain [name | level]** Enter this keyword followed by the domain name or domain level.
- **ma-name name** Enter this keyword followed by the name of the maintenance association.

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>
mep cross-check

Enable cross-checking for an MEP.

Syntax

```
mep cross-check mep-id
```

Parameters

- `mep-id` Enter the MEP ID
  Range: 1-8191

Defaults
None

Command Modes
ECFM DOMAIN

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

mep cross-check enable

Enable cross-checking.

Syntax

```
mep cross-check enable {port | vlan-id}
```

Parameters

- `port` Down service with no VLAN association.
- `vlan-id` Enter the VLAN to apply the cross-check.

Defaults
None

Command Modes
ECFM DOMAIN

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

mep cross-check start-delay

Configure the amount of time the system waits for a remote MEP to come up before the cross-check operation is started.

Syntax

```
mep cross-check start-delay number
```

Parameters

- `start-delay number` Enter a start-delay in seconds.
  Range: 3-100 seconds

Defaults
3 ccms
### ping ethernet

Send a Loopback message.

**Syntax**

```plaintext
ping ethernet domain [name | level] ma-name m a-name remote {dest-mep-id | mac-addr mac-address} source {src-mep-id | port interface}
```

**Parameters**

- `name | level`: Enter the domain name or level.
- `ma-name ma-name`: Enter the keyword followed by the maintenance association name.
- `dest-mep-id`: Enter the MEP ID that will be the target of the ping.
- `mac-addr mac-address`: Enter the keyword followed by the MAC address that will be the target of the ping.
- `src-mep-id`: Enter the MEP ID that will originate the ping.
- `port interface`: Enter the keyword followed by the interface that will originate the ping.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

- Version 8.3.7.0: Introduced on the S4810.
- Version 8.3.1.0: Introduced on S-Series

### show ethernet cfm domain

Display maintenance domain information.

**Syntax**

```plaintext
show ethernet cfm domain [name | level | brief]
```

**Parameters**

- `name | level`: Enter the maintenance domain name or level.
- `brief`: Enter this keyword to display a summary output.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

- Version 8.3.7.0: Introduced on the S4810.
- Version 8.3.1.0: Introduced on S-Series
Example

FTOS# show ethernet cfm domain

Domain Name: customer
Level: 7
Total Service: 1

<table>
<thead>
<tr>
<th>MA-Name</th>
<th>VLAN</th>
<th>CC-Int</th>
<th>X-CHK Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>My_MA</td>
<td>200</td>
<td>10s</td>
<td>enabled</td>
</tr>
</tbody>
</table>

Domain Name: My_Domain
Level: 6
Total Service: 1

<table>
<thead>
<tr>
<th>MA-Name</th>
<th>VLAN</th>
<th>CC-Int</th>
<th>X-CHK Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your_MA</td>
<td>100</td>
<td>10s</td>
<td>enabled</td>
</tr>
</tbody>
</table>

show ethernet cfm maintenance-points local

Display configured MEPs and MIPs.

Syntax

show ethernet cfm maintenance-points local [mep | mip]

Parameters

- **mep**: Enter this keyword to display configured MEPs.
- **mip**: Enter this keyword to display configured MIPs.

Defaults

None

Command Modes

EXEC Privilege

Command History

- Version 8.3.7.0: Introduced on the S4810.
- Version 8.3.1.0: Introduced on S-Series

Example

FTOS# show ethernet cfm maintenance-points local mip

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>Level</th>
<th>Type</th>
<th>Port</th>
<th>CCM-Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>service1</td>
<td>4</td>
<td>MIP</td>
<td>Gi 0/5</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>My_MA</td>
<td>3333</td>
<td>DOWN</td>
<td>00:01:e8:0b:c6:36</td>
<td>Disabled</td>
</tr>
<tr>
<td>0</td>
<td>service1</td>
<td>4</td>
<td>MIP</td>
<td>Gi 0/5</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Your_MA</td>
<td>3333</td>
<td>UP</td>
<td>00:01:e8:0b:c6:36</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

show ethernet cfm maintenance-points remote

Display the MEP Database.

Syntax

show ethernet cfm maintenance-points remote detail [active | domain {level | name} | expired | waiting]

Parameters

- **active**: Enter this keyword to display only the MEPs in active state.
- **domain [name | level]**: Enter this keyword followed by the domain name or domain level.
show ethernet cfm mipbd
Display the MIP Database.

Syntax:
```
show ethernet cfm mipdb
```

Defaults: None

Command Modes: EXEC Privilege

Command History:
- Version 8.3.7.0: Introduced on the S4810.
- Version 8.3.1.0: Introduced on S-Series

show ethernet cfm statistics
Display MEP statistics.

Syntax:
```
show ethernet cfm statistics [domain \{name | level\} vlan-id vlan-id mpid mpid]
```

Parameters:
- **domain**
  - Enter this keyword to display statistics for a particular domain.
- **name | level**
  - Enter the domain name or level.
- **vlan-id vlan-id**
  - Enter this keyword followed by a VLAN ID.
- **mpid mpid**
  - Enter this keyword followed by a maintenance point ID.

Defaults: None
show ethernet cfm port-statistics

Display CFM statistics by port.

Syntax

```
show ethernet cfm port-statistics [interface type slot/port]
```

Parameters

- **interface type**: Enter this keyword followed by the interface type.
- **slot/port**: Enter the slot and port numbers for the port.

Defaults

None

Command Modes

EXEC Privilege

Command History

- **Version 8.3.7.0**: Introduced on the S4810.
- **Version 8.3.1.0**: Introduced on S-Series

Example

```
FTOS#show ethernet cfm port-statistics
Port statistics for port: Gi 0/5
==================================
RX Statistics
-------------------
Total CFM Pkts 75394 CCM Pkts 75394
LBM Pkts 0 LTM Pkts 0
LBR Pkts 0 LTR Pkts 0
Bad CFM Pkts 0 CFM Pkts Discarded 0
CFM Pkts forwarded 102417
TX Statistics
-------------------
Total CFM Pkts 10303 CCM Pkts 0
LBM Pkts 0 LTM Pkts 3
LBR Pkts 0 LTR Pkts 0
```

show ethernet cfm traceroute-cache

Display the Link Trace Cache.
### Syntax

```
show ethernet cfm traceroute-cache
```

### Defaults

None

### Command Modes

EXEC Privilege

### Command History

- **Version 8.3.7.0**: Introduced on the S4810.
- **Version 8.3.1.0**: Introduced on S-Series

### Example

```
FTOS#show ethernet cfm traceroute-cache
Traceroute to 00:01:e8:52:4a:f8 on Domain Customer2, Level 7, MA name Test2 with VLAN 2
------------------------------------------------------------------------------------------
Hops              Host              IngressMAC     Ingr Action   Relay Action     Next Host            Egress MAC     Egress Action  FWD Status
------------------------------------------------------------------------------------------
4      00:00:00:01:e8:53:4a:f8   00:01:e8:52:4a:f8  IngOK             RlyHit     00:00:00:01:e8:52:4a:f8                                        Terminal MEP
```

### service

```
Create maintenance association.
```

### Syntax

```
service name vlan vlan-id
```

### Parameters

- **name**: Enter a maintenance association name.
- **vlan vlan-id**: Enter this keyword followed by the VLAN ID.
  - **Range**: 1-4094

### Defaults

None

### Command Modes

ECFM DOMAIN

### Command History

- **Version 8.3.7.0**: Introduced on the S4810.
- **Version 8.3.1.0**: Introduced on S-Series

### traceroute cache hold-time

```
Set the amount of time a trace result is cached.
```

### Syntax

```
traceroute cache hold-time minutes
```

### Parameters

- **minutes**: Enter a hold-time.
  - **Range**: 10-65535 minutes

### Defaults

100 minutes

### Command Modes

ETHERNET CFM
### traceroute cache size

Set the size of the Link Trace Cache.

**Syntax**

```markdown
traceroute cache size entries
```

**Parameters**

- `entries`: Enter the number of entries the Link Trace Cache can hold.
  - Range: 1 - 4095 entries

**Defaults**

100 entries

**Command Modes**

ETHERNET CFM

**Command History**

- **Version 8.3.7.0**: Introduced on the S4810.
- **Version 8.3.1.0**: Introduced on S-Series

---

### traceroute ethernet

Send a Linktrace message to an MEP.

**Syntax**

```markdown
traceroute ethernet domain [name | level] ma-name ma-name remote {mep-id mep-id | mac-addr mac-address}
```

**Parameters**

- `domain name | level`: Enter the keyword followed by the domain name or level.
- `ma-name ma-name`: Enter the keyword followed by the maintenance association name.
- `mepid mep-id`: Enter the MEP ID that will be the trace target.
- `mac-addr mac-address`: Enter the MAC address of the trace target.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

- **Version 8.3.7.0**: Introduced on the S4810.
- **Version 8.3.1.0**: Introduced on S-Series
802.3ah

Overview

802.3ah is available only on platform: S

Commands

This chapter contains the following commands:

- clear ethernet oam statistics
- ethernet oam (enable/disable)
- ethernet oam (parameters)
- ethernet oam event-log size
- ethernet oam link-monitor frame
- ethernet oam link-monitor frame-seconds
- ethernet oam link-monitor high-threshold action
- ethernet oam link-monitor on
- ethernet oam link-monitor supported
- ethernet oam link-monitor symbol-period
- ethernet oam mode
- ethernet oam remote-failure
- ethernet oam remote-loopback
- ethernet oam remote-loopback (interface)
- ethernet oam timeout
- show ethernet oam discovery
- show ethernet oam status
- show ethernet oam statistics
- show ethernet oam summary
**clear ethernet oam statistics**

Clear Link Layer OAM statistics.

**Syntax**
clear ethernet oam statistics interface interface

**Parameters**

- **interface** Enter the interface for which you want to clear statistics, for example **gig 0/1**.

- **Parameters**
  - None

- **Defaults**
  - None

- **Command Mode**
  - EXEC Privilege

- **Command History**
  - Version 8.4.1.0 Introduced on S-Series

---

**ethernet oam (enable/disable)**

Enable Ethernet OAM.

**Syntax**
ethernet oam

**Parameters**

- None

**Defaults**

- Disabled

**Command Mode**

- INTERFACE

**Command History**

- Version 8.4.1.0 Introduced on S-Series

---

**ethernet oam (parameters)**

Specify a the maximum or minimum number of OAMPDUs to be sent per second.

**Syntax**
ethernet oam {max-rate value | min-rate value}

**Parameters**

- **max-rate value** Enter a maximum or minimum rate in OAMPDU/second.
  - Range: 1-10

- **Defaults**
  - 10

**Command Mode**

- INTERFACE

**Command History**

- Version 8.4.1.0 Introduced on S-Series
ethernet oam event-log size

Specify the size of the event log.

Syntax
ethernet oam event-log size entries

Parameters
entries Enter the number of entries for the log size.
Range: 0 to 200.
Default: 50.

Defaults
50

Command Mode
CONFIGURATION

Command History

Version 8.4.1.0 Introduced on S-Series

ethernet oam link-monitor frame

Set the frame error thresholds and window.

Syntax
ethernet oam link-monitor frame threshold {high {frames | none} | low frames | window frames}

Parameters
high {frames | none} Specify the high threshold value for frame errors, or disable the high threshold.
Range: 1-65535
Default: None

low frames Specify the low threshold for frame errors.
Range: 0-65535
Default: 1

window frames Specify the time period for frame errors per millisecond condition.
Range: 10-600 milliseconds
Default: 100 milliseconds

Defaults
As above

Command Mode
INTERFACE

Command History

Version 8.4.1.0 Introduced on S-Series

ethernet oam link-monitor frame-seconds

Set the frame-error seconds per time period thresholds and window.

Syntax
ethernet oam link-monitor frame-seconds threshold {high {milliseconds | none} | low milliseconds | window milliseconds}
**Parameters**

**high** *(milliseconds | none)*  
Specify the high threshold value for frame error seconds per time period, or disable the high threshold.  
Range: 1-900  
Default: None

**low** *(milliseconds)*  
Specify the low threshold for frame error seconds per time period.  
Range: 1-900  
Default: 1

**window** *(milliseconds)*  
Specify the time period for error second per time period condition.  
Range: 100-900, in multiples of 100  
Default: 1000 milliseconds

**Defaults**  
As above

**Command Mode**  
INTERFACE

**Command History**  
Version 8.4.1.0  
Introduced on S-Series

---

**ethernet oam link-monitor high-threshold action**

Enable an interface when the high threshold is exceeded for any of the monitored error conditions.

**Syntax**  
ethernet oam link-monitor high-threshold action error-disable-interface

**Defaults**  
Enabled

**Command Mode**  
INTERFACE

**Command History**  
Version 8.4.1.0  
Introduced on S-Series

---

**ethernet oam link-monitor on**

Start link performance monitoring on an interface. To stop link monitoring, enter the `no ethernet oam link-monitor on` command.

Link monitoring is started on an interface by default when you enable Ethernet OAM with the `ethernet oam` command.

**Syntax**  
ethernet oam link-monitor on

**Defaults**  
Enabled

**Command Mode**  
INTERFACE

**Command History**  
Version 8.4.1.0  
Introduced on S-Series
### ethernet oam link-monitor supported

Enable support for link performance monitoring on an interface. To disable support for link monitoring, enter the **no ethernet oam link-monitor supported** command.

Support for link monitoring is enabled on an interface by default when you enable Ethernet OAM with the **ethernet oam** command.

#### Syntax

```
ethernet oam link-monitor supported
```

#### Defaults

Enabled

#### Command Mode

INTERFACE

#### Command History

- **Version 8.4.1.0**
  - Introduced on S-Series

### ethernet oam link-monitor symbol-period

Set the symbol error thresholds and window.

#### Syntax

```
ethernet oam link-monitor symbol-period threshold {high {symbols | none} | low symbols | window symbols}
```

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**high {symbols</td>
<td>none}**</td>
</tr>
<tr>
<td></td>
<td>threshold.</td>
</tr>
<tr>
<td></td>
<td>Range: 1-65535</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td><strong>low symbols</strong></td>
<td>Specify the low threshold for symbol errors.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-65535</td>
</tr>
<tr>
<td></td>
<td>Default: 10</td>
</tr>
<tr>
<td><strong>window symbols</strong></td>
<td>Specify the time period for symbol errors per second condition.</td>
</tr>
<tr>
<td></td>
<td>Range: 1-65535 times 1,000,000 symbols</td>
</tr>
<tr>
<td></td>
<td>Default: 10 times 1,000,000 symbols (10,000,000 symbols)</td>
</tr>
</tbody>
</table>

#### Defaults

As above

#### Command Mode

INTERFACE

#### Command History

- **Version 8.4.1.0**
  - Introduced on S-Series

### ethernet oam mode

Set the transmission mode to active or passive.

#### Syntax

```
ethernet oam mode {active | passive}
```

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Choose either active or passive mode for the interface.</td>
</tr>
<tr>
<td>passive</td>
<td></td>
</tr>
</tbody>
</table>
ethernet oam remote-failure

Block or disable an interface when a particular critical link event occurs.

**Syntax**
```
ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action {error-block-interface | error-disable-interface}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical-event</td>
<td>An unspecified critical event occurred.</td>
</tr>
<tr>
<td>dying-gasp</td>
<td>An unrecoverable local failure condition occurred.</td>
</tr>
<tr>
<td>link-fault</td>
<td>A fault occurred in the receive direction of the local peer.</td>
</tr>
<tr>
<td>error-block-interface</td>
<td>Block the interface if the specified fault occurs.</td>
</tr>
<tr>
<td>error-disable-interface</td>
<td>Disable the interface if the specified fault occurs.</td>
</tr>
</tbody>
</table>

**Defaults**
Disabled

**Command Mode**
INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

---

ethernet oam remote-loopback

Start or stop loopback operation on a local interface with a remote peer.

**Syntax**
```
ethernet oam remote-loopback {start | stop} interface interface
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>stop</td>
</tr>
<tr>
<td>interface interface</td>
<td>Specify the interface on which remote-loopback starts/stops, for example gigabitethernet 0/1.</td>
</tr>
</tbody>
</table>

**Defaults**
Enabled

**Command Mode**
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>
**ethernet oam remote-loopback (interface)**

Syntax: `ethernet oam remote-loopback {supported | timeout seconds}

Parameters:
- **supported**: Start or stop a loopback operation on a peer.
- **timeout seconds**: Specify the number of seconds that the local peer waits to receive a returned frame before considering a remote peer to be non-operational. Valid values are from 1 to 10.

Defaults: None

Command Mode: INTERFACE

Command History:
- Introduced on S-Series

**ethernet oam timeout**

Syntax: `ethernet oam timeout value`

Parameters:
- **value**: Enter a timeout value in seconds. Range: 2-30 seconds

Defaults: 5 seconds

Command Mode: INTERFACE

Command History:
- Introduced on S-Series

**show ethernet oam discovery**

Syntax: `show ethernet oam discovery interface interface`

Parameters:
- **interface**: Enter the interface for which you want to display status, for example `gig 0/1`.

Defaults: None

Command Mode: EXEC Privilege

Command History:
- Introduced on S-Series
Example

```
FTOS# show ethernet oam discovery interface <interface-name>
```

Local client

Administrative configurations:
- Mode: active
- Unidirection: not supported
- Link monitor: supported (on)
- Remote loopback: not supported
- MIB retrieval: not supported
- Mtu size: 1500

Operational status:
- Port status: operational
- Loopback status: no loopback
- PDU permission: any
- PDU revision: 1

Remote client

MAC address: 0030.88fe.87de
Vendor (OUI): 0x00 0x00 0x0C

Administrative configurations:
- Mode: active
- Unidirection: not supported
- Link monitor: supported
- Remote loopback: not supported
- MIB retrieval: not supported
- Mtu size: 1500

show ethernet oam statistics

Display Link Layer OAM statistics per interface.

**Syntax**

```
show ethernet oam statistics interface interface
```

**Parameters**

`interface` Enter the interface for which you want to display statistics, for example `gig 0/1`.

**Defaults**

None

**Command Mode**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>S-Series</td>
</tr>
</tbody>
</table>
Example

FTOS# show ethernet oam statistics interface <interface-name>

@interface-name

Counters:

Information OAMPDU Tx: 3439489
Information OAMPDU Rx: 9489
Unique Event Notification OAMPDU Tx: 0
Unique Event Notification OAMPDU Rx: 0
Duplicate Event Notification OAMPDU Tx: 0
Duplicate Event Notification OAMPDU Rx: 0
Loopback Control OAMPDU Tx: 0
Loopback Control OAMPDU Rx: 2
Variable Request OAMPDU Tx: 0
Variable Request OAMPDU Rx: 0
Variable Response OAMPDU Tx: 0
Variable Response OAMPDU Rx: 0
Force10 OAMPDU Tx:: 10
Force10 OAMPDU Rx:: 21
Unsupported OAMPDU Tx: 0
Unsupported OAMPDU Rx: 0
Frame Lost due to OAM: 0

Local Faults:

0 Link Fault Records
0 Dying Gasp Records
Total dying Gasp:: 2
Time Stamp: 00:40:23
Total dying Gasp:: 1
Time Stamp: 00:41:23
0 Critical Event Records

Remote Faults:

0 Link Fault Records
0 Dying Gasp Records
0 Critical Event Records

Local Event Logs:

0 Errored Symbol Period Records
0 Errored Frame Records
0 Errored Frame Period Records
0 Errored Frame Second Records

Remote Event Logs:

0 Errored Symbol Period Records
0 Errored Frame Records
0 Errored Frame Period Records
0 Errored Frame Second Records
show ethernet oam status

Display Link Layer OAM status per interface.

Syntax

show ethernet oam status interface interface

Parameters

interface Enter the interface for which you want to display status, for example gig 0/1.

Defaults

None

Command Mode

EXEC Privilege

Command History

Version 8.4.1.0 Introduced on S-Series

Example

FTOS# show ethernet oam status interface <interface-name>

Output Format :

<interface-name>

General

Mode:active
PDU max rate:10 packets per second
PDU min rate:1 packet per second
Link timeout:5 seconds
High threshold action:no action

Link Monitoring

Status supported (on)
Symbol Period Error
  Window:1 million symbols
  Low threshold:1 error symbol(s)
  High threshold:none
Frame Error
  Window:1 million symbols
  Low threshold:1 error symbol(s)
  High threshold:none
Frame Period Error
  Window:1 x 100,000 frames
  Low threshold:1 error symbol(s)
  High threshold:none
Frame Seconds Error
  Window:600 x 100 milliseconds
  Low threshold:1 error second(s)
  High threshold:none
show ethernet oam summary

Display Link Layer OAM sessions.

**Syntax**

```
show ethernet oam summary
```

**Defaults**

None

**Command Mode**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version 8.4.1.0</th>
<th>Introduced on S-Series</th>
</tr>
</thead>
</table>

**Example**

```
FTOS# show ethernet oam summary

Output format:

Symbols:* - Master Loopback State, # - Slave Loopback State
Capability codes:L - Link Monitor, R - Remote Loopback
U - Unidirection,V - Variable Retrieval

LocalRemote
InterfaceMAC AddressOUIModeCapability
Gi6/1/10023.84ac.b8000000DactiveL R
```
The 802.1X Port Authentication commands are:

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

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

Dell Networking OS supports RADIUS and Active Directory environments using 802.1X Port Authentication.

**Important Points to Remember**

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

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

**debug dot1x**

Display 802.1X debugging information.

**Syntax**

```
debug dot1x [all | errors | packets | state-machine] [interface interface]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable all 802.1X debug messages.</td>
</tr>
<tr>
<td>errors</td>
<td>Display information about all 802.1X errors.</td>
</tr>
<tr>
<td>packets</td>
<td>Display information about all 802.1X packets.</td>
</tr>
<tr>
<td>state-machine</td>
<td>Restricts the debugging information to an interface.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter one of the following interfaces and slot/port information:</td>
</tr>
<tr>
<td></td>
<td>• For a Fast Ethernet interface, enter the keyword <code>FastEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>• C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For a SONET interface, enter the keyword <code>sonet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 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 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.4.1.0** Introduced on C-Series and S-Series
**dot1x auth-type mab-only**

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

**Syntax**

`dot1x auth-type mab-only`

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

Version 8.4.2.1 Introduced on the C-Series and S-Series

**Usage Information**

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

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

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

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

**Related Commands**

- `dot1x mac-auth-bypass`

---

**dot1x authentication (Configuration)**

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

**Syntax**

`dot1x authentication`

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

Version 7.6.1.0 Introduced on C-Series and S-Series

Version 7.4.1.0 Introduced on E-Series

**Related Commands**

- `dot1x authentication (Interface)`
**dot1x authentication (Interface)**

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

**Syntax**

```
dot1x authentication
```

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

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Related Commands**

- `dot1x port-control`
- `dot1x guest-vlan`
- `show dot1x interface`

**Commands History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

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

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

**Related Commands**

- `dot1x auth-fail-vlan`
### dot1x auth-server

Configure the authentication server to RADIUS.

**Syntax**

```markdown
dot1x auth-server radius
```

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

### dot1x guest-vlan

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

**Syntax**

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

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

**Parameters**

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

**Defaults**

Not configured

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

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

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

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

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

**Related Commands**

- `dot1x auth-fail-vlan`
- `dot1x reauthentication`
- `show dot1x interface`
**dot1x host-mode**

Enable single-host or multi-host authentication.

**Syntax**

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

**Parameters**

- **single-host**: Enable single-host authentication.
- **multi-host**: Enable multi-host authentication.
- **multi-auth**: Enable multi-supplicant authentication.

**Defaults**

single-host

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>The <code>multi-auth</code> option was introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>8.3.2.0</td>
<td>The <code>single-host</code> and <code>multi-host</code> options were introduced on the C-Series, E-Series TeraScale, and S-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

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

**Related Commands**

- `show dot1x interface`

**dot1x mac-auth-bypass**

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

**Syntax**

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

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

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

**Related Commands**

- `dot1x auth-type`
- `mab-only`
**dot1x max-eap-req**

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

**Syntax**

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

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

**Parameters**

- `number` Enter the number of times an EAP request is transmitted before a session time-out.
  - Range: 1 to 10
  - Default: 2

**Defaults**

2

**Command Modes**

INTERFACE

**Command History**

- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

**dot1x max-supplicants**

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

**Syntax**

```
dot1x max-supplicants number
```

**Parameters**

- `number` Enter the number of supplicants that can be authenticated on a single port in multi-auth mode.
  - Range: 1-128
  - Default: 128

**Defaults**

128 hosts can be authenticated on a single authenticator port.

**Command Modes**

INTERFACE

**Command History**

- Version 8.4.1.0 Introduced on C-Series and S-Series

**Related Commands**

- `dot1x host-mode`

**dot1x port-control**

Enable port control on an interface.

**Syntax**

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

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

**dot1x quiet-period**

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

**Syntax**

```
dot1x quiet-period seconds
```

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

**Parameters**

- `seconds`
  - Enter the number of seconds.
  - Range: 1 to 65535
  - Default: 30

**Defaults**

30 seconds

**Command Modes**

INTERFACE

**Command History**

- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

**dot1x reauthentication**

Enable periodic re-authentication of the client.

**Syntax**

```
dot1x reauthentication [interval seconds]
```

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interval seconds</code></td>
<td>(Optional) Enter the keyword <code>interval</code> followed by the interval time, in seconds, after which re-authentication will be initiated. Range: 1 to 31536000 (1 year) Default: 3600 (1 hour)</td>
</tr>
</tbody>
</table>

### Defaults

3600 seconds (1 hour)

### Command Modes

INTERFACE

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

### dot1x reauth-max

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

**Syntax**

```
show dot1x reauth-max number
```

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter the permitted number of re-authentications. Range: 1 - 10 Default: 2</td>
</tr>
</tbody>
</table>

### Defaults

2

### Command Modes

INTERFACE

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
dot1x server-timeout

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

Syntax

```
dot1x server-timeout seconds
```

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

Parameters

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

Defaults

30 seconds

Command Modes

INTERFACE

Command History

- **Version 7.6.1.0**
  - Introduced on C-Series and S-Series
- **Version 7.4.1.0**
  - Introduced on E-Series

Usage Information

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

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

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

For example:

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

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

**Syntax**

```
dot1x supplicant-timeout seconds
```

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

**Parameters**

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

**Defaults**

30 seconds

**Command Modes**

INTERFACE

**Command History**

- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

---

**dot1x tx-period**

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

**Syntax**

```
dot1x tx-period seconds
```

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

**Parameters**

- `seconds` Enter the interval time, in seconds, that EAPOL PDUs are transmitted.
  - Range: 1 to 31536000 (1 year)
  - Default: 30

**Defaults**

30 seconds

**Command Modes**

INTERFACE

**Command History**

- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series
show dot1x cos-mapping interface

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

Syntax

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

Parameters

- **interface**: Enter one of the following keywords and slot/port or number information:
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
  - For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.

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

Defaults

No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

- Version 8.4.6.0: Added support for the keyword `fortyGigE`.
- Version 8.4.2.1: Introduced on the C-Series and S-Series

Usage Information

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

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

Example
**Figure 8-1. show dot1x cos-mapping interface Command Example**

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

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

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

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

802.1p CoS re-map table for Supplicant: 00:00:01:00:07:00

----------------------------------
Dot1p       Remapped Dot1p
0           7
1           6
2           5
3           4
4           3
5           2
6           1
7           0
```
show dot1x interface

Display the 802.1X configuration of an interface.

Syntax

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

Parameters

- **interface**: Enter one of the following keywords and slot/port or number information:
  - For a Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For a Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.
  - For a Ten Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

- **mac-address**: (Optional) MAC address of a supplicant.

Defaults

No default values or behavior

Command Modes

- EXEC
- EXEC privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced <strong>mac-address</strong> option on the C-Series and S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

Usage Information

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

If 802.1X multi-suppliant authentication is enabled on a port, additional 802.1X configuration details (port authentication status, untagged VLAN ID, authentication PAE state, and backend state) are displayed for each supplicant as shown in Figure 8-4.

Example

---

[Example output]

---
Figure 8-2.  show dot1x interface Command Example

FTOS#show dot1x int Gi 2/32

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

Auth PAE State:      Initialize
Backend State:       Initialize

FTOS#

Figure 8-3.  show dot1x interface mac-address Command Example

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

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

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

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

FTOS#
Figure 8-4. show dot1x interface (with Multi-Supplicant Authentication enabled) Example

FTOS#show dot1x interface g 0/21

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

Port status and State info for Supplicant: 00:00:00:00:00:10
Port Auth Status: AUTHORIZED
Untagged VLAN id: 400
Auth PAE State: Authenticated
Backend State: Idle

Port status and State info for Supplicant: 00:00:00:00:00:11
Port Auth Status: AUTHORIZED
Untagged VLAN id: 300
Auth PAE State: Authenticated
Backend State: Idle

Port status and State info for Supplicant: 00:00:00:00:00:15
Port Auth Status: AUTHORIZED(GUEST-VLAN)
Untagged VLAN id: 100
Auth PAE State: Authenticated
Backend State: Idle
Access Control Lists (ACL)

Overview

Access Control Lists (ACLs) are supported on platforms E S.

Dell Networking OS supports the following types of Access Control List (ACL), IP prefix list, and route map:

- 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
- AS-Path Commands
- IP Community List Commands

Note: For ACL commands used in the Trace function, see the section Trace List Commands in the chapter Security.

Note: For IPv6 ACL commands, see Chapter 25, IPv6 Access Control Lists (IPv6 ACLs).

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
- show config
description

Configure a short text string describing the ACL.

Syntax
description text

Parameters
text Enter a text string up to 80 characters long.

Defaults Not enabled.

Command Modes
CONFIGURATION-STANDARD-ACCESS-LIST
CONFIGURATION-EXTENDED-ACCESS-LIST
CONFIGURATION-MAC ACCESS LIST-STANDARD
CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

remark

Enter a description for an ACL entry.

Syntax
remark [remark-number] [description]

Parameters
remark-number Enter the remark number. Note that the same sequence number can be used 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-STANDARD-ACCESS-LIST
CONFIGURATION-EXTENDED-ACCESS-LIST
CONFIGURATION-MAC ACCESS LIST-STANDARD
CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.4.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

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 the CONFIGURATION-STANDARD-ACCESS-LIST mode. Here, the same sequence number was used for the remark and for an associated ACL rule. The remark will precede 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 Figure 9-1. Command Example: remark

```
FTOS(config-std-nacl)#remark 10 Deny rest of the traffic
FTOS(config-std-nacl)#remark 5 Permit traffic from XYZ Inc.
FTOS(config-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(config-std-nacl)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show config</td>
<td>Display the current ACL configuration.</td>
</tr>
</tbody>
</table>

show config

Display the current ACL configuration.

Syntax

```
show config
```

Command Modes

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

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example Figure 9-2. Command Example: show config

```
FTOS(config-ext-nacl)#show conf
!
ip access-list extended patches
FTOS(config-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.
and S platforms support Ingress IP ACLs only.

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>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced</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>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
ip access-group

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

**Syntax**

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

**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. **Note**: Available only on 12-port 1-Gigabit Ethernet FLEX line card. Refer to your line card documentation for specifications. Not available on S-Series.
- `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 number of the VLANs. Range: 1 to 4094, 1-2094 for ExaScale (can used IDs 1-4094)
- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.

**Defaults**

Not enabled.

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

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

**Note:** This command is supported on the loopback interfaces of EE3, and EF series RPMs. It is *not* supported on loopback interfaces ED series RPM, or on C-Series or S-Series loopback interfaces.

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

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

**Related Commands**

- `ip access-list standard`: Configure a standard ACL.
- `ip access-list extended`: Configure an extended ACL.
show ip access-lists

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

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-name</td>
<td>Enter the name of a configured MAC ACL, up to 140 characters.</td>
</tr>
<tr>
<td>interface interface</td>
<td>Enter the keyword <code>interface</code> followed by the one of the following keywords</td>
</tr>
<tr>
<td></td>
<td>and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>- For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code></td>
</tr>
<tr>
<td></td>
<td>followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a Port Channel interface, enter the keyword <code>port-channel</code></td>
</tr>
<tr>
<td></td>
<td>followed by a number:</td>
</tr>
<tr>
<td></td>
<td>C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 255 for TeraScale and 1 - 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>- For a SONET interface, enter the keyword <code>sonet</code></td>
</tr>
<tr>
<td></td>
<td>followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code></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 <code>fortyGigE</code></td>
</tr>
<tr>
<td></td>
<td>followed by the slot/port information.</td>
</tr>
<tr>
<td>in</td>
<td>out</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 63.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

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 [vrf vrf-name]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-name</td>
<td>Enter the name of the ACL to be displayed.</td>
</tr>
<tr>
<td>cam_count</td>
<td>List the count of the CAM rules for this ACL.</td>
</tr>
</tbody>
</table>
**interface interface** Enter the keyword **interface** followed by the interface type and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
- For a Port Channel interface, enter the keyword **port-channel** followed by a number:
  - **C-Series and S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword **sonet** followed by the 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.

**vrf vrf-name** (OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>EXEC Privilege</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

**Figure 9-3. Command Example: show ip accounting access-lists**

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

Table 9-1 defines the information in **Figure 9-3**.

**Table 9-1. 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.

C and S platforms support Ingress IP ACLs only.

The commands needed to configure a Standard IP ACL are:

- `deny`
- `ip access-list standard`
- `permit`
- `resequence access-list`
- `resequence prefix-list ipv4`
- `seq`

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] | log [dscp value] [order] [monitor] [fragments]}
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- 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 <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 only.</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>log</td>
<td>(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to enter ACL matches in the log.</td>
</tr>
<tr>
<td>dscp</td>
<td>(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DCSCP values.</td>
</tr>
<tr>
<td>order</td>
<td>(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS order of priority for the ACL entry.</td>
</tr>
<tr>
<td></td>
<td>Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)</td>
</tr>
<tr>
<td></td>
<td>Default: If the order keyword is not used, the ACLs have the lowest order by default(255).</td>
</tr>
</tbody>
</table>
**monitor** (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

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

---

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION-STANDARD-ACCESS-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Add DSCP value for ACL matching.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the <code>monitor</code> option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Expanded to include the optional QoS <code>order</code> priority for the ACL entry.</td>
</tr>
</tbody>
</table>

**Usage Information**

The `order` option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the `log` option, CP processor logs details about the packets that match. Depending on how many packets match the `log` entry and at what rate, the CP may become busy as it has to log these packets’ details.

The `monitor` option is relevant in the context of flow-based monitoring only. See the Chapter 44, Port Monitoring.

The C-Series and S-Series cannot count both packets and bytes, so when you enter the `count byte` options, only bytes are incremented.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list standard</code></td>
<td>Configure a standard ACL.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Configure a permit filter.</td>
</tr>
</tbody>
</table>

**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

Command History

Usage Information

Example

Figure 9-4. Command Example: ip access-list standard

Related Commands

permit

Syntax

Parameters

Enter the IP address in dotted decimal format of the network from which the packet was sent.

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

Enter the keyword any to specify that all routes are subject to the filter.

Enter the keyword host followed by the IP address to specify a host IP address or host name.

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

(Optional) Enter the keyword dscp to match to the IP DSCP values.

(Optional) Enter the keyword byte to count bytes processed by the filter.
**log**  
(Optional, E-Series only) Enter the keyword log to enter ACL matches in the log.

**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).

**monitor**  
(Optional) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

**Usage Information**

The order option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the log option, CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The monitor option is relevant in the context of flow-based monitoring only. See Chapter 44, Port Monitoring.

The C-Series and S-Series cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

**Related Commands**

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

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

**Syntax**

```
resequence access-list {ipv4 | ipv6 | mac} {access-list-name StartingSeqNum Step-to-Increment}
```

**Parameters**

- **ipv4 | ipv6 | 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 - 4294967290
- **Step-to-Increment**: Enter the step to increment the sequence number. Range: 1 - 4294967290

**Defaults**

No default values or behavior

**Command Modes**

EXEC
EXEC Privilege

**Command History**

- Version 8.2.1.0 Introduced on E-Series ExaScale (IPv6)
- Version 8.1.1.0 Introduced on E-Series ExaScale (IPv4)
- Version 7.8.1.0 Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 7.4.1.0 Introduced

**Usage Information**

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

**Related Commands**

- `resequence prefix-list ipv4` Resequence 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 – 65535
- **Step-to-Increment**: Enter the step to increment the sequence number. Range: 1 – 65535

**Defaults**

No default values or behavior
Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

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

### Parameters

- **sequence-number**: Enter a number from 0 to 4294967290.
- **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.
- **source**: Enter a IP address in dotted decimal format of the network from which the packet was received.
- **mask**: (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.
- **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 or hostname.
- **count**: (OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
- **byte**: (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
- **log**: (OPTIONAL, E-Series only) Enter the keyword `log` to enter ACL matches in the log.
- **dscp**: (OPTIONAL) Enter the keyword `dscp` to match to the IP DCSCP values.
**order**  
(Optional) Enter the keyword `order` to specify the QoS order 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).

**monitor**  
(Optional) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

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

**Defaults**  
Not configured

**Command Modes**  
CONFIGURATION-STANDARD-ACCESS-LIST

**Command History**  
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Add DSCP value for ACL matching.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the <code>monitor</code> option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <code>order</code> priority for the ACL entry.</td>
</tr>
</tbody>
</table>

**Usage Information**  
The `monitor` option is relevant in the context of flow-based monitoring only. See Chapter 44, Port Monitoring.

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.

When you use the `log` option, CP processor logs details about the packets that match. Depending on how many packets match the `log` entry and at what rate, the CP may become busy as it has to log these packets’ details.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

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

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

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

**c** and **s** platforms support Ingress IP ACLs only.

- deny
- deny arp
- deny ether-type
- deny icmp
- deny tcp
- deny udp
- ip access-list extended
- permit
- permit arp
- permit ether-type
- permit icmp
- permit tcp
- permit udp
- resequence access-list
- resequence prefix-list ipv4
- seq arp
- seq ether-type
- seq

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

deny

**c** **e** **s**

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

**Syntax**

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

To remove this filter, you have two choices:

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Enter the keyword <code>ip</code> to configure a generic IP access list. The keyword <code>ip</code> specifies that the access list will 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>
</tbody>
</table>
### Command Modes

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Add DSCP value for ACL matching.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the <strong>monitor</strong> option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <strong>order</strong> priority for the ACL entry.</td>
</tr>
</tbody>
</table>

### Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

The C-Series and S-Series cannot count both packets and bytes, so when you enter the **count byte** options, only bytes are incremented.
The **monitor** option is relevant in the context of flow-based monitoring only. See the Chapter 44, Port Monitoring.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny tcp</td>
<td>Assign a filter to deny TCP packets.</td>
</tr>
<tr>
<td>deny udp</td>
<td>Assign a filter to deny UDP packets.</td>
</tr>
<tr>
<td>ip access-list extended</td>
<td>Create an extended ACL.</td>
</tr>
</tbody>
</table>

---

### deny arp

Configure an egress filter that drops ARP packets on egress ACL supported line cards (see your line card documentation).

#### Syntax

```
deny arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number} [count | byte] [log] [order] [monitor]
```

To remove this filter, use one of the following:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no deny arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number}` command.

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-mac-address</td>
<td>Enter a MAC address and mask in the nn:nn:nn:nn:nn format.</td>
</tr>
<tr>
<td>mac-address-mask</td>
<td>For the MAC address mask, specify which bits in the MAC address must match.</td>
</tr>
<tr>
<td></td>
<td>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>any</td>
<td>Enter the keyword <code>any</code> to match and drop any ARP traffic on the interface.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>Enter the keyword <code>vlan</code> followed by the VLAN ID to filter traffic</td>
</tr>
<tr>
<td></td>
<td>associated with a specific VLAN.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Enter an IP address in dotted decimal format (A.B.C.D) as the target IP</td>
</tr>
<tr>
<td></td>
<td>address of the ARP.</td>
</tr>
<tr>
<td>opcode code-number</td>
<td>Enter the keyword <code>opcode</code> followed by the number of the ARP opcode.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 23.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the</td>
</tr>
<tr>
<td></td>
<td>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>log</td>
<td>(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to have the information</td>
</tr>
<tr>
<td></td>
<td>kept in an ACL log file.</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).

### monitor

(Optional) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

---

### deny ether-type

Configure an egress filter that drops specified types of Ethernet packets on egress ACL supported line cards (see your line card documentation).

**Syntax**

```markdown
deny ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any} [count [byte] | log] [order] [monitor]
```

To remove this filter, use one of the following:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or...
Use the **no deny ether-type protocol-type-number \( \text{destination-mac-address} \) mac-address-mask \{ any \} vlan vlan-id \{ source-mac-address mac-address-mask \| any \}** command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protocol-type-number</strong></td>
<td>Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.</td>
</tr>
<tr>
<td><strong>destination-mac-address</strong> &lt;br&gt; <strong>mac-address-mask</strong></td>
<td>Enter a MAC address and mask in the ( \text{nn:nn:nn:nn:nn} ) format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ( \text{ff:ff:ff:ff:ff:ff} ) allows entries that do not match and a mask of ( \text{00:00:00:00:00:00} ) only allows entries that match exactly.</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Enter the keyword <strong>any</strong> to match and drop specific Ethernet traffic on the interface.</td>
</tr>
<tr>
<td><strong>vlan vlan-id</strong></td>
<td>Enter the keyword <strong>vlan</strong> followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094, 1-2094 for ExaScale (can used IDs 1-4094) To filter all VLAN traffic specify VLAN 1.</td>
</tr>
<tr>
<td><strong>source-mac-address</strong> &lt;br&gt; <strong>mac-address-mask</strong></td>
<td>Enter a MAC address and mask in the ( \text{nn:nn:nn:nn:nn} ) format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ( \text{ff:ff:ff:ff:ff:ff} ) allows entries that do not match and a mask of ( \text{00:00:00:00:00:00} ) only allows entries that match exactly.</td>
</tr>
<tr>
<td><strong>count</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>count</strong> to count packets processed by the filter.</td>
</tr>
<tr>
<td><strong>byte</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>byte</strong> to count bytes processed by the filter.</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td>(OPTIONAL, E-Series only) Enter the keyword <strong>log</strong> to have the information kept in an ACL log file.</td>
</tr>
<tr>
<td><strong>order</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>order</strong> 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>monitor</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>monitor</strong> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

**CONFIGURATION-EXTENDED-ACCESS-LIST**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added <strong>monitor</strong> option</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <strong>order</strong> priority for the ACL entry.</td>
</tr>
</tbody>
</table>
The **order** option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide* for more information.

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

The **monitor** option is relevant in the context of flow-based monitoring only. See Chapter 44, Port Monitoring.

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs (ARP and Ether-type) to Layer 2 interfaces only.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

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] | log] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the **no seq sequence-number** command if you know the filter’s sequence number or
- Use the **no deny icmp {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><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>destination</strong></td>
<td>Enter the IP address of the network or host to which the packets are sent.</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>message-type</strong></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 9-2). Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code</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>log</strong></td>
<td>(OPTIONAL, E-Series only) Enter the keyword log to have the information kept in an ACL log file.</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).

**monitor**

(Optional) Enter the keyword **monitor** when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

**fragments**

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

---

**Defaults**

Not configured

**Command Modes**

CONFIGURATION-EXTENDED-ACCESS-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added <strong>dscp</strong> keyword.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the <strong>monitor</strong> option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <strong>order</strong> priority for the ACL entry.</td>
</tr>
</tbody>
</table>

**Usage Information**

The **order** option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

The **monitor** option is relevant in the context of flow-based monitoring only. See Chapter 44, Port Monitoring.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

**Table 9-2** lists the keywords displayed in the CLI help and their corresponding ICMP Message Type Name.

**Table 9-2. ICMP Message Type Keywords**

<table>
<thead>
<tr>
<th><strong>Keyword</strong></th>
<th><strong>ICMP Message Type Name</strong></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>
</tbody>
</table>
Table 9-2. ICMP Message Type Keywords

<table>
<thead>
<tr>
<th>Keyword</th>
<th>ICMP Message Type Name</th>
</tr>
</thead>
<tbody>
<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>
<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>
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] | log] [order] [monitor] [fragments]

To remove this filter, you have two choices:

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword host followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td>dscp</td>
<td>Enter this keyword to deny a packet based on DSCP value. Range: 0-63</td>
</tr>
<tr>
<td>bit</td>
<td>Enter a flag or combination of bits: ack: acknowledgement field fin: finish (no more data from the user) psh: push function rst: reset the connection syn: synchronize sequence numbers urg: urgent field</td>
</tr>
<tr>
<td>operator</td>
<td>(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 command parameter.</td>
</tr>
<tr>
<td>port</td>
<td>Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535.</td>
</tr>
<tr>
<td>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>Command</td>
<td>Usage Information</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword <strong>byte</strong> to count bytes processed by the filter.</td>
</tr>
<tr>
<td>log</td>
<td>(OPTIONAL, E-Series only) Enter the keyword <strong>log</strong> to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.</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). |
| monitor  | (OPTIONAL) Enter the keyword **monitor** when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide. |
| fragments| Enter the keyword **fragments** to use ACLs to control packet fragments. |

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION-EXTENDED-ACCESS-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added <strong>dscp</strong> keyword.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the <strong>monitor</strong> option. Deprecated <strong>established</strong> keyword.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <strong>order</strong> priority for the ACL entry.</td>
</tr>
</tbody>
</table>

**Usage Information**

The **order** option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

The C-Series and S-Series cannot count both packets and bytes, so when you enter the **count byte** options, only bytes are incremented.

The **monitor** option is relevant in the context of flow-based monitoring only. See Chapter 44, Port Monitoring.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

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 8 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>1111111111000000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111100000</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>1111110000000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111000000000</td>
<td>1111111000000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111110000000</td>
<td>1111111111000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111110100000</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>Assign a filter to deny IP traffic.</td>
</tr>
<tr>
<td>deny udp</td>
<td>Assign a filter to deny UDP traffic.</td>
</tr>
</tbody>
</table>

**deny udp**

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

**Syntax**

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

To remove this filter, you have two choices:

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><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 <strong>any</strong> to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td><strong>host ip-address</strong></td>
<td>Enter the keyword <strong>host</strong> 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>
</tbody>
</table>
operator  (OPTIONAL) Enter one of the following logical operand:
   • eq = equal to
   • neq = not equal to
   • gt = greater than
   • lt = less than
   • range = inclusive range of ports

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.

log  (OPTIONAL, E-Series only) Enter the keyword log to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.

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).

monitor  (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

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

Defaults  Not configured

Command Modes  CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added dscp keyword.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>

Usage Information

The order option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the log option, CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.
The C-Series and S-Series cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

The monitor option is relevant in the context of flow-based monitoring only. See the Chapter 44, Port Monitoring.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

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 8 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 1111111111100000 4000  4031  32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0000111111000000 1111111111000000 4032  4095  64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000 1111100000000000 4096  6143  2048</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000 1111100000000000 6144  7167  1024</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0001111000000000 1111111000000000 7168  7679  512</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0001111100000000 1111111100000000 7680  7935  256</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0001111101000000 1111111111000000 7936  7999  64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0001111110000000 1111111111100000 8000  8000  1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Ports: 4001

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

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

Total Ports: 1024

### Related Commands
- **deny** Assign a deny filter for IP traffic.
- **deny tcp** Assign a deny filter for TCP traffic.

### ip access-list extended

**Syntax**
```
ip access-list extended access-list-name
```

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

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

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

**Command Modes**
CONFIGURATION
Command History

<table>
<thead>
<tr>
<th>Version 8.1.1.0</th>
<th>Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Prior to 7.8.1.0, names are up to 16 characters long.

Example

**Figure 9-5. Command Example: ip access-list extended**

```
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>Configure a standard IP access list.</td>
</tr>
<tr>
<td>show config</td>
<td>Display 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] | log] [dscp value] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Enter the keyword <code>ip</code> to configure a generic IP access list. The keyword <code>ip</code> specifies that the access list will permit all IP protocols.</td>
</tr>
<tr>
<td>ip-protocol-number</td>
<td>Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header.</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>
</tbody>
</table>
### log
(Optional, E-Series only) Enter the keyword **log** to enter ACL matches in the log.

### dscp
(Optional) Enter the keyword **dscp** to match to the IP DSCP values.

### order
(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).

### monitor
(Optional) Enter the keyword **monitor** when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

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

---

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION-EXTENDED-ACCESS-LIST

**Command History**
- **Version 8.3.1.0** Add DSCP value for ACL matching.
- **Version 8.2.1.0** Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Support added for S-Series
- **Version 7.5.1.0** Support added for C-Series
- **Version 7.4.1.0** Added support for non-contiguous mask and added the **monitor** option.
- **Version 6.5.10** Expanded to include the optional QoS **order** priority for the ACL entry.

**Usage Information**
The **order** option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

The C-Series and S-Series cannot count both packets and bytes, so when you enter the **count byte** options, only bytes are incremented.

The **monitor** option is relevant in the context of flow-based monitoring only. See the Chapter 44, Port Monitoring.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

**Related Commands**
- **ip access-list extended** Create an extended ACL.
- **permit tcp** Assign a permit filter for TCP packets.
- **permit udp** Assign a permit filter for UDP packets.
permit arp

Configure a filter that forwards ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax

```
permit arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number} [count | byte | log | order | monitor | [fragments]
```

To remove this filter, use one of the following:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no permit arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number}` command.

Parameters

- **destination-mac-address**
  - **mac-address-mask**
    - Enter a MAC address and mask in the nn:nn:nn:nn:nn format.
    - For the MAC address mask, 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.

- **any**
  - Enter the keyword `any` to match and drop any ARP traffic on the interface.

- **vlan vlan-id**
  - Enter the keyword `vlan` followed by the VLAN ID to filter traffic associated with a specific VLAN.
  - Range: 1 to 4094, 1-2094 for ExaScale (can use IDs 1-4094)
  - To filter all VLAN traffic specify VLAN 1.

- **ip-address**
  - Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.

- **opcode code-number**
  - Enter the keyword `opcode` followed by the number of the ARP opcode.
  - Range: 1 to 16.

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

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

- **log**
  - (OPTIONAL, E-Series only) Enter the keyword `log` to have the information kept in an ACL log file.

- **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).

- **monitor**
  - (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

- **fragments**
  - Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults

- Not configured.

Command Modes

- `CONFIGURATION-EXTENDED-ACCESS-LIST`
**Access Control Lists (ACL)**

The **order** option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide* for more information.

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

The **monitor** option is relevant in the context of flow-based monitoring only. See the Chapter 44, Port Monitoring.

You cannot include IP, TCP or UDP filters in an ACL configured with ARP filters.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

### permit ether-type

Configure a filter that allows traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

**Syntax**

```
permit ether-type protocol-type-number \{destination-mac-address mac-address-mask | any\} vlan vlan-id \{source-mac-address mac-address-mask | any\} [count [byte] | log] [order] [monitor]
```

To remove this filter, use one of the following:

- Use the **no seq** sequence-number command syntax if you know the filter’s sequence number or
- Use the **no permit ether-type protocol-type-number \{destination-mac-address mac-address-mask | any\} vlan vlan-id \{source-mac-address mac-address-mask | any\}** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protocol-type-number</strong></td>
<td>Enter a number from 600 to FFF as the specific Ethernet type traffic to drop.</td>
</tr>
<tr>
<td><strong>destination-mac-address</strong></td>
<td>Enter a MAC address and mask in the nn:nn:nn:nn:nn:nn format. For the MAC address mask, 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><strong>any</strong></td>
<td>Enter the keyword any to match and drop specific Ethernet traffic on the interface.</td>
</tr>
<tr>
<td><strong>vlan vlan-id</strong></td>
<td>Enter the keyword vlan followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094, 1-2094 for ExaScale (can used IDs 1-4094) To filter all VLAN traffic specify VLAN 1.</td>
</tr>
</tbody>
</table>
source-mac-address  
mac-address-mask

For the MAC address mask, 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.

count

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

byte

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

log

(Optional, E-Series only) Enter the keyword log to have the information kept in an ACL log file.

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).

monitor

(Optional) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

Defaults
Not configured.

Command Modes
CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added monitor option</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>

Usage Information

The order option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the log option, CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The monitor option is relevant in the context of the flow-based monitoring feature only. See Chapter 44, Port Monitoring.

You cannot include IP, TCP or UDP filters in an ACL configured with ARP filters.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.
permit icmp

Configure a filter to allow all or specific ICMP messages.

**Syntax**

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

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- 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 9-2). 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.
- **log**: (OPTIONAL, E-Series only) Enter the keyword `log` to have the information kept in an ACL log file.
- **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).
- **monitor**: (OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.
- **fragments**: Enter the keyword `fragments` to use ACLs to control packet fragments.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION-STANDARD-ACCESS-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added <code>dscp</code> keyword.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the <code>monitor</code> option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <code>order</code> priority for the ACL entry.</td>
</tr>
</tbody>
</table>
The order option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the Dell Networking OS Configuration Guide for more information.

When you use the log option, CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

The monitor option is relevant in the context of the flow-based monitoring feature only. See Chapter 44, Port Monitoring.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

### permit tcp

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

**Syntax**

```
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] | log] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the **no seq sequence-number** command syntax if you know the filter’s sequence number or
- Use the **no permit tcp {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.
- **bit** Enter a flag or combination of bits:
  - **ack**: acknowledgement field
  - **fin**: finish (no more data from the user)
  - **psh**: push function
  - **rst**: reset the connection
  - **syn**: synchronize sequence numbers
  - **urg**: urgent field
- **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 port for the **port** parameter.)
**port port**
Enter the application layer port number. Enter two port numbers if using the range logical operand.
Range: 0 to 65535.
The following list includes some common TCP port numbers:
23 = Telnet
20 and 21 = FTP
25 = SMTP
169 = SNMP

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

**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.

**log**
(Optional, E-Series only) Enter the keyword **log** to enter ACL matches in the log.

**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).

**monitor**
(Optional) Enter the keyword **monitor** when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

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

### Defaults
Not configured.

### Command Modes
**CONFIGURATION-EXTENDED-ACCESS-LIST**

<table>
<thead>
<tr>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added <strong>dscp</strong> keyword.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the <strong>monitor</strong> option. Deprecated <strong>established</strong> keyword.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <strong>order</strong> priority for the ACL entry.</td>
</tr>
</tbody>
</table>

### Usage Information
The order option is relevant in the context of the Policy QoS feature only. See the Quality of Service chapter of the Dell Networking OS Configuration Guide for more information.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See Chapter 44, Port Monitoring.
When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

The C-Series and S-Series 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 8 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>1111111111110000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111110000</td>
<td>1111111110000000</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>0001111100000000</td>
<td>1111111100000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111110000000</td>
<td>1111111110000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111111010000</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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list extended</td>
<td>Create an extended ACL.</td>
</tr>
<tr>
<td>permit</td>
<td>Assign a permit filter for IP packets.</td>
</tr>
<tr>
<td>permit udp</td>
<td>Assign a permit filter for UDP packets.</td>
</tr>
</tbody>
</table>

**permit udp**

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

**Syntax**

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

To remove this filter, you have two choices:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td>host ip-address</td>
<td>Enter the keyword host followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td>dscp</td>
<td>Enter this keyword to deny a packet based on DSCP value. Range: 0-63</td>
</tr>
<tr>
<td>operator</td>
<td>(OPTIONAL) Enter one of the following logical operand:</td>
</tr>
<tr>
<td></td>
<td>• eq = equal to</td>
</tr>
<tr>
<td></td>
<td>• neq = not equal to</td>
</tr>
<tr>
<td></td>
<td>• gt = greater than</td>
</tr>
<tr>
<td></td>
<td>• lt = less than</td>
</tr>
<tr>
<td></td>
<td>• range = inclusive range of ports (you must specify two ports for the port parameter.)</td>
</tr>
<tr>
<td>port port</td>
<td>(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535</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>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.</td>
</tr>
<tr>
<td>log</td>
<td>(OPTIONAL, E-Series only) Enter the keyword log to enter ACL matches in the log.</td>
</tr>
<tr>
<td>order</td>
<td>(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the order keyword is not used, the ACLs have the lowest order by default (255).</td>
</tr>
<tr>
<td>monitor</td>
<td>(OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.</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-EXTENDED-ACCESS-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added dscp keyword.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>

Usage Information

The order option is relevant in the context of the Policy QoS feature only. See the Quality of Service chapter of the Dell Networking OS Configuration Guide for more information.
The **monitor** option is relevant in the context of the flow-based monitoring feature only. See Chapter 44, Port Monitoring.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packet’s details.

The C-Series and S-Series 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 8 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 1111111110000000 4000  4031  32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0000111111000000 1111111110000000 4032  4095  64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000 1111100000000000 4096  6143  2048</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000 1111110000000000 6144  7167  1024</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000 1111111000000000 7168  7679  512</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0001111000000000 1111111100000000 7680  7935  256</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000 1111111110000000 7936  7999  64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0001111110000000 1111111111000000 8000  8000  1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Ports: 4001

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

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

Total Ports: 1024

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list extended</code></td>
<td>Configure an extended ACL.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Assign a permit filter for IP packets.</td>
</tr>
<tr>
<td><code>permit tcp</code></td>
<td>Assign a permit filter for TCP packets.</td>
</tr>
</tbody>
</table>

**Syntax**

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ipv4</td>
<td>mac`</td>
</tr>
<tr>
<td><code>access-list-name</code></td>
<td>Enter the name of a configured IP access list, up to 140 characters.</td>
</tr>
<tr>
<td><code>StartingSeqNum</code></td>
<td>Enter the starting sequence number to resequence.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 - 4294967290</td>
</tr>
<tr>
<td><code>Step-to-Increment</code></td>
<td>Enter the step to increment the sequence number.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 - 4294967290</td>
</tr>
</tbody>
</table>

### Defaults

No default values or behavior

### Command Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

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

Prior to 7.8.1.0, names are up to 16 characters long.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>resequence prefix-list ipv4</code></td>
<td>Resequence a prefix list</td>
</tr>
</tbody>
</table>

---

### resequence prefix-list ipv4

C E S

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

**Syntax**

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

**Parameters**

<table>
<thead>
<tr>
<th>Name</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 long.</td>
</tr>
<tr>
<td><code>StartingSeqNum</code></td>
<td>Enter the starting sequence number to resequence.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 – 65535</td>
</tr>
<tr>
<td><code>Step-to-Increment</code></td>
<td>Enter the step to increment the sequence number.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 – 65535</td>
</tr>
</tbody>
</table>

**Defaults**

No default values or behavior

**Command Modes**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
</tbody>
</table>

---
Usage Information

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

Prior to 7.8.1.0, names are up to 16 characters long.

Related Commands

resquence access-list Resequence an access-list

seq arp

Configure an egress filter with a sequence number that filters ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax

```
seq sequence-number {deny | permit} arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number} [count [byte] | log | order] [monitor]
```

To remove this filter, use the no seq sequence-number command.

Parameters

- **sequence-number**: Enter a number from 0 to 4294967290.
- **deny**: Enter the keyword deny to drop all traffic meeting the filter criteria.
- **permit**: Enter the keyword permit to forward all traffic meeting the filter criteria.
- **destination-mac-address mac-address-mask**: Enter a MAC address and mask in the nn:nn:nn:nn:nn:nn format. For the MAC address mask, 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.
- **any**: Enter the keyword any to match and drop any ARP traffic on the interface.
- **vlan vlan-id**: Enter the keyword vlan followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094, 1-2094 for ExaScale (can used IDs 1-4094) To filter all VLAN traffic specify VLAN 1.
- **ip-address**: Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
- **opcode code-number**: Enter the keyword opcode followed by the number of the ARP opcode. Range: 1 to 16.
- **count**: (OPTIONAL) Enter the keyword count to count packets processed by the filter.
- **byte**: (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.
- **log**: (OPTIONAL, E-Series only) Enter the keyword log to have the information kept in an ACL log file.

Version 7.6.1.0 Added support for S-Series
Version 7.5.1.0 Added support for C-Series
Version 7.4.1.0 Introduced for E-Series
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).

monitor  

(Optional) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

Defaults

Not configured.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added <code>monitor</code> option</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS <code>order</code> priority for the ACL entry.</td>
</tr>
</tbody>
</table>

Usage Information

The `monitor` option is relevant in the context of the flow-based monitoring feature only. See Chapter 44, Port Monitoring.

When you use the `log` option, CP processor logs details about the packets that match. Depending on how many packets match the `log` entry and at what rate, the CP may become busy as it has to log these packets’ details.

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.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs to interfaces in Layer 2 mode.
seq ether-type

Configure an egress filter with a specific sequence number that filters traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

**Syntax**

```
seq sequence-number {deny | permit} ether-type protocol-type-number
{destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any} [count [byte] | log [order] [monitor]
```

**Parameters**

- `sequence-number` Enter a number from 0 to 4294967290.
- `deny` Enter the keyword `deny` to drop all traffic meeting the filter criteria.
- `permit` Enter the keyword `permit` to forward all traffic meeting the filter criteria.
- `protocol-type-number` Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.
- `destination-mac-address` Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, 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.
- `any` Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
- `vlan vlan-id` Enter the keyword `vlan` followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094, 1 to 2094 for ExaScale (can use IDs 1 to 4094) To filter all VLAN traffic specify VLAN 1.
- `source-mac-address` Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, 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.
- `count` (OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
- `byte` (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
- `log` (OPTIONAL, E-Series only) Enter the keyword `log` to have the information kept in an ACL log file.
- `order` (OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. Range: 0 to 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).
- `monitor` (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

**Defaults**

Not configured.
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] [log] [dscp value] [order] [monitor] [fragments]
```

Parameters

- `sequence-number` Enter a number from 0 to 4294967290.
- `deny` Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
- `permit` Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
- `ip-protocol-number` Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
- `icmp` Enter the keyword `icmp` to configure an ICMP access list filter.
- `ip` Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list will permit all IP protocols.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>Enter the keyword tcp to configure a TCP access list filter.</td>
</tr>
<tr>
<td>udp</td>
<td>Enter the keyword udp 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 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>
</tbody>
</table>
| operator | (OPTIONAL) Enter one of the following logical operands:  
- `eq` = equal to  
- `neq` = not equal to  
- `gt` = greater than  
- `lt` = less than  
- `range` = inclusive range of ports (you must specify two ports for the `port` parameter.) |
| port port | (OPTIONAL) Enter the application layer port number. Enter two port numbers if using the `range` logical operand.  
Range: 0 to 65535  
The following list includes some common TCP port numbers:  
- 23 = Telnet  
- 20 and 21 = FTP  
- 25 = SMTP  
- 169 = SNMP |
| destination | Enter the IP address of the network or host to which the packets are sent. |
| message-type | (OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 9-2).  
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. |
| log | (OPTIONAL, E-Series only) Enter the keyword log to enter ACL matches in the log. Supported on Jumbo-enabled line cards only. |
| dscp | (OPTIONAL) Enter the keyword dscp to match to the IP DCSCP values. |
| order | (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry.  
Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority)  
Default: If the order keyword is not used, the ACLs have the lowest order by default (255). |
| monitor | (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide. |
| fragments | Enter the keyword fragments to use ACLs to control packet fragments. |

**Defaults**

Not configured

**Command Modes**

CONFIGURATION-EXTENDED-ACCESS-LIST
The `monitor` option is relevant in the context of the flow-based monitoring feature only. See Chapter 44, Port Monitoring.

When you use the `log` option, CP processor logs details about the packets that match. Depending on how many packets match the `log` entry and at what rate, the CP may become busy as it has to log these packets’ details.

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.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Configure a filter to drop packets.</td>
</tr>
<tr>
<td>permit</td>
<td>Configure 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.

Platforms support Ingress MAC ACLs only.

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.

**Syntax**
clear counters mac access-group [mac-list-name]

**Parameters**

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

**Command Modes**
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version</td>
<td>Introduced for E-Series</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**

<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 access list, up to 140 characters.</td>
</tr>
<tr>
<td>vlan vlan-range</td>
<td>(OPTIONAL) Enter the keyword <strong>vlan</strong> followed a range of VLANs. Note that this option is available only with the <strong>in</strong> keyword option. Range: 1 to 4094, 1 to 2094 for ExaScale (can used IDs 1 to 4094)</td>
</tr>
<tr>
<td>in</td>
<td>Enter the keyword <strong>in</strong> to configure the ACL to filter incoming traffic.</td>
</tr>
<tr>
<td>out</td>
<td>Enter the keyword <strong>out</strong> to configure the ACL to filter outgoing traffic. Not available on S-Series.</td>
</tr>
</tbody>
</table>

**Defaults**
No default behavior or configuration

**Command Modes**
INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**
You can assign one ACL (standard or extended) to an interface.
Prior to 7.8.1.0, names are up to 16 characters long.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac access-list standard</td>
<td>Configure a standard MAC ACL.</td>
</tr>
<tr>
<td>mac access-list extended</td>
<td>Configure an extended MAC ACL.</td>
</tr>
</tbody>
</table>
show mac access-lists

Display 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 displayed.

**Syntax**

```
show mac access-lists [access-list-name] [interface interface] [in | out]
```

**Parameters**

- `access-list-name` Enter the name of a configured MAC ACL, up to 140 characters.
- `interface interface` Enter the keyword `interface` followed by the one of the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **C-Series** and **S-Series** Range: 1 to 128
    - **E-Series** Range: 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
- `in | out` Identify whether ACL is applied on ingress or egress side.

**Command Modes**

EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.4.1.0** Introduced

---

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
```

**Command Modes**

EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.4.1.0** Introduced
### Parameters

<table>
<thead>
<tr>
<th>access-list-name</th>
<th>Enter the name of a configured MAC ACL, up to 140 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface</td>
<td>Enter the keyword <code>interface</code> followed by the one of the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>• <strong>C-Series and S-Series</strong> Range: 1 to 128</td>
</tr>
<tr>
<td></td>
<td>• <strong>E-Series</strong> Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td>in</td>
<td>out</td>
</tr>
</tbody>
</table>

### Command Modes

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>EXEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command History</td>
<td>EXEC Privilege</td>
</tr>
<tr>
<td>Version 8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>Version 8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

### Example

**Figure 9-6. Command Example: show mac accounting access-list**

FTOS#show mac accounting access-list mac-ext interface po 1
Extended mac access-list mac-ext on GigabitEthernet 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 GigabitEthernet 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.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac accounting destination</td>
<td>Display destination counters for Layer 2 traffic (available on physical interfaces only).</td>
</tr>
</tbody>
</table>
Standard MAC ACL Commands

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

**C** and **S** platforms support Ingress MAC ACLs only.

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]] [log] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- 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><code>any</code></td>
<td>Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.</td>
</tr>
<tr>
<td><code>mac-source-address-mask</code></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><code>count</code></td>
<td>(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.</td>
</tr>
<tr>
<td><code>byte</code></td>
<td>(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to log the packets.</td>
</tr>
<tr>
<td><code>monitor</code></td>
<td>(OPTIONAL) Enter the keyword <code>monitor</code> when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.</td>
</tr>
</tbody>
</table>

**Defaults**

Not enabled.

**Command Modes**

- CONFIGURATION-MAC ACCESS LIST-STANDARD
When you use the `log` option, CP processor logs details about the packets that match. Depending on how many packets match the `log` entry and at what rate, the CP may become busy as it has to log these packets’ details.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>permit</code></td>
<td>Configure a MAC address filter to pass packets.</td>
</tr>
<tr>
<td><code>seq</code></td>
<td>Configure a MAC address filter with a specified sequence number.</td>
</tr>
</tbody>
</table>

### mac access-list standard

Name a new or existing MAC access control list (MAC ACL) and enter the MAC ACCESS LIST mode to configure a standard MAC ACL. See Commands Common to all ACL Types and Common MAC Access List Commands.

**Syntax**

```
mac access-list standard 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

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

Prior to 7.8.1.0, names are up to 16 characters long.

The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

C-Series and S-Series support ingress ACLs only.
**permit**

Configure a filter to forward packets from a specific source MAC address.

**Syntax**

```
permit {any | mac-source-address [mac-source-address-mask]} [count [byte]] [log] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- 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**

- **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.

- **log**
  - (OPTIONAL, E-Series only) Enter the keyword `log` to log the packets.

- **monitor**
  - (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

**Defaults**

Not configured.

**Command Modes**

- CONFIGURATION-MAC ACCESS LIST-STANDARD

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
When you use the log option, CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

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]]  [log]  [monitor]
```

**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-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.
- `log`: (OPTIONAL, E-Series only) Enter the keyword log to log the packets.
- `monitor`: (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

**Defaults**

Not configured.

**Command Modes**

- **CONFIGURATION-MAC ACCESS LIST-STANDARD**

**Command History**

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Support added for S-Series
- **Version 7.5.1.0** Support added for C-Series
Usage Information

When you use the log option, CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Configure a filter to drop packets.</td>
</tr>
<tr>
<td>permit</td>
<td>Configure a filter to forward packets.</td>
</tr>
</tbody>
</table>

Extended MAC ACL Commands

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

C and S platforms support Ingress MAC ACLs only.

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]] [log] [monitor]
```

**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>
</tbody>
</table>
## mac-source-address
Enter the source MAC address in nn:nn:nn:nn:nn:nn format.

## mac-source-address-mask
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.

## mac-destination-address
Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.

## mac-destination-address-mask
Specify which bits in the MAC address must 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.

## ethertype operator
(Optional) To filter based on protocol type, enter one of the following Ethertypes:
- ev2 - is the Ethernet II frame format.
- llc - is the IEEE 802.3 frame format.
- snap - is the IEEE 802.3 SNAP frame format.

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

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

## log
(Optional, E-Series only) Enter the keyword log to log the packets.

## monitor
(Optional) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

## Defaults
Not configured.

## Command Modes
CONFIGURATION-MAC ACCESS LIST-EXTENDED

## Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added monitor option</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

## Usage Information
When you use the log option, CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

## Related Commands
- **permit** Configure a filter to forward based on MAC addresses.
- **seq** Configure a filter with specific sequence numbers.
**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Prior to 7.8.1.0, names are up to 16 characters long.

**Example**

**Figure 9-8. Command Example: mac-access-list extended**

```
FTOS(conf)#mac-access-list access-list extended TestMATExt
FTOS(config-ext-macl)#remark 5 IPv4
FTOS(config-ext-macl)#seq 10 permit any any ev2 eq 800 count bytes
FTOS(config-ext-macl)#remark 15 ARP
FTOS(config-ext-macl)#seq 20 permit any any ev2 eq 806 count bytes
FTOS(config-ext-macl)#seq 30 permit any any ev2 eq 86dd count bytes
FTOS(config-ext-macl)#exit
FTOS(conf)#do show mac accounting access-list snickers interface g0/47 in

Extended mac access-list snickers on GigabitEthernet 0/47
seq 10  permit any any ev2 eq 800 count bytes (559851886 packets 191402152148 bytes)
seq 20  permit any any ev2 eq 806 count bytes (74481486 packets 5031686754 bytes)
seq 30  permit any any ev2 eq 86dd count bytes (7751519 packets 797843521 bytes)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac access-list standard</code></td>
<td>Configure a standard MAC access list.</td>
</tr>
<tr>
<td><code>show mac accounting access-list</code></td>
<td>Display MAC access list configurations and counters (if configured).</td>
</tr>
</tbody>
</table>
permit

Configure a filter to pass packets matching the criteria specified.

Syntax

```
permit {any | host mac-address | mac-source-address mac-source-address-mask} {any |
host mac-address | mac-destination-address mac-destination-address-mask} [ethertype
operator] [count [byte]] [log] [monitor]
```

To remove this filter, you have two choices:

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

Parameters

- **any**
  - Enter the keyword `any` to forward all packets.

- **host**
  - Enter the keyword `host` followed by a MAC address to forward packets with that host address.

- **mac-source-address**
  - Enter the source MAC address in nn:nn:nn:nn:nn:nn format.

- **mac-source-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.

- **mac-destination-address**
  - Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.

- **mac-destination-address-mask**
  - Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

- **ethertype operator**
  - (Optional) To filter based on protocol type, enter one of the following Ethertypes:
    - `ev2` - is the Ethernet II frame format.
    - `llc` - is the IEEE 802.3 frame format.
    - `snap` - is the IEEE 802.3 SNAP frame format.

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

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

- **log**
  - (Optional, E-Series only) Enter the keyword `log` to log the packets.

- **monitor**
  - (Optional) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the Dell Networking OS Configuration Guide.

Defaults

Not configured.

Command Modes

- **CONFIGURATION-MAC ACCESS LIST-EXTENDED**
When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

**Note:** When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>deny</strong></td>
<td>Configure a filter to drop traffic based on the MAC address.</td>
</tr>
<tr>
<td><strong>seq</strong></td>
<td>Configure a filter with specific sequence numbers.</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]] [log] [monitor]
```

**Parameters**

- **sequence-number**: Enter a number as the filter sequence number.
  Range: zero (0) to 65535.
- **deny**: Enter the keyword **deny** to drop any traffic matching this filter.
- **permit**: Enter the keyword **permit** to forward any traffic matching this filter.
- **any**: Enter the keyword **any** to filter all packets.
- **host mac-address**: Enter the keyword **host** followed by a MAC address to filter packets with that host address.
- **mac-source-address**: Enter the source MAC address in nn:nn:nn:nn:nn:nn format.
  The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
- **mac-source-address-mask**: Specify which bits in the MAC address must be matched.
- **mac-destination-address**: Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
- **mac-destination-address-mask**: Specify which bits in the MAC address must be matched.
  The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
- **ethertype operator**: (OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes:
  - **ev2** - is the Ethernet II frame format.
  - **llc** - is the IEEE 802.3 frame format.
  - **snap** - is the IEEE 802.3 SNAP frame format.
**count** (OPTIONAL) Enter the keyword **count** to count packets processed by the filter.

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

**log** (OPTIONAL, E-Series only) Enter the keyword **log** to log the packets.

**monitor** (OPTIONAL) Enter the keyword **monitor** when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule will be applied to the monitored interface. For details, see the section “Flow-based Monitoring” in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION-MAC ACCESS LIST-STANDARD

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced</td>
<td>on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support</td>
<td>added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support</td>
<td>added for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added</td>
<td>monitor option</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced</td>
<td>for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

When you use the **log** option, CP processor logs details about the packets that match. Depending on how many packets match the **log** entry and at what rate, the CP may become busy as it has to log these packets’ details.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

**Related Commands**

- **deny** Configure a filter to drop traffic.
- **permit** Configure a filter to forward traffic.

---

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-name</td>
<td>(OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Default

Clears "hit" counters for all prefix lists unless a prefix list is specified.

Related Commands

- `ip prefix-list` Configure a prefix list.

---

deny

Configure a filter to drop packets meeting the criteria specified.

Syntax

`deny ip-prefix [ge min-prefix-length] [le max-prefix-length]`

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-prefix</td>
<td>Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.</td>
</tr>
<tr>
<td>ge min-prefix-length</td>
<td>(OPTIONAL) Enter the keyword ge followed by the minimum prefix length, which is a number from zero (0) to 32.</td>
</tr>
<tr>
<td>le max-prefix-length</td>
<td>(OPTIONAL) Enter the keyword le followed by the maximum prefix length, which is a number from zero (0) to 32.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

PREFIX-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If the options `ge` or `le` are not used, only packets with an exact match to the prefix are filtered.
**ip prefix-list**

Enter the 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 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.8.1.0 Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

**Usage Information**

Prefix lists redistribute OSPF and RIP routes meeting specific criteria. For related RIP commands supported on C-Series and E-Series, see Chapter 48, Router Information Protocol (RIP). For related OSPF commands supported on all three platforms, see Chapter 38, Open Shortest Path First (OSPFv2 and OSPFv3).

Prior to 7.8.1.0, names are up to 16 characters long.

**Related Commands**

- `show ip route list` Display IP routes in an IP prefix list.
- `show ip prefix-list summary` Display a summary of the configured prefix lists.

**permit**

Configure a filter that passes packets meeting the criteria specified.

**Syntax**

```
permit ip-prefix [ge min-prefix-length] [le max-prefix-length]
```

**Parameters**

- `ip-prefix` Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
- `ge min-prefix-length` (OPTIONAL) Enter the keyword `ge` followed by the minimum prefix length, which is a number from zero (0) to 32.
- `le max-prefix-length` (OPTIONAL) Enter the keyword `le` followed by the maximum prefix length, which is a number from zero (0) to 32.

**Command Modes**

- PREFIX-LIST
Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If the options `ge` or `le` are not used, only packets with an exact match to the prefix are filtered.

**Related Commands**

- `deny` Configure a filter to drop packets.
- `seq` Configure a drop or permit filter with a specified sequence number.

**Syntax**

```
seq sequence-number {deny | permit} {any} | [ip-prefix /nn {ge min-prefix-length} {le max-prefix-length}] | [bitmask number]
```

**Parameters**

- `sequence-number`: Enter a number. Range: 1 to 4294967294.
- `deny`: Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
- `permit`: Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
- `any`: (OPTIONAL) Enter the keyword `any` to match any packets.
- `ip-prefix /nn`: (OPTIONAL) Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
- `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.
- `bitmask number`: Enter the keyword `bitmask` followed by a bit mask number in dotted decimal format.

**Defaults**

Not configured.

**Command Modes**

PREFIX-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added bit mask option</td>
</tr>
</tbody>
</table>

**Usage Information**

If the options `ge` or `le` are not used, only packets with an exact match to the prefix are filtered.
### show config

Display the current PREFIX-LIST configurations.

**Syntax**

```
show config
```

**Command Modes**

PREFIX-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

Figure 9-9. Command Example: show config

```
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>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Configure a filter to drop packets.</td>
</tr>
<tr>
<td>permit</td>
<td>Configure a filter to pass packets.</td>
</tr>
</tbody>
</table>
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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Example

Figure 9-11. Command Example: show ip prefix-list summary

FTOS#show ip prefix summary
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
  count: 3, range entries: 1, sequences: 5 - 15
ip prefix-list test1:
  count: 2, range entries: 2, sequences: 5 - 10
ip prefix-list test2:
  count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test3:
  count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test4:
  count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test5:
  count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test6:
  count: 1, range entries: 1, sequences: 5 - 5
FTOS#
Route Map Commands

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

The following commands allow you to configure route maps and their redistribution criteria.

- continue
- description
- match as-path
- match community
- match interface
- match ip address
- match ip next-hop
- match ip route-source
- match metric
- match origin
- match route-type
- match tag
- route-map
- set as-path
- set automatic-tag
- set comm-list delete
- set community
- set level
- set local-preference
- set metric
- set metric-type
- set next-hop
- set origin
- set tag
- set weight
- 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:

<table>
<thead>
<tr>
<th>sequence-number</th>
<th>(OPTIONAL) Enter the route map sequence number. Range: 1 - 65535</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default: no sequence number</td>
</tr>
</tbody>
</table>

Defaults:

Not Configured
The **continue** feature allows movement from one route-map entry to a specific route-map entry (the **sequence number**). If the sequence number is not specified, 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 will execute 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 will fall 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, then set actions is performed first followed by the continue clause jump to the specified route map entry.

- If a set actions occurs in the first route map entry and then 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 **set community additive** and **set as-path prepend** are configure, the communities and AS numbers are prepended.

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set community</td>
<td>Specify a COMMUNITY attribute</td>
</tr>
<tr>
<td>set as-path</td>
<td>Configure a filter to modify the AS path</td>
</tr>
</tbody>
</table>

**Syntax**  

```
description {description}  
```
<table>
<thead>
<tr>
<th><strong>Parameters</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>description</code></td>
<td>Enter a description to identify the route map (80 characters maximum).</td>
</tr>
</tbody>
</table>

| **Defaults** | No default behavior or values |

| **Command Modes** | ROUTE-MAP |

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
<th><strong>Version 8.1.1.0</strong> Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Version 7.8.1.0</strong> Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td></td>
<td><strong>Version 7.6.1.0</strong> Support added for S-Series</td>
</tr>
<tr>
<td></td>
<td><strong>Version 7.5.1.0</strong> Support added for C-Series</td>
</tr>
<tr>
<td></td>
<td><strong>pre-Version 6.1.1.0</strong> Introduced for E-Series</td>
</tr>
</tbody>
</table>

| **Related Commands** | | route-map | Enable a route map |

### match as-path

Configure a filter to match routes that have a certain AS number in their BGP path.

| **Syntax** | `match as-path as-path-name` |

| **Parameters** | **as-path-name** | Enter the name of an established AS-PATH ACL, up to 140 characters. |

| **Defaults** | Not configured. |

| **Command Modes** | ROUTE-MAP |

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
<th><strong>Version 8.1.1.0</strong> Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Version 7.8.1.0</strong> Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td></td>
<td><strong>Version 7.6.1.0</strong> Support added for S-Series</td>
</tr>
<tr>
<td></td>
<td><strong>Version 7.5.1.0</strong> Support added for C-Series</td>
</tr>
<tr>
<td></td>
<td><strong>pre-Version 6.1.1.0</strong> Introduced for E-Series</td>
</tr>
</tbody>
</table>

| **Related Commands** | set as-path | Add information to the BGP AS_PATH attribute. |

### match community

Configure a filter to match routes that have a certain COMMUNITY attribute in their BGP path.

| **Syntax** | `match community community-list-name [exact]` |

| **Parameters** | **community-list-name** | Enter the name of a configured community list. |
| **exact** | (OPTIONAL) Enter the keywords `exact` to process only those routes with this community list name. |

| **Defaults** | Not configured. |

| **Command Modes** | ROUTE-MAP |

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
<th><strong>Version 8.1.1.0</strong> Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Version 7.8.1.0</strong> Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td></td>
<td><strong>Version 7.6.1.0</strong> Support added for S-Series</td>
</tr>
<tr>
<td></td>
<td><strong>Version 7.5.1.0</strong> Support added for C-Series</td>
</tr>
<tr>
<td></td>
<td><strong>pre-Version 6.1.1.0</strong> Introduced for E-Series</td>
</tr>
</tbody>
</table>

| **Related Commands** | set as-path | Add information to the BGP AS_PATH attribute. |
match interface

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

**Syntax**

```
match interface interface
```

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

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
    - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
    - For the loopback interface, enter the keyword `loopback` followed by a number from zero (0) to 16383.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
      - **C-Series and S-Series** Range: 1-128
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
    - For a Ten 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, 1-2094 for ExaScale (can use IDs 1-4094).

**Defaults**

Not configured

**Command Modes**

ROUTE-MAP

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Support added for S-Series
- **Version 7.5.1.0** Support added for C-Series
- **pre-Version 6.1.1.0** Introduced for E-Series

**Related Commands**

- `ip community-list` Configure an Community Access list.
- `set community` Specify a COMMUNITY attribute.
- `neighbor send-community` Send COMMUNITY attribute to peer or peer group.
- `match ip address` Redistribute routes that match an IP address.
- `match ip next-hop` Redistribute routes that match the next-hop IP address.
- `match ip route-source` Redistribute routes that match routes advertised by other routers.
match ip address

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

Syntax

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

Parameters

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

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

- **Version 8.1.1.0**: Introduced on E-Series ExaScale
- **Version 7.8.1.0**: Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- **Version 7.6.1.0**: Support added for S-Series
- **Version 7.5.1.0**: Support added for C-Series
- **pre-Version 6.1.1.0**: Introduced for E-Series

Related Commands

- `match interface` Redistribute routes that match the next-hop interface.
- `match ip next-hop` Redistribute routes that match the next-hop IP address.
- `match ip route-source` Redistribute routes that match routes advertised by other routers.
- `match metric` Redistribute routes that match a specific metric.
- `match route-type` Redistribute routes that match a route type.
- `match tag` Redistribute routes that match a specific tag.

match ip next-hop

Configure a filter to match based on the next-hop IP addresses specified in an IP access list or IP prefix list.

Syntax

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

Defaults

Not configured.

Command Modes

ROUTE-MAP
match ip route-source

Configure a filter to match based on the routes advertised by routes 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Related Commands

match interface
Redistribute routes that match the next-hop interface.

match ip address
Redistribute routes that match an IP address.

match ip route-source
Redistribute routes that match routes advertised by other routers.

match metric
Redistribute routes that match a specific metric.

match route-type
Redistribute routes that match a route type.

match tag
Redistribute routes that match a specific tag.
### match metric

**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 8.1.1.0**: Introduced on E-Series ExaScale
- **Version 7.6.1.0**: Support added for S-Series
- **Version 7.5.1.0**: Support added for C-Series
- **pre-Version 6.1.1.0**: Introduced for E-Series

**Related Commands**

- **match interface**: Redistribute routes that match the next-hop interface.
- **match ip address**: Redistribute routes that match an IP address.
- **match ip next-hop**: Redistribute routes that match the next-hop IP address.
- **match ip route-source**: Redistribute routes that match routes advertised by other routers.
- **match route-type**: Redistribute routes that match a route type.
- **match tag**: Redistribute routes that match a specific tag.

### match origin

**Syntax**

```
match origin {egp | igp | incomplete}
```

**Parameters**

- **egp**: Enter the keyword egp to match routes originating outside the AS.
- **igp**: Enter the keyword igp to match routes originating within the same AS.
- **incomplete**: Enter the keyword incomplete to match routes with incomplete routing information.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

- **Version 8.1.1.0**: Introduced on E-Series ExaScale
- **pre-Version 6.1.1.0**: Introduced for E-Series
**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 | level-1 | level-2 | 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.
- **level-1**: Enter the keyword `level-1` to match IS-IS Level 1 routes.
- **level-2**: Enter the keyword `level-2` to match IS-IS Level 2 routes.
- **local**: Enter the keyword `local` to match only on routes generated within the switch.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

- **Version 8.1.1.0**: Introduced on E-Series ExaScale
- **Version 7.6.1.0**: Support added for S-Series
- **Version 7.5.1.0**: Support added for C-Series
- **pre-Version 6.1.1.0**: Introduced for E-Series

**Related Commands**

- `match interface`: Redistribute routes that match the next-hop interface.
- `match ip address`: Redistribute routes that match an IP address.
- `match ip next-hop`: Redistribute routes that match the next-hop IP address.
- `match ip route-source`: Redistribute routes that match routes advertised by other routers.
- `match metric`: Redistribute routes that match a specific metric.
- `match tag`: Redistribute routes that match a tag.

**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

**Command History**

- **Version 8.1.1.0**: Introduced on E-Series ExaScale
- **Version 7.6.1.0**: Support added for S-Series
Related Commands

- **match interface**: Redistribute routes that match the next-hop interface.
- **match ip address**: Redistribute routes that match an IP address.
- **match ip next-hop**: Redistribute routes that match the next-hop IP address.
- **match ip route-source**: Redistribute routes that match routes advertised by other routers.
- **match metric**: Redistribute routes that match a specific metric.
- **match route-type**: Redistribute routes that match a route type.

**route-map**

Enable a route map statement and configure its action and sequence number. This command also places you in the 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 8.1.1.0: Introduced on E-Series ExaScale
- Version 7.8.1.0: Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- Version 7.6.1.0: Support added for S-Series
- Version 7.5.1.0: Support added for C-Series
- pre-Version 6.1.1.0: Introduced for E-Series

**Example**

```
FTOS(conf)#route-map dempsey
FTOS(config-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.
Prior to 7.8.1.0, names are up to 16 characters long.

### Related Commands
- **show config** Display the current configuration.

---

## set as-path

Configure a filter to modify the AS path for BGP routes.

**Syntax**

```
set as-path prepend as-number [... as-number]
```

**Parameters**

- **prepend as-number** Enter the keyword `prepend` followed by up to eight AS numbers to be inserted into the BGP path information.
  - Range: 1 to 65535

**Defaults**

Not configured

**Command Modes**

ROUTE-MAP

**Command History**

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Support added for S-Series
- **Version 7.5.1.0** Support added for C-Series
- **pre-Version 6.1.1.0** Introduced for E-Series

**Usage Information**

You can prepend up to eight AS numbers to a BGP route.

This command influences best path selection in BGP by inserting a tag or AS number into the AS_PATH attribute.

**Related Commands**

- **match as-path** Redistribute routes that match an AS-PATH attribute.
- **ip as-path access-list** Configure an AS-PATH access list.
- **neighbor filter-list** Configure a BGP filter based on the AS-PATH attribute.
- **show ip community-lists** Display configured IP Community access lists.

---

## 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 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Support added for S-Series
set comm-list delete

Configure a filter to remove the specified community list from the BGP route’s COMMUNITY attribute.

**Syntax**

```
set comm-list community-list-name delete
```

**Parameters**

- `community-list-name`: Enter the name of an established Community list, up to 140 characters.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The community list used in the `set comm-list delete` command must be configured so that each filter contains only one community. For example, the filter `deny 100:12` is acceptable, but the filter `deny 120:13 140:33` results in an error.

If the `set comm-list delete` command and the `set community` command are configured in the same route map sequence, then the deletion command (set comm-list delete) is processed before the insertion command (set community).

Prior to 7.8.1.0, names are up to 16 characters long.

**Related Commands**

- `ip community-list`: Configure community access list.
- `match community`: Redistribute routes that match the COMMUNITY attribute.
- `set community`: Specify a COMMUNITY attribute.
set community

Allows you to assign a BGP COMMUNITY attribute.

**Syntax**

```
set community {community-number | local-as | no-advertise | no-export | none} [additive]
```

To delete a BGP COMMUNITY attribute assignment, use the `no set community {community-number | local-as | no-advertise | no-export | none}` command.

**Parameters**

- **community-number**: Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
- **local-AS**: Enter the keywords `local-AS` to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xffffff03) community attribute must not be advertised to external BGP peers.
- **no-advertise**: Enter the keywords `no-advertise` to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xffffff02) community attribute must not be advertised to other BGP peers.
- **no-export**: Enter the keywords `no-export` to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xffffff01) community attribute must not be advertised outside a BGP confederation boundary.
- **none**: Enter the keywords `none` to remove the community attribute from routes meeting the route map criteria.
- **additive**: (OPTIONAL) Enter the keyword `additive` to add the communities to already existing communities.

**Defaults**

Not configured

**Command Modes**

ROUTE-MAP

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

**Related Commands**

- `ip community-list` Configure a Community access list.
- `match community` Redistribute routes that match a BGP COMMUNITY attribute.
- `neighbor send-community` Assign the COMMUNITY attribute.
- `show ip bgp community` Display BGP community groups.
- `show ip community-lists` Display configured Community access lists.
**set level**

Configure a filter to specify the IS-IS level or OSPF area to which matched routes are redistributed.

**Syntax**

```
set level {backbone | level-1 | level-1-2 | level-2 | stub-area}
```

**Parameters**

- **backbone**
  - Enter the keyword **backbone** to redistribute matched routes to the OSPF backbone area (area 0.0.0.0).
- **level-1**
  - Enter the keyword **level-1** to redistribute matched routes to IS-IS Level 1.
- **level-1-2**
  - Enter the keyword **level-1-2** to redistribute matched routes to IS-IS Level 1 and Level 2.
- **level-2**
  - Enter the keyword **level-2** to redistribute matched routes to IS-IS Level 2.
- **stub-area**
  - Enter the keyword **stub** to redistribute matched routes to OSPF stub areas.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

**Related Commands**

- `set automatic-tag` Compute the tag value of the route.
- `set metric` Specify the metric value assigned to redistributed routes.
- `set metric-type` Specify the metric type assigned to redistributed routes.
- `set tag` Specify the tag assigned to redistributed routes.

**set local-preference**

Configure a filter to set the BGP LOCAL_PREF attribute for routers within the local autonomous system.

**Syntax**

```
set local-preference value
```

**Parameters**

- **value**
  - Enter a number as the LOCAL_PREF attribute value.
  - Range: 0 to 4294967295

**Defaults**

Not configured

**Command Modes**

ROUTE-MAP

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series
Usage

Information

The `set local-preference` command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the `bgp default local-preference` command.

Related

Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp default local-preference</code></td>
<td>Change default LOCAL_PREF attribute for all routes.</td>
</tr>
</tbody>
</table>

**set metric**

Configure a filter to assign a new metric to redistributed routes.

**Syntax**

```
set metric [+] metric-value
```

To delete a setting, enter `no set metric`.

**Parameters**

- `+` *(OPTIONAL)* Enter `+` to add a metric-value to the redistributed routes.
- `-` *(OPTIONAL)* Enter `-` to subtract a metric-value from the redistributed routes.

**Defaults**

Not configured

**Command Modes**

ROUTE-MAP

**History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- `set automatic-tag` Compute the tag value of the route.
- `set level` Specify the OSPF area for route redistribution.
- `set metric-type` Specify the route type assigned to redistributed routes.
- `set tag` Specify 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**

- `internal` Enter the keyword `internal` to assign the Interior Gateway Protocol metric of the next hop as the route’s BGP MULTI_EXIT_DES (MED) value.
- `external` Enter the keyword `external` to assign the IS-IS external metric.
- `type-1` Enter the keyword `type-1` to assign the OSPF Type 1 metric.
- `type-2` Enter the keyword `type-2` to assign the OSPF Type 2 metric.

**Defaults**

Not configured.
set next-hop

Configure a filter to specify an IP address as the next hop.

Syntax

```
set next-hop ip-address
```

Parameters

- `ip-address`: Specify an IP address in dotted decimal format.

Defaults

Not configured.

Command Modes

- ROUTE-MAP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Implemented <strong>internal</strong> keyword</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

- If the **set next-hop** command is configured, its configuration takes precedence over the **neighbor next-hop-self** command in the ROUTER BGP mode.

- If you configure the **set next-hop** command with the interface’s (either Loopback or physical) IP address, the software declares the route unreachable.

Related Commands

- **match ip next-hop**: Redistribute routes that match the next-hop IP address.
- **neighbor next-hop-self**: Configure the routers as the next hop for a BGP neighbor.
set origin

Configure a filter to manipulate the BGP ORIGIN attribute.

Syntax

```
set origin {igp | egp | incomplete}
```

Parameters

- **egp**: Enter the keyword `egp` to set routes originating from outside the local AS.
- **igp**: Enter the keyword `igp` to set routes originating within the same AS.
- **incomplete**: Enter the keyword `incomplete` to set routes with incomplete routing information.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

- **Version 8.1.1.0**: Introduced on E-Series ExaScale
- **Version 7.6.1.0**: Support added for S-Series
- **Version 7.5.1.0**: Support added for C-Series
- **pre-Version 6.1.1.0**: Introduced for E-Series

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 8.1.1.0**: Introduced on E-Series ExaScale
- **Version 7.6.1.0**: Support added for S-Series
- **Version 7.5.1.0**: Support added for C-Series
- **pre-Version 6.1.1.0**: Introduced for E-Series

Related Commands

- **set automatic-tag**: Compute the tag value of the route.
- **set level**: Specify the OSPF area for route redistribution.
- **set metric**: Specify the metric value assigned to redistributed routes.
- **set metric-type**: Specify the route type assigned to redistributed routes.
set weight

Configure a filter to add a non-RFC compliant attribute to the BGP route to assist with route selection.

Syntax

```plaintext
set weight weight
```

Parameters

- `weight`: Enter a number as the weight to be used by the route meeting the route map specification. Routes with a higher weight are preferred when there are multiple routes to the same destination.
  - Range: 0 to 65535
  - Default: router-originated = 32768; all other routes = 0

Defaults

- router-originated = 32768; all other routes = 0

Command Modes

- ROUTE-MAP

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

Usage Information

If you do not use the `set weight` command, router-originated paths have a weight attribute of 32768 and all other paths have a weight attribute of zero.

show config

Display the current route map configuration.

Syntax

```plaintext
show config
```

Command Modes

- ROUTE-MAP

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

Example

```
Figure 9-13. Command Example: show config

FTOS(config-route-map)#show config
#
route-map hopper permit 10
FTOS(config-route-map)#
```

show route-map

Display the current route map configurations.

Syntax

```plaintext
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Example

Figure 9-14.  Command Example: show route-map

```
FTOS#show route-map
route-map firpo, permit, sequence 10
   Match clauses:
   Set clauses:
      tag 34
FTOS#
```

Related Commands

route-map  Configure a route map.

AS-Path Commands

This feature is supported on E-Series only, as indicated by this character under each command heading: 

The following commands configure AS-Path ACLs.

- deny
- ip as-path access-list
- permit
- show config
- show ip as-path-access-lists
deny

Create a filter to drop routes that match the route’s AS-PATH attribute. Use regular expressions to identify which routes are affected by the filter.

**Syntax**

`deny as-regular-expression`

**Parameters**

- **as-regular-expression**: Enter a regular expression to match BGP AS-PATH attributes.
  - a regular expression to match BGP AS-PATH attributes. Use one or a combination of the following:
    - . = (period) matches on any single character, including white space
    - * = (asterisk) matches on sequences in a pattern (zero or more sequences)
    - + = (plus sign) matches on sequences in a pattern (one or more sequences)
    - ? = (question mark) matches sequences in a pattern (0 or 1 sequences).
    - ^ = (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
    - $ = (dollar sign) matches the end of the output string.
    - _ = (underscore) matches a comma (,), left brace ({}), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.
    - | = (pipe) matches either character.

**Defaults**

Not configured

**Command Modes**

AS-PATH ACL

**Usage Information**

The regular expression must match part of the ASCII-text in the AS-PATH attribute of the BGP route.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**ip as-path access-list**

Enter the AS-PATH ACL mode and configure an access control list based on the BGP AS_PATH attribute.

**Syntax**

`ip as-path access-list as-path-name`

**Parameters**

- **as-path-name**: Enter the access-list name, up to 140 characters.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION
**Example**

Figure 9-15. Command Example: ip as-path access-list

FTOS(conf)#ip as-path access-list TestPath
FTOS(config-as-path)#

**Usage Information**

Use the **match as-path** or **neighbor filter-list** commands to apply the AS-PATH ACL to BGP routes.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- **match as-path** Match on routes contain a specific AS-PATH.
- **neighbor filter-list** Configure filter based on AS-PATH information.

---

**permit**

Create a filter to forward BGP routes that match the route’s AS-PATH attributes. Use regular expressions to identify which routes are affected by this filter.

**Syntax**

`permit as-regular-expression`

**Parameters**

*as-regular-expression* Enter a regular expression to match BGP AS-PATH attributes. Use one or a combination of the following:

- `.=` (period) matches on any single character, including white space
- `*=` (asterisk) matches on sequences in a pattern (zero or more sequences)
- `+=` (plus sign) matches on sequences in a pattern (one or more sequences)
- `?=` (question mark) matches sequences in a pattern (0 or 1 sequences). **You must enter an escape sequence (CNTL+v) prior to entering the ? regular expression.**
- `[]` (brackets) matches a range of single-character patterns.
- `^` (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
- `$` (dollar sign) matches the end of the output string.
- `_` (underscore) matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.
- `|` (pipe) matches either character.

**Defaults**

Not configured

**Command Modes**

AS-PATH ACL

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
show config

Display the current configuration.

Syntax

show config

Command Mode

AS-PATH ACL

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale
pre-Version 6.1.1.0 Introduced for E-Series

Example

Figure 9-16. Command Example: show config (AS-PATH ACL)

FTOS(config-as-path)#show config
!
ip as-path access-list snickers
  deny .3
FTOS(config-as-path)#

show ip as-path-access-lists

Display the all AS-PATH access lists configured on the E-Series.

Syntax

show ip as-path-access-lists

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale
pre-Version 6.1.1.0 Introduced for E-Series

Example

Figure 9-17. Command Example: show ip as-path-access-lists

FTOS#show ip as-path-access-lists
ip as-path access-list 1
  permit ^$  
  permit \((.*)\)$
  deny .* 
ip as-path access-list 91
  permit ^$  
  deny .* 
  permit \((.*)\)$
FTOS#

IP Community List Commands

IP Community List commands are supported on E-Series only, as indicated by this character under each command heading: ℹ️

The commands in this section are:

- deny
deny

Create a filter to drop routes matching a BGP COMMUNITY number.

Syntax

deny {community-number | local-AS | no-advertise | no-export | quote-regexp
regular-expressions-list | regexp regular-expression}

Parameters

community-number Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.

local-AS Enter the keywords local-AS to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise Enter the keywords no-advertise to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFF02) community attribute must not be advertised to other BGP peers.

no-export Enter the keywords no-export to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

regexp regular-expression Enter the keyword regexp followed by a regular expression. Use one or a combination of the following:

- . = (period) matches on any single character, including white space
- * = (asterisk) matches on sequences in a pattern (zero or more sequences)
- + = (plus sign) matches on sequences in a pattern (one or more sequences)
- ? = (question mark) matches sequences in a pattern (0 or 1 sequences). You must enter an escape sequence (CNTL+v) prior to entering the ? regular expression.
- [] = (brackets) matches a range of single-character patterns.
- ^ = (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
- $ = (dollar sign) matches the end of the output string.
- _ = (underscore) matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.
- | = (pipe) matches either character.

Defaults Not configured.

Command Modes COMMUNITY-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
ip community-list

Enter COMMUNITY-LIST mode and create an IP community-list for BGP.

Syntax

```
ip community-list comm-list-name
```

To delete a community-list, use the `no ip community-list comm-list-name` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>comm-list-name</td>
<td>Enter a text string as the name of the community-list, up to 140 characters.</td>
</tr>
</tbody>
</table>

Command Modes

CONFIGURATION

Example

```
FTOS(conf)#ip community-list TestComList
FTOS(config-community-list)#
```

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

permit

Configure a filter to forward routes that match the route’s COMMUNITY attribute.

Syntax

```
permit {community-number | local-AS | no-advertise | no-export | quote-regexp regular-expressions-list | regexp regular-expression}
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community-number</td>
<td>Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.</td>
</tr>
<tr>
<td>local-AS</td>
<td>Enter the keywords <code>local-AS</code> to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Enter the keywords <code>no-advertise</code> to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.</td>
</tr>
</tbody>
</table>

FTOS(config)#permit community-number 100
FTOS(config)#permit local-AS
FTOS(config)#permit no-advertise
FTOS(config)#permit no-export
FTOS(config)#permit quote-regexp regular-expression
FTOS(config)#permit regexp regular-expression
**no-export**  
Enter the keywords **no-export** to drop all routes containing the well-known community attribute of NO_EXPORT.  
All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

**regexp**  
**regular-expression**  
Enter the keyword **regexp** followed by a regular expression. Use one or a combination of the following:

- `.=` (period) matches on any single character, including white space
- `*=` (asterisk) matches on sequences in a pattern (zero or more sequences)
- `+` = (plus sign) matches on sequences in a pattern (one or more sequences)
- `?` = (question mark) matches sequences in a pattern (0 or 1 sequences). **You must enter an escape sequence (CNTL+v) prior to entering the ? regular expression.**
- `[]` = (brackets) matches a range of single-character patterns.
- `^` = (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
- `$` = (dollar sign) matches the end of the output string.
- `_` = (underscore) matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.
- `|` = (pipe) matches either character.

**Defaults**  
Not configured

**Command Modes**  
COMMUNITY-LIST

**Command History**  
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**show config**

Display the non-default information in the current configuration.

**Syntax**  
show config

**Command Mode**  
COMMUNITY-LIST

**Command History**  
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**  

**Figure 9-19. Command Example: show config (COMMUNITY-LIST)**

```plaintext
FTOS(config-std-community-list)#show config
!
ip community-list standard patches
deny 45:1
permit no-export
FTOS(config-std-community-list)#
```
show ip community-lists

Display configured IP community lists in alphabetic order.

Syntax

show ip community-lists [name]

Parameters

name (OPTIONAL) Enter the name of the standard or extended IP community list, up to 140 characters.

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.8.1.0 Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
pre-Version 6.1.1.0 Introduced for E-Series

Example

Figure 9-20. Command Example: show ip community-lists

FTOS#show ip community-lists
ip community-list standard 1
deny 701:20
deny 702:20
deny 703:20
deny 704:20
deny 705:20
deny 14551:20
deny 701:112
deny 702:112
deny 703:112
deny 704:112
deny 705:112
deny 14551:112
deny 701:666
deny 702:666
deny 703:666
deny 704:666
deny 705:666
deny 14551:666
FTOS#
ACL VLAN Group

Overview

The ACL VLAN Group feature is available only on the E-Series, as indicated by this symbol under each command heading: 🚀

Since VLAN ACLs exist as multiple ACLs in the CAM, the size of the ACLs can be limited in the CAM. The ACL VLAN Group feature permits you to group VLANs and apply ACLs to the group so that ACLs exist as a single ACL in the CAM.

Note: This feature is supported on IPv4 only and can only be used with the ipv4-egacl-16k CAM Profile with the acl-group microcode. See Chapter 13, Content Addressable Memory (CAM).

Commands

The ACL VLAN Group commands are:

• acl-vlan-group
• description
• ip access-group
• member vlan
• show acl-vlan-group
• show config
• show running config acl-vlan-group

See other VLAN commands in Chapter 9, Access Control Lists (ACL).

acl-vlan-group

Create an ACL VLAN group

Syntax

acl-vlan-group {group name}

Parameters

| group name | Specify the name of the ACL VLAN group (maximum 140 characters). |

Defaults

No default behavior or values

Command Modes

CONFIGURATION
**Command History**

Version 7.8.1.0  
Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.

Version 6.3.1.0  
Introduced on E-Series

**Usage Information**

You can have up to 8 different ACL VLAN groups at any given time.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show acl-vlan-group</td>
<td>Display the ACL VLAN groups</td>
</tr>
</tbody>
</table>

**description**

Add a description to the ACL VLAN group.

**Syntax**

description description

**Parameters**

- **description** Enter a description to identify the ACL VLAN group (80 characters maximum).

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION (conf-acl-vl-grp)

**Command History**

Version 6.3.1.0  
Introduced on E-Series

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show acl-vlan-group</td>
<td>Display the ACL VLAN groups</td>
</tr>
</tbody>
</table>

**ip access-group**

Apply an egress IP ACL to the ACL VLAN group.

**Syntax**

ip access-group {group name} out implicit-permit

**Parameters**

- **group name** Enter the name of the ACL VLAN group where you want the egress IP ACLs applied, up to 140 characters.

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION (conf-acl-vl-grp)

**Command History**

Version 7.8.1.0  
Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.

Version 6.3.1.0  
Introduced on E-Series

**Usage Information**

**Note:** Only an egress IP ACL can be applied on an ACL VLAN group.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-vlan-group</td>
<td>Create an ACL VLAN Group and name</td>
</tr>
</tbody>
</table>
member vlan

Add VLAN member(s) to an ACL VLAN group.

**Syntax**

```
member vlan {VLAN-range}
```

**Parameters**

- **VLAN-range**
  
  Enter the comma separated VLAN ID set. For example, 1-10,400-410,500

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION (conf-acl-vl-grp)

**Command History**

- **Version 6.3.1.0**
  
  Introduced on E-Series

**Usage Information**

At a maximum, there can be only 32 VLAN members in all ACL VLAN groups. A VLAN can belong to only one group at any given time.

**Related Commands**

- `show acl-vlan-group` Display the ACL VLAN Groups

show acl-vlan-group

Display all the ACL VLAN Groups or display a specific ACL VLAN Group, identified by name.

**Syntax**

```
show acl-vlan-group {group name | detail}
```

**Parameters**

- **group name**
  
  (Optional) Display only the ACL VLAN Group that is specified, up to 140 characters.

- **detail**
  
  Display information in a line-by-line format to display the names in their entirety.

  **Note:** Without the detail option, the output is displayed in a table style and information may be truncated.

**Defaults**

No default behavior or values

**Command Modes**

EXEC

EXEC Privilege

**Command History**

- **Version 7.8.1.0**
  
  Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.

- **Version 6.3.1.0**
  
 Introduced on E-Series

**Usage Notes**

When an ACL-VLAN-Group name or the Access List Group Name contains more than 30 characters, the name will be truncated in the `show acl-vlan-group` command output.

**Examples**

Figure 10-1 shows the table style display used with the `show acl-vlan-group` command. Note that some group names and some access list names are truncated.
Figure 10-1. Command Example: show acl-vlan-group

FTOS#show acl-vlan-group
Group Name                  Egress IP Acl               Vlan Members
TestGroupSeventeenTwenty    SpecialAccessOnlyExperts    100,200,300
CustomerNumberIdentificationEleven   AnyEmployeeCustomerElevenGrantedAccess    2-10,99
HostGroup                   Group5                      1,1000
FTOS#                        Truncated Group and Access List Names

show acl-vlan-group detail

Display all the ACL VLAN Groups or display a specific ACL VLAN Group by name. The output is show in a line-by-line format to display the names in their entirety.

Syntax: show acl-vlan-group detail

Defaults: No default behavior or values

Command Modes: EXEC
EXEC Privilege

Command History

| Version 7.8.1.0 | Introduced on E-Series |

Usage Notes

The output for this command is shown in a line-by-line format. This allows the ACL-VLAN-Group names (or the Access List Group Names) to display in their entirety.

Example

**Figure 10-4. Command Example: show acl-clan-group**

```
FTOS(conf-acl-vl-grp)#show config
acl-vlan-group group1
    description Acl Vlan Group1
    member vlan 1-10,400-410,500
    ip access-group acl1 out implicit-permit
FTOS#
```

**show config**

Display the current configuration of the ACL VLAN group.

**Syntax**

```
show config
```

**Defaults**

No default behavior or values

**Command Modes**

EXEC

**Command History**

| Version 6.3.1.0 | Introduced on E-Series |

**Example**

**Figure 10-5. show config Command Example**

```
FTOS(conf-acl-vl-grp)#show config
acl-vlan-group group1
    description Acl Vlan Group1
    member vlan 1-10,400-410,500
    ip access-group acl1 out implicit-permit
FTOS#
```

**show running config acl-vlan-group**

Display the running configuration of all or a given ACL VLAN Group.

**Syntax**

```
show running config acl-vlan-group group name
```

**Parameters**

| group name | Display only the ACL VLAN Group that is specified. The group name can be up to 140 characters |

**Defaults**

No default behavior or values

**Command Modes**

EXEC
**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 10-6.  show running-config acl-vlan-group Command Example Output**

```
FTOS#show running-config acl-vlan-group
!
acl-vlan-group group1
  description Acl Vlan Group1
  member vlan 1-10,400-410,500
  ip access-group acl1 out implicit-permit
!
acl-vlan-group group2
  member vlan 20
  ip access-group acl2 out
FTOS#

FTOS#show running-config acl-vlan-group group1
!
acl-vlan-group group1
  description Acl Vlan Group1
  member vlan 1-10,400-410,500
  ip access-group acl1 out implicit-permit
FTOS#
```
Bidirectional Forwarding Detection (BFD)

Overview

Bidirectional Forwarding Detection (BFD) is a detection protocol that provides fast forwarding path failure detection. The Dell Networking OS implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03 and supports BFD on all Layer 3 physical interfaces including VLAN interfaces and port-channels.

BFD is supported on the C-Series and E-Series, where indicated by the \( \text{c} \) and \( \text{e} \) characters under command headings.

BFD is supported on E-Series ExaScale \( \text{e} \) with Dell Networking OS 8.2.1.0 and later.

Commands

- bfd all-neighbors
- bfd disable
- bfd enable (Configuration)
- bfd enable (Interface)
- bfd interval
- bfd neighbor
- bfd protocol-liveness
- clear bfd counters
- debug bfd
- ip route bfd
- isis bfd all-neighbors
- neighbor bfd
- neighbor bfd disable
- show bfd counters
- show bfd neighbors
- vrrp bfd
**bfd all-neighbors**

Enable BFD sessions with all neighbors discovered by Layer 3 protocols IS-IS, OSPF, or BGP on router interfaces, and (optionally) reconfigure the default timer values.

**Syntax**

```
bfd all-neighbors [interval interval min_rx min_rx multiplier value role {active | passive}]
```

**Parameters**

- **interval milliseconds** (OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval.
  - Range: 50-1000
  - Default: 100

- **min_rx milliseconds** Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system.
  - Range: 50-100
  - Default: 100

- **multiplier value** Enter this keyword to specify the number of packets that must be missed in order to declare a session down.
  - Range: 3-50
  - Default: 3

- **role [active | passive]** Enter the role that the local system assumes:
  - Active—The active system initiates the BFD session. Both systems can be active for the same session.
  - Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system.
  - Default: Active

**Defaults**

See Parameters

**Command Modes**

- ROUTER OSPF
- ROUTER BGP
- ROUTER ISIS (Not available on C-Series)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.5</td>
<td>BFD for BGP was introduced on the C-Series and E-Series TeraScale.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>BFD for BGP was introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.3</td>
<td>BFD for BGP was introduced on the E-Series ExaScale.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>BFD for OSPF and ISIS introduced on the E-Series ExaScale.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>BFD for OSPF introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>BFD for ISIS introduced on the E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>BFD for OSPF introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

All neighbors inherit the timer values configured with the `bfd all-neighbors` command except in the following cases:

- Timer values configured with the `isis bfd all-neighbors` command in INTERFACE mode override timer values configured with the `bfd all-neighbors` command. Likewise, using the `no bfd all-neighbors` command does not disable BFD on an interface if BFD is explicitly enabled using the command `isis bfd all-neighbors`.

---

Note: The image contains the header and footer of the page, which are not relevant to the content of the document. The content is a detailed explanation of the `bfd all-neighbors` command, including syntax, parameters, default values, and command modes, along with historical versions and usage information.
Neighbors that have been explicitly enabled or disabled for a BFD session with the `bfd neighbor` or `neighbor bfd disable` commands in ROUTER BGP mode do not inherit the global BFD enable/disable values configured with the `bfd all-neighbors` command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values (configured with the `bfd all-neighbors` command).

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show bfd neighbors</code></td>
<td>Display BFD neighbor information on all interfaces or a specified interface.</td>
</tr>
<tr>
<td><code>bfd</code></td>
<td>Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.</td>
</tr>
<tr>
<td><code>neighbor bfd disable</code></td>
<td>Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.</td>
</tr>
</tbody>
</table>

**Bfd disable**

Disable BFD on all interfaces.

**Syntax**

`bfd disable`

Re-enable BFD using the command `no bfd disable`.

**Defaults**

BFD is disabled by default.

**Command Modes**

INTERFACE VRRP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Bfd enable (Configuration)**

Enable BFD on all interfaces.

**Syntax**

`bfd enable`

Disable BFD using the `no bfd enable` command.

**Defaults**

BFD is disabled by default.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
**bfd enable (Interface)**

Enable BFD on an interface.

**Syntax**

```
bfd enable
```

**Defaults**

BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.

**Command Modes**

```
INTERFACE
```

**Command History**

<table>
<thead>
<tr>
<th>Command</th>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd enable</td>
<td>8.2.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>bfd enable</td>
<td>7.6.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>bfd enable</td>
<td>7.4.1.0</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

**bfd interval**

Specify non-default BFD session parameters beginning with the transmission interval.

**Syntax**

```
bfd interval interval min_rx min_rx multiplier value role {active | passive}
```

**Parameters**

- `interval milliseconds`:
  - Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval.
  - Range: 50-1000
  - Default: 100

- `min_rx milliseconds`:
  - Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system.
  - Range: 50-100
  - Default: 100

- `multiplier value`:
  - Enter this keyword to specify the number of packets that must be missed in order to declare a session down.
  - Range: 3-50
  - Default: 3

- `role [active | passive]`:
  - Enter the role that the local system assumes:
    - Active—The active system initiates the BFD session. Both systems can be active for the same session.
    - Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system.
  - Default: Active

**Defaults**

See Parameters

**Command Modes**

```
INTERFACE
```

**Command History**

<table>
<thead>
<tr>
<th>Command</th>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd interval</td>
<td>8.2.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>bfd interval</td>
<td>7.6.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>bfd interval</td>
<td>7.4.1.0</td>
<td>E-Series</td>
</tr>
</tbody>
</table>
**Example**

**Figure 11-1. bfd interval Command Example**

```
FTOS(conf-if-gi-0/3)#bfd interval 250 min_rx 300 multiplier 4 role passive
FTOS(conf-if-gi-0/3)#
```

---

**bfd neighbor**

Establish a BFD session with a neighbor.

**Syntax**

`bfd neighbor ip-address`

**Parameters**

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

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on C-Series
- Version 7.5.1.0 Added support for VLAN and port-channel interfaces on E-Series.
- Version 7.4.1.0 Introduced on E-Series

**Related Commands**

- `show bfd neighbors` Display BFD neighbor information on all interfaces or a specified interface.

---

**bfd protocol-liveness**

Enable the BFD protocol liveness feature.

**Syntax**

`bfd protocol-liveness`

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.4.1.0 Introduced on E-Series

**Usage Information**

Protocol Liveness is a feature that notifies the BFD Manager when a client protocol (e.g. OSPF, ISIS) is disabled. When a client is disabled, all BFD sessions for that protocol are torn down. Neighbors on the remote system receive an Admin Down control packet and are placed in the Down state. Peer routers might take corrective action by choosing alternative paths for the routes that originally pointed to this router.
clear bfd counters

Clear all BFD counters, or counters for a particular interface.

Syntax

```
clear bfd counters [interface]
```

Parameters

- `interface` (OPTIONAL) Enter one of the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` followed by the 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.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a port-channel interface, enter the keyword `port-channel` followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale, and 1 to 512 for ExaScale
  - For VLAN interfaces, enter the keyword `vlan` followed by a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1-2730 (VLAN IDs can be 0-4093).

Defaults

None

Command Modes

EXEC Privilege

Command History

- Version 8.4.6.0 Added support for the keyword `fortyGigE`.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.7.1.0 Introduced on C-Series
- Version 7.5.1.0 Added support for VLAN and port-channel interfaces on E-Series
- Version 7.4.1.0 Introduced on E-Series

Related Commands

- `show bfd counters` Display BFD counter information.
debug bfd

Enable BFD debugging.

detail (OPTIONAL) Enter this keyword to display detailed information about BFD packets.

event (OPTIONAL) Enter this keyword to display information about BFD state. The mode option is not available with this option.

packet (OPTIONAL) Enter this keyword packet to display brief information about control packets.

all Enter this keyword to enable debugging on all interfaces. The count option is not available with this option.

interface Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword gigabitethernet followed by the 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.
- For a SONET interface, enter the keyword sonet followed by the slot/port information.
- For a port-channel interface, enter the keyword port-channel followed by a number:
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 255 for EtherScale, 1 to 512 for TeraScale, and 1 to 512 for ExaScale
- For VLAN interfaces, enter the keyword vlan followed by a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1-2730 (VLAN IDs can be 0-4093).

mode (OPTIONAL) Enter one of the following debug transmission modes:

- Enter the keyword both to display information for both received and sent packets.
- Enter the keyword rx to display information for received packets.
- Enter the keyword tx to display information for sent packets.

Default: both

count number (OPTIONAL) Enter this keyword followed by the number of debug messages to display.

Range: 1-65534

Default: Infinite—that is, if a count number is not specified an infinite number of debug messages will display.

Defaults

Disabled

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for VLAN and port-channel interfaces on E-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
Since BFD can potentially transmit 20 packets per interface, debugging information should be restricted.

**ip route bfd**

Enable BFD for all neighbors configured through static routes.

**Syntax**

```
ip route bfd [interval interval min_rx min_rx multiplier value role {active | passive}]```

**Parameters**

- **interval** milliseconds
  - (OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval.
  - Range: 50-1000
  - Default: 100

- **min_rx** milliseconds
  - Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system.
  - Range: 50-100
  - Default: 100

- **multiplier** value
  - Enter this keyword to specify the number of packets that must be missed in order to declare a session down.
  - Range: 3-50
  - Default: 3

- **role** [active | passive]
  - Enter the role that the local system assumes:
    - **Active**—The active system initiates the BFD session. Both systems can be active for the same session.
    - **Passive**—The passive system does not initiate a session. It only responds to a request for session initialization from the active system.
  - Default: Active

**Defaults**

See Parameters

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on C-Series
- Version 7.4.1.0 Introduced on E-Series

**Related Commands**

- `show bfd neighbors` — Display BFD neighbor information on all interfaces or a specified interface.
isis bfd all-neighbors

Enable BFD on all IS-IS neighbors discovered on an interface.

Syntax

```
isis bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}] ]
```

Parameters

- **disable** (OPTIONAL) Enter the keyword disable to disable BFD on this interface.
- **interval milliseconds** (OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval.
  - Range: 50-1000
  - Default: 100
- **min_rx milliseconds** Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system.
  - Range: 50-100
  - Default: 100
- **multiplier value** Enter this keyword to specify the number of packets that must be missed in order to declare a session down.
  - Range: 3-50
  - Default: 3
- **role [active | passive]** Enter the role that the local system assumes:
  - Active—The active system initiates the BFD session. Both systems can be active for the same session.
  - Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system.
  - Default: Active

Defaults

See Parameters

Command Modes

INTERFACE

Command History

- **Version 8.2.1.0** Introduced on E-Series ExaScale
- **Version 7.5.1.0** Introduced on E-Series

Usage Information

This command provides the flexibility to fine tune the timer values based on individual interface needs when ISIS BFD is configured in CONFIGURATION mode. Any timer values specified with this command override timers set using the command bfd all-neighbors. Using the no form of this command will not disable BFD if BFD is configured in CONFIGURATION mode.

Use the keyword disabled to disable BFD on a specific interface while BFD is configured in from CONFIGURATION mode.
**neighbor bfd**

Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.

**Syntax**

```
neighbor {ip-address | peer-group-name} bfd
```

**Parameters**

- **ip-address**: Enter the IP address of the BGP neighbor that you want to explicitly enable for BFD sessions in dotted decimal format (A.B.C.D).
- **peer-group-name**: Enter the name of the peer group that you want to explicitly enable for BFD sessions.

**Defaults**

None

**Command Modes**

- ROUTER BGP

**Command History**

- Version 8.4.2.5 Introduced on the C-Series and E-Series TeraScale.
- Version 8.3.8.0 Introduced on the S4810.
- Version 8.4.1.3 Introduced on the E-Series ExaScale.

**Usage Information**

When you enable a BFD session with a specified BGP neighbor or peer group using the `bfd neighbor` command, the default BFD session parameters are used (interval: 100 milliseconds, min_rx: 100 milliseconds, multiplier: 3 packets, and role: active) if no parameters have been specified with the `bfd all-neighbors` command.

When you explicitly enable a BGP neighbor for a BFD session with the `bfd neighbor` command:

- The neighbor does not inherit the global BFD enable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

**Related Commands**

- `bfd all-neighbors` Enable BFD sessions with all neighbors discovered by Layer 3 protocols.
- `neighbor bfd disable` Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.
- `show bfd neighbors` Display BFD neighbor information on all interfaces or a specified interface.

**neighbor bfd disable**

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

**Syntax**

```
neighbor {ip-address | peer-group-name} bfd disable
```

**Parameters**

- **ip-address**: Enter the IP address of the BGP neighbor that you want to explicitly disable for BFD sessions in dotted decimal format (A.B.C.D).
- **peer-group-name**: Enter the name of the peer group that you want to explicitly disable for BFD sessions.

**Defaults**

None
When you explicitly disable a BGP neighbor for a BFD session with the `neighbor bfd disable` command, the neighbor does not inherit the global BFD values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.

When you remove the disabled state of a BFD for BGP session with a specified neighbor by entering the `no neighbor bfd disable` command, the BGP neighbor uses the BFD session parameters globally configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bfd all-neighbors</code></td>
<td>Enable BFD sessions with all neighbors discovered by Layer 3 protocols.</td>
</tr>
<tr>
<td><code>bfd neighbor</code></td>
<td>Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.</td>
</tr>
<tr>
<td><code>show bfd neighbors</code></td>
<td>Display BFD neighbor information on all interfaces or a specified interface.</td>
</tr>
</tbody>
</table>

**Syntax**

```
show bfd counters [bgp | isis | ospf | vrrp | static-route] [interface]
```

**Parameters**

`interface`  
Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` followed by the 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.
- For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
- For a port-channel interface, enter the keyword `port-channel` followed by a number:
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale, and 1 to 512 for ExaScale
- For VLAN interfaces, enter the keyword `vlan` followed by a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1-2730 (VLAN IDs can be 0-4093).

`bgp`  
(Optional) Enter this keyword to display counter information for BFD sessions established with BGP neighbors.

`isis`  
(Optional) Enter this keyword to display counter information for BFD sessions established with ISIS neighbors. This option is not available on C-Series.

`ospf`  
(Optional) Enter this keyword to display counter information for BFD sessions established with OSPF neighbors.
show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

Syntax

```
show bfd neighbors interface [detail]
```

**Example**

```
FTOS#show bfd neighbors

Interface               Tx          Rx
GigabitEthernet 1/3    522         625
FTOS#
```
Bidirectional Forwarding Detection (BFD) | 315

Parameters

**interface**

Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` followed by the 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.
- For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale, and 1 to 512 for ExaScale
- For VLAN interfaces, enter the keyword `vlan` followed by a number
  - From 1 to 4094. For ExaScale VLAN interfaces, the range is 1-2730 (VLAN IDs can be 0-4093).

**detail**

(Optional) Enter the keyword `detail` to view detailed information about BFD neighbors.

Defaults

None

Command Modes

EXEC

EXEC Privilege

Command History

- **Version 8.4.6.0**: Added support for the keyword `fortyGigE`.
- **Version 8.4.2.5**: Added support for BFD for BGP on the C-Series and E-Series TeraScale.
- **Version 8.3.7.0**: Added support for BFD for BGP on the S4810.
- **Version 8.3.8.0**: Added support for BFD for BGP on the S4810.
- **Version 8.4.1.3**: Added support for BFD for BGP on the E-Series ExaScale.
- **Version 8.2.1.0**: Introduced on E-Series ExaScale
- **Version 7.6.1.0**: Introduced on C-Series
- **Version 7.5.1.0**: Added BFD on VLAN and port-channel interfaces on E-Series
- **Version 7.4.1.0**: Introduced BFD on physical ports on E-Series

Example

**Figure 11-3. show bfd neighbors Command**

```
FTOS#show bfd neighbors
*   - Active session role
Ad Dn  - Admin Down
C      - CLI
I      - ISIS
O      - OSPF
R      - Static Route (RTM)

LocalAddr  RemoteAddr  Interface State Rx-int Tx-int Mult Clients
* 10.1.3.2     10.1.3.1   Gi 1/3    Up    300    250    3    C
FTOS#
```
Example

```plaintext
FTOS#show bfd neighbors detail
Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: GigabitEthernet 1/3
State: Up
Configured parameters:
  TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
  TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
  TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
  Number of packets received from neighbor: 376
  Number of packets sent to neighbor: 314
  Number of state changes: 2
  Number of messages from IFA about port state change: 0
  Number of messages communicated b/w Manager and Agent: 6
FTOS#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd neighbor</td>
<td>Establish a BFD session with a neighbor.</td>
</tr>
<tr>
<td>bfd all-neighbors</td>
<td>Establish BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.</td>
</tr>
</tbody>
</table>
vrrp bfd

Establish a VRRP BFD session.

**Syntax**

```
vrrp bfd {all-neighbors | neighbor ip-address} [interval interval min_rx min_rx multiplier value role {active | passive}]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-neighbors</td>
<td>Establish BFD sessions with all BFD neighbors on an interface.</td>
</tr>
<tr>
<td>neighbor ip-address</td>
<td>Enter the IP address of the BFD neighbor.</td>
</tr>
<tr>
<td>interval milliseconds</td>
<td>(OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range:50-1000 Default:100</td>
</tr>
<tr>
<td>min_rx milliseconds</td>
<td>Enter this keyword to specify the minimum rate at which the local system would like to receive control packets from the remote system. Range:50-100 Default:100</td>
</tr>
<tr>
<td>multiplier</td>
<td>Enter this keyword to specify the number of packets that must be missed in order to declare a session down. Range:3-50 Default:3</td>
</tr>
</tbody>
</table>
| role [active | passive] | Enter the role that the local system assumes:  
  • Active—The active system initiates the BFD session. Both systems can be active for the same session.  
  • Passive—The passive system does not initiate a session. It only responds to a request for session initialization from the active system. Default: Active |

**Defaults**

See Parameters.

**Command Modes**

INTERFACE

**Command History**

- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on C-Series
- Version 7.5.1.0 Introduced on E-Series
Border Gateway Protocol IPv4 (BGPv4)

Overview

BGPv4 is supported as shown in the following table.

<table>
<thead>
<tr>
<th>Dell Networking OS version</th>
<th>Platform support</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>pre-7.7.1.0</td>
<td>E-Series TeraScale</td>
</tr>
</tbody>
</table>

For detailed information on configuring BGP, refer to the BGP chapter in the *Dell Networking OS Configuration Guide*.

This chapter contains the following sections:

- **BGPv4 Commands**
- **MBGP Commands**
- **BGP Extended Communities (RFC 4360)**

**BGPv4 Commands**

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP version 4 (BGPv4) supports Classless InterDomain Routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

**Note:** Dell Networking OS Version 7.7.1 supports 2-Byte (16-bit) and 4-Byte (32-bit) format for Autonomous System Numbers (ASNs), where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295.

**Note:** Dell Networking OS Version 8.3.1.0 supports Dotted format as well as the Traditional Plain format for AS Numbers. The dot format is displayed when using the *show ip bgp* commands. To determine the comparable dot format for an ASN from a traditional format, use **ASN/65536. ASN%65536**.

For more information about using the 2 or 4-Byte format, refer to the *Dell Networking OS Configuration Guide*. 
The following commands enable you to configure and enable BGP.

- address-family
- aggregate-address
- bgp always-compare-med
- bgp asnotation
- bgp bestpath as-path ignore
- bgp bestpath med confed
- bgp bestpath med missing-as-best
- bgp bestpath router-id ignore
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp dampening
- bgp default local-preference
- bgp enforce-first-as
- bgp fast-external-fallover
- bgp four-octet-as-support
- bgp graceful-restart
- bgp log-neighbor-changes
- bgp non-deterministic-med
- bgp recursive-bgp-next-hop
- bgp regex-eval-optz-disable
- bgp retain-ibgp-nexthop
- bgp router-id
- bgp soft-reconfig-backup
- capture bgp-pdu neighbor
- capture bgp-pdu max-buffer-size
- clear ip bgp ipv4 unicast soft
- clear ip bgp dampening
- clear ip bgp flap-statistics
- debug ip bgp
- debug ip bgp dampening
- debug ip bgp events
- debug ip bgp keepalives
- debug ip bgp notifications
- debug ip bgp ipv4 unicast soft-reconfiguration
- debug ip bgp updates
- default-metric
- description
- distance bgp
- maximum-paths
- neighbor activate
- neighbor advertisement-interval
- neighbor advertisement-start
- neighbor allowas-in
- neighbor default-originate
- neighbor description
- neighbor distribute-list
- neighbor ebgp-multihop
- neighbor fall-over
- neighbor filter-list
- neighbor graceful-restart
- neighbor local-as
- neighbor maximum-prefix
- neighbor next-hop-self
- neighbor password
- neighbor peer-group (assigning peers)
- neighbor peer-group (creating group)
- neighbor peer-group passive
- neighbor remote-as
- neighbor remove-private-as
- neighbor route-map
- neighbor route-reflector-client
- neighbor send-community
- neighbor shutdown
- neighbor soft-reconfiguration inbound
- neighbor timers
- neighbor update-source
- neighbor weight
- network
- network backdoor
- redistribute
- redistribute isis
- redistribute ospf
- router bgp
- show capture bgp-pdu neighbor
- show config
- show ip bgp
- show ip bgp cluster-list
- show ip bgp community
- show ip bgp community-list
- show ip bgp dampened-paths
- show ip bgp detail
- show ip bgp extcommunity-list
- show ip bgp filter-list
- show ip bgp flap-statistics
- show ip bgp inconsistent-as
- show ip bgp neighbors
- show ip bgp next-hop
- show ip bgp paths
- show ip bgp paths as-path
address-family

Enable the IPv4 multicast or the IPv6 address family.

Syntax

address-family [ipv4 {multicast | vrf vrf-name} | ipv6 unicast]

Parameters

ipv4 multicast Enter BGPv4 multicast mode.

ipv4 vrf vrf-name Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.

ipv6 unicast Enter BGPv6 mode.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version 8.4.6.0 Added support for VRF.
Version 6.5.1.0 Introduced

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

aggregate-address ip-address mask [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]

Parameters

ip-address mask Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).

advertise-map map-name (OPTIONAL) Enter the keywords advertise-map followed by the name of a configured route map to set filters for advertising an aggregate route.

as-set (OPTIONAL) Enter the keyword as-set to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

attribute-map map-name (OPTIONAL) Enter the keywords attribute-map followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.

summary-only (OPTIONAL) Enter the keyword summary-only to advertise only the aggregate address. Specific routes will not be advertised.

suppress-map map-name (OPTIONAL) Enter the keywords suppress-map followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.
bgp always-compare-med

Enables you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

Syntax

```
bgp always-compare-med
```

To disable comparison of MED, enter `no bgp always-compare-med.`

Defaults

Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes

ROUTER BGP

Usage Information

Any update without a MED attribute is the least preferred route

If you enable this command, use the `clear ip bgp ipv4 unicast soft *` command to recompute the best path.

Command History

```
Version 8.2.1.0        Introduced command
Version 7.7.1.0        Introduced support on C-Series
```
bgp asnotation

Enables you to implement a method for AS Number representation in the CLI.

Syntax

bgp asnotation [asplain | asdot+ | asdot]

To disable a dot or dot+ representation and return to ASPLAIN, enter no bgp asnotation.

Defaults

asplain

Command Modes

ROUTER BGP

Usage Information

You must enable bgp four-octet-as-support before enabling this feature. If you disable four-octet-support after using dot or dot+ format, the AS Numbers revert to asplain text.

When you apply an anotation, it is reflected in the running-configuration. If you change the notation type, the running-configure is updated dynamically and the new notation is shown.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp four-octet-as-support</td>
<td>Enable 4-Byte support for the BGP process</td>
</tr>
</tbody>
</table>

Command History

Version 8.3.1.0 Introduced Dynamic Application of AS Notation changes

Version 8.2.1.0 Introduced

Example

Figure 12-1. Dynamic changes of the bgp asnotation command in the running config

```bash
(conf)#router bgp 1
(conf-router_bgp)#bgp asnotation asdot
(conf-router_bgp)#ex
(conf)#do show run | grep bgp
router bgp 1
bgp four-octet-as-support
bgp asnotation asdot

(conf)#router bgp 1
(conf-router_bgp)#bgp asnotation asdot+
(conf-router_bgp)#ex

(conf)#do show run | grep bgp
router bgp 1
bgp four-octet-as-support
bgp asnotation asdot+

(conf)#router bgp 1
(conf-router_bgp)#bgp asnotation asplain
(conf-router_bgp)#ex

(conf)#do show run | grep bgp
router bgp 1
bgp four-octet-as-support

(conf)#
```
bgp bestpath as-path ignore

Syntax  bgp bestpath as-path ignore

To return to the default, enter no bgp bestpath as-path ignore.

Defaults Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes ROUTER BGP

Usage Information If you enable this command, use the clear ip bgp ipv4 unicast soft * command to recompute the best path.

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

bgp bestpath med confed

Syntax  bgp bestpath med confed

To disable MED comparison on BGP confederation paths, enter no bgp bestpath med confed.

Defaults Disabled

Command Modes ROUTER BGP

Usage Information The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the clear ip bgp ipv4 unicast soft * command to recompute the best path.

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

bgp bestpath med missing-as-best

Syntax  bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

Defaults Disabled

Command Modes ROUTER BGP
The MED is a 4-Byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0 Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0 Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 6.3.1.0 Introduced</td>
</tr>
</tbody>
</table>

**bgp bestpath router-id ignore**

Do not compare router-id information for external paths during best path selection.

**Syntax**

```
bgp bestpath router-id ignore
```

To return to the default selection, use the `no bgp bestpath router-id ignore` command.

**Defaults**

Disabled

**Command Modes**

ROUTER BGP

**Usage Information**

Configuring this option will retain the current best-path. When the session is subsequently reset, the oldest received path will be chosen as the best-path.

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.3.1.0 Introduced</td>
</tr>
</tbody>
</table>

**bgp client-to-client reflection**

Enables you to enable route reflection between clients in a cluster.

**Syntax**

```
bgp client-to-client reflection
```

To disable client-to-client reflection, enter `no bgp client-to-client reflection`.

**Defaults**

Enabled when a route reflector is configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Route reflection to clients is not necessary if all client routers are fully meshed.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp cluster-id</td>
</tr>
<tr>
<td>neighbor route-reflector-client</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0 Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0 Introduced support on C-Series</td>
</tr>
</tbody>
</table>
bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

Syntax: `bgp cluster-id {ip-address | number}`

To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

- ip-address: Enter an IP address as the route reflector cluster ID.
- number: Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults: Not configured.

Command Modes: ROUTER BGP

Usage Information

When a BGP cluster contains only one route reflector, the cluster ID is the route reflector’s router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it will be displayed as an integer.

Related Commands

- `bgp client-to-client reflection`: Enable route reflection between route reflector and clients.
- `neighbor route-reflector-client`: Configure a route reflector and clients.
- `show ip bgp cluster-list`: View paths with a cluster ID.

Command History

- Version 7.8.1.0: Introduced support on S-Series
- Version 7.7.1.0: Introduced support on C-Series

bgp confederation identifier

Configure an identifier for a BGP confederation.

Syntax: `bgp confederation identifier as-number`

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

- as-number: Enter the AS number.
  - Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)

Defaults: Not configured.

Command Modes: ROUTER BGP

Usage Information

You must configure your system to accept 4-Byte formats before entering a 4-Byte AS Number. All the routers in the Confederation must be 4 or 2-Byte identified routers. You cannot mix them.
The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

FTOS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp four-octet-as-support</code></td>
<td>Enable 4-Byte support for the BGP process.</td>
</tr>
<tr>
<td><code>bgp confederation peers </code></td>
<td>Specify the Autonomous Systems (ASs) that belong to the BGP confederation.</td>
</tr>
</tbody>
</table>

**Syntax**

```
bgp confederation peers as-number [...as-number]
```

To return to the default, enter `no bgp confederation peers`.

**Parameters**

<table>
<thead>
<tr>
<th>as-number</th>
<th>Enter the AS number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>...as-number</th>
<th>(OPTIONAL) Enter up to 16 confederation numbers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

All the routers in the Confederation must be 4 or 2 byte identified routers. You cannot mix them.

The Autonomous Systems configured in this command are visible to the EBGP neighbors. Each Autonomous System is fully meshed and contains a few connections to other Autonomous Systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp confederation identifier</code></td>
<td>Configure a confederation ID.</td>
</tr>
<tr>
<td><code>bgp four-octet-as-support</code></td>
<td>Enable 4-Byte support for the BGP process.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td></td>
</tr>
<tr>
<td>7.7.1.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced support on C-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Added support for 4-Byte format</td>
</tr>
</tbody>
</table>

328 | Border Gateway Protocol IPv4 (BGPv4)
bgp dampening

Enable BGP route dampening and configure the dampening parameters.

Syntax

```
bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]
```

To disable route dampening, use the `no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]` command.

Parameters

- **half-life**
  - (OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires.
  - Range: 1 to 45.
  - Default: 15 minutes

- **reuse**
  - (OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route’s Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed).
  - Range: 1 to 20000.
  - Default: 750

- **suppress**
  - (OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route’s Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed).
  - Range: 1 to 20000.
  - Default: 2000

- **max-suppress-time**
  - (OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value.
  - Range: 1 to 255.
  - Default: 60 minutes

- **route-map map-name**
  - (OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map.
  - Only match commands in the configured route map are supported.

Defaults

Disabled.

Command Modes

ROUTER-BGP-ADDRESS FAMILY

Usage Information

If you enter `bgp dampening`, the default values for `half-life`, `reuse`, `suppress`, and `max-suppress-time` are applied. The parameters are position-dependent, therefore, if you configure one parameter, you must configure the parameters in the order they appear in the CLI.

Related Commands

- `show ip bgp dampened-paths` View the BGP paths

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>
**bgp default local-preference**

Change the default local preference value for routes exchanged between internal BGP peers.

**Syntax**

```
bgp default local-preference value
```

To return to the default value, enter `no bgp default local-preference`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. Range: 0 to 4294967295 Default: 100</td>
</tr>
</tbody>
</table>

**Defaults**

100

**Command Modes**

ROUTER BGP

**Usage Information**

The `bgp default local-preference` command setting is applied by all routers within the AS. To set the local preference for a specific route, use the `set local-preference` command in the ROUTE-MAP mode.

**Related Commands**

- `set local-preference` Assign a local preference value for a specific route.

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced on C-Series

---

**bgp enforce-first-as**

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

**Syntax**

```
bgp enforce-first-as
```

To turn off the default, use the `no bgp enforce-first-as` command.

**Defaults**

Enabled

**Command Modes**

ROUTER BGP

**Usage Information**

This is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. Use the `show ip bgp neighbors` command to view the “failed enforce-first-as check counter.

If enforce-first-as is disabled, it can be viewed via the `show ip protocols` command.

**Related Commands**

- `show ip bgp neighbors` View the information exchanged by BGP neighbors
- `show ip protocols` View Information on routing protocols.

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
bgp fast-external-fallover

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

Syntax

```
bgp fast-external-fallover
```

To disable fast external fallover, enter `no bgp fast-external-fallover`.

Defaults

Enabled.

Command Modes

ROUTER BGP

Usage Information

The `bgp fast-external-fallover` command appears in the `show config` command output.

Command History

```
Version 7.8.1.0  Introduced support on S-Series
Version 7.7.1.0  Introduced support for C-Series
```

bgp four-octet-as-support

Enable 4-Byte support for the BGP process.

Syntax

```
bgp four-octet-as-support
```

To disable fast external fallover, enter `no bgp four-octet-as-support`.

Defaults

Disabled (supports 2-Byte format)

Command Modes

ROUTER BGP

Usage Information

Routers supporting 4-Byte ASNs advertise that function in the OPEN message. The behavior of a 4-Byte router will be slightly different depending on whether it is speaking to a 2-Byte router or a 4-Byte router.

When creating Confederations, all the routers in the Confederation must be 4 or 2 byte identified routers. You cannot mix them.

Where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295. Both formats are accepted, and the advertisements will reflect the entered format.

For more information about using the 2 or 4-Byte format, refer to the `Dell Networking OS Configuration Guide`. 
bgp graceful-restart

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

Syntax

```
bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]
```

To return to the default, enter the `no bgp graceful-restart` command.

Parameters

- **restart-time seconds**: Enter the keyword `restart-time` followed by the maximum number of seconds needed to restart and bring-up all the peers.
  - Range: 1 to 3600 seconds
  - Default: 120 seconds

- **stale-path-time seconds**: Enter the keyword `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer’s stale paths.
  - Default: 360 seconds.

- **role receiver-only**: Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults

as above

Command Modes

ROUTER-BGP

Usage Information

This feature is advertised to BGP neighbors through a capability advertisement. In receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

Command History

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced command</td>
</tr>
<tr>
<td></td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

Syntax

```
bgp log-neighbor-changes
```

To disable logging, enter `no bgp log-neighbor-changes`.

Defaults

Enabled.

Command Modes

ROUTER BGP

Usage Information

Use the `show logging` command in the EXEC mode to view BGP neighbor resets.
The `bgp log-neighbor-changes` command appears in the `show config` command output.

<table>
<thead>
<tr>
<th>Command</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>View logging settings and system messages logged to the system.</td>
</tr>
</tbody>
</table>

**Related Commands**

**bgp recursive-bgp-next-hop**

`bgp recursive-bgp-next-hop` Enable next-hop resolution through other routes learned by BGP.

**Syntax**

`bgp recursive-bgp-next-hop`

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

**Defaults**

Enabled

**Command Modes**

ROUTER BGP

**Usage Information**

This command is a knob to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route’s protocol source and is checked if the route is learned from BGP or not.

**bgp non-deterministic-med**

`bgp non-deterministic-med` Compare MEDs of paths from different Autonomous Systems.

**Syntax**

`bgp non-deterministic-med`

To return to the default, enter `no bgp non-deterministic-med`.

**Defaults**

Disabled (that is, paths/routes for the same destination but from different ASs will not have their MEDs compared).

**Command Modes**

ROUTER BGP

**Usage Information**

In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to FTOS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors since MED may or may not get compared between adjacent paths. In deterministic mode (`no bgp non-deterministic-med`), FTOS compares MED between adjacent paths within an AS group since all paths in the AS group are from the same AS.

When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter `clear ip bgp ipv4 unicast soft` command to clear existing paths.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>

**bgp recursive-bgp-next-hop**

`bgp recursive-bgp-next-hop` Enable next-hop resolution through other routes learned by BGP.

**Syntax**

`bgp recursive-bgp-next-hop`

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

**Defaults**

Enabled

**Command Modes**

ROUTER BGP

**Usage Information**

This command is a knob to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route’s protocol source and is checked if the route is learned from BGP or not.
The **clear ip bgp** command is required for this command to take effect and to keep the BGP database consistent. Execute the **clear ip bgp** command right after executing this command.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clear ip bgp ipv4 unicast soft</strong></td>
<td>Clear and reapply policies for IPv4 routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

**Syntax**

```
bgp regex-eval-optz-disable
```

**Defaults**

Enabled by default

**Command Modes**

ROUTER BGP (conf-router_bgp)

**Usage Information**

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the show bgp commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expense of RP1 processor memory.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip protocols</strong></td>
<td>View information on all routing protocols enabled and active on the E-Series.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
**bgp retain-ibgp-nexthop**

BGP does not update the NEXT_HOP attribute if it is a Route-Reflector. Use this command to retain the NEXT_HOP attribute when advertising to internal BGP peer.

**Syntax**

```
bgp retain-ibgp-nexthop
```

**Defaults**

Disabled

**Command Modes**

ROUTER BGP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced on E-Series TeraScale, C-Series, and S-Series.</td>
</tr>
<tr>
<td>8.3.1.2</td>
<td>Introduced on E-Series ExaScale.</td>
</tr>
</tbody>
</table>

**bgp router-id**

Assign a user-given ID to a BGP router.

**Syntax**

```
bgp router-id ip-address
```

To delete a user-assigned IP address, enter `no bgp router-id`.

**Parameters**

- `ip-address`: Enter an IP address in dotted decimal format to reset only that BGP neighbor.

**Defaults**

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

**Command Modes**

ROUTER BGP

**Usage Information**

Peering sessions are reset when you change the router ID of a BGP router.

---

**Example**

**Figure 12-2. Command Example: no bgp regex-eval-optz-disable**

```
{conf-router_bgp)#no bgp regex-eval-optz-disable
{conf-router_bgp)#do show ip protocols
Routing Protocol is "ospf 22222"
  Router ID is 2.2.2.2
  Area 51 Routing for Networks 51 10.10.10.0/00

Routing Protocol is "bgp 1"
  Cluster Id is set to 10.10.10.0
  Router Id is set to 10.10.10.0
  Fast-external-fallover enabled
  Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
    BGP table version is 0, main routing table version 0
    Distance: external 20 internal 200 local 200

{conf-router_bgp)#
```

Version 8.4.1.0 Introduced on E-Series TeraScale, C-Series, and S-Series.

Version 8.3.1.2 Introduced on E-Series ExaScale.

---
**Command History**

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**bgp soft-reconfig-backup**

Use this command *only* when route-refresh is *not* negotiated between peers to avoid having a peer resend BGP updates.

**Syntax**

```
bgp soft-reconfig-backup
```

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

**Defaults**

Off

**Command Modes**

ROUTER BGP

**Usage Information**

When soft-reconfiguration is enabled for a neighbor and the `clear ip bgp soft in` is executed, the update database stored in the router is replayed and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is *not* negotiated with the peer. If the request is indeed negotiated (upon execution of `clear ip bgp soft in`), then BGP sends a route-refresh request to the neighbor and receives all of the peer’s updates.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ip bgp ipv4 unicast soft in</code></td>
<td>Activate inbound policies for IPv4 routes without resetting the BGP TCP session.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version 8.4.1.0</th>
<th>Added support for IPv4 multicast and IPv6 unicast address families</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 7.2.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**capture bgp-pdu neighbor**

Enable capture of an IPv4 BGP neighbor packet.

**Syntax**

```
capture bgp-pdu neighbor ipv4-address direction {both | rx | tx}
```

To disable capture of the IPv4 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv4-address` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4-address</code></td>
<td>Enter the IPv4 address of the target BGP neighbor.</td>
</tr>
<tr>
<td><code>direction</code></td>
<td>Enter the keyword <code>direction</code> and a direction—either <code>rx</code> for inbound, <code>tx</code> for outbound, or <code>both</code>.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

EXEC Privilege
### capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

**Syntax**

```
capture bgp-pdu max-buffer-size 100-102400000
```

**Parameters**

- `100-102400000`: Enter a size for the capture buffer.

**Defaults**

- 40960000 bytes.

**Command Modes**

- EXEC Privilege

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture bgp-pdu neighbor</code></td>
<td>Enable capture of an IPv4 BGP neighbor packet.</td>
</tr>
<tr>
<td><code>capture bgp-pdu neighbor (ipv6)</code></td>
<td>Enable capture of an IPv6 BGP neighbor packet.</td>
</tr>
<tr>
<td><code>show capture bgp-pdu neighbor</code></td>
<td>Display BGP packet capture information for an IPv6 address on the E-Series.</td>
</tr>
</tbody>
</table>

**Command History**

- **Version 7.8.1.0**: Introduced support on S-Series
- **Version 7.7.1.0**: Introduced support on C-Series
- **Version 7.5.1.0**: Introduced

### clear ip bgp ipv4 unicast soft

Clear and reapply policies for IPv4 routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

**Syntax**

```
clear ip bgp [* | as-number | ipv4-neighbor-addr | ipv6-neighbor-addr | peer-group name] [ipv4 unicast] soft [in | out]
```

**Parameters**

- `*`: Clear and reapply policies for all BGP sessions.
- `as-number`: Clear and reapply policies for all neighbors belonging to the AS.
  - Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4-neighbor-addr</code></td>
<td>Clear and reapply policies for a neighbor.</td>
</tr>
<tr>
<td><code>ipv6-neighbor-addr</code></td>
<td></td>
</tr>
<tr>
<td><code>peer-group name</code></td>
<td>Clear and reapply policies for all BGP routers in the specified peer group.</td>
</tr>
<tr>
<td><code>ipv4 unicast</code></td>
<td>Clear and reapply policies for all IPv4 unicast routes.</td>
</tr>
</tbody>
</table>

**Command History**

- **Version 7.5.1.0**: Introduced

---

Border Gateway Protocol IPv4 (BGPv4) | 337
### clear ip bgp peer-group

- **Description:** Reset a peer-group’s BGP sessions.

- **Syntax:**
  
  ```plaintext
  clear ip bgp peer-group peer-group-name
  ```

- **Parameters:**
  - `peer-group-name`: Enter the peer group name to reset the BGP sessions within that peer group.

- **Command Modes:**
  - EXEC Privilege

- **Command History:**
  - Version 8.4.1.0: Added BGP Soft Reconfiguration support for IPv4 unicast and IPv6 routes
  - Version 7.8.1.0: Introduced support on S-Series
  - Version 7.7.1.0: Introduced support on C-Series
  - Version 7.2.1.0: Introduced

### clear ip bgp dampening

- **Description:** Clear information on route dampening and return suppressed route to active state.

- **Syntax:**
  
  ```plaintext
  clear ip bgp dampening [vrf vrf-name] [ip-address mask]
  ```

- **Parameters:**
  - `vrf vrf-name`: (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
  - `ip-address mask`: (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.

- **Command Modes:**
  - EXEC Privilege

- **Usage Information:**
  - After you enter this command, the software deletes history routes and returns suppressed routes to active state.

- **Command History:**
  - Version 8.4.6.0: Added support for VRF.
  - Version 7.8.1.0: Introduced support on S-Series
  - Version 7.7.1.0: Introduced support on C-Series
clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

**Syntax**

`clear ip bgp flap-statistics [vrf vrf-name | ip-address mask | filter-list as-path-name | regexp regular-expression]`

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.
- **ip-address mask** (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.
- **filter-list as-path-name** (OPTIONAL) Enter the keyword filter-list followed by the name of a configured AS-PATH list.
- **regexp regular-expression** (OPTIONAL) Enter the keyword regexp followed by regular expressions. Use one or a combination of the following:
  - . = (period) any single character (including a white space)
  - * = (asterisk) the sequences in a pattern (0 or more sequences)
  - + = (plus) the sequences in a pattern (1 or more sequences)
  - ? = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
  - [ ] = (brackets) a range of single-character patterns.
  - ( ) = (parenthesis) groups a series of pattern elements to a single element
  - { } = (braces) minimum and the maximum match count
  - ^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - $ = (dollar sign) the end of the output string.

**Command Modes**

EXEC Privilege

**Usage Information**

If you enter clear ip bgp flap-statistics without any parameters, all statistics are cleared.

**Related Commands**

- `show debugging` View enabled debugging operations.
- `show ip bgp flap-statistics` View BGP flap statistics.
- `undebug all` Disable all debugging operations.

**Command History**

- Version 8.4.6.0 Added support for VRF.
- Version 7.8.1.0 Introduced support on S-Series.
- Version 7.7.1.0 Introduced support on C-Series.

---

display ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

**Syntax**

`debug ip bgp [vrf vrf-name | ip-address | peer-group peer-group-name] [in | out]`

To disable all BGP debugging, enter `no debug ip bgp`. 
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF. Range: 1 to 63.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group peer-group-name</td>
<td>Enter the keyword <code>peer-group</code> followed by the name of the peer group.</td>
</tr>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword <code>in</code> to view only information on inbound BGP routes.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword <code>out</code> to view only information on outbound BGP routes.</td>
</tr>
</tbody>
</table>

### Command Modes

**EXEC Privilege**

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the debugging command. The `in` and `out` parameters cancel each other; for example, if you enter `debug ip bgp in` and then enter `debug ip bgp out`, you will not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

### Related Commands

- `debug ip bgp events` View information about BGP events.
- `debug ip bgp keepalives` View information about BGP keepalives.
- `debug ip bgp notifications` View information about BGP notifications.
- `debug ip bgp updates` View information about BGP updates.
- `show debugging` View enabled debugging operations.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for VRF.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

### debug ip bgp dampening

**Syntax**

```
debug ip bgp dampening [in | out]
```

Display information on routes being dampened.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword <code>in</code> to view only inbound dampened routes.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword <code>out</code> to view only outbound dampened routes.</td>
</tr>
</tbody>
</table>

**Command Modes**

**EXEC Privilege**

Enter `no debug ip bgp` command to remove all configured debug commands for BGP.
### debug ip bgp events

Display information on local BGP state changes and other BGP events.

**Syntax**
```
debug ip bgp [ip-address | peer-group peer-group-name] events [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] events` command.

**Parameters**
- `ip-address` (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- `peer-group peer-group-name` (OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
- `in` (OPTIONAL) Enter the keyword `in` to view only events on inbound BGP messages.
- `out` (OPTIONAL) Enter the keyword `out` to view only events on outbound BGP messages.

**Command Modes**
EXEC Privilege

**Usage Information**
Enter `no debug ip bgp` command to remove all configured debug commands for BGP.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

### debug ip bgp keepalives

Display information about BGP keepalive messages.

**Syntax**
```
debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

**Parameters**
- `ip-address` (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- `peer-group peer-group-name` (OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
- `in` (OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
- `out` (OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.
debug ip bgp notifications

Enables you to view information about BGP notifications received from neighbors.

Syntax
debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]

To disable debugging, use the no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out] command.

Parameters
- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group peer-group-name** (OPTIONAL) Enter the keyword peer-group followed by the name of the peer group.
- **in** (OPTIONAL) Enter the keyword in to view BGP notifications received from neighbors.
- **out** (OPTIONAL) Enter the keyword out to view BGP notifications sent to neighbors.

Command Modes
EXEC Privilege

Usage Information
Enter no debug ip bgp command to remove all configured debug commands for BGP.

Command History
Version 7.8.1.0 Introduced support on S-Series
Version 7.7.1.0 Introduced support on C-Series

debug ip bgp ipv4 unicast soft-reconfiguration

Enable soft-reconfiguration debugging for IPv4 unicast routes.

Syntax
debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv4 unicast soft-reconfiguration

To disable debugging, use the no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv4 unicast soft-reconfiguration command.

Parameters
- **ipv4-address | ipv6-address** Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
- **peer-group-name** Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
- **ipv4 unicast** Debug soft reconfiguration for IPv4 unicast routes.
Defaults
Disabled

Command Modes
EXEC Privilege

Usage Information
This command turns on BGP soft-reconfiguration inbound debugging for IPv4 unicast routes. If no neighbor is specified, debug is turned on for all neighbors.

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced support for IPv4 multicast and IPv6 unicast routes</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**debug ip bgp updates**

Enables you to view information about BGP updates.

**Syntax**

```
default-metric
```

Enables you to change the metrics of redistributed routes to locally originated routes. Use this command with the redistribute command.

**Syntax**

```
default-metric number
```

To return to the default setting, enter `no default-metric`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword <code>in</code> to view only BGP updates received from neighbors.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword <code>out</code> to view only BGP updates sent to neighbors.</td>
</tr>
<tr>
<td>prefix-list</td>
<td>(OPTIONAL) Enter the keyword <code>prefix-list</code> followed by the name of an established prefix list. If the prefix list is not configured, the default is <code>permit</code> (to allow all routes).</td>
</tr>
<tr>
<td>prefix-list-name</td>
<td>(OPTIONAL) Enter the keyword <code>prefix-list-name</code> followed by the name of an established prefix list. If the prefix list is not configured, the default is <code>permit</code> (to allow all routes).</td>
</tr>
<tr>
<td>ip-address</td>
<td>(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Usage Information**

Enter no debug ip bgp command to remove all configured debug commands for BGP.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>
The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter a number as the metric to be assigned to routes from other protocols. Range: 1 to 4294967295.</td>
</tr>
</tbody>
</table>

**Defaults**

0

**Command Modes**

ROUTER BGP

**Usage Information**

The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp always-compare-med</code></td>
<td>Enable comparison of all BGP MED attributes.</td>
</tr>
<tr>
<td><code>redistribute</code></td>
<td>Redistribute routes from other routing protocols into BGP.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**description**

Enter a description of the BGP routing protocol.

**Syntax**

```
description {description}
```

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

**Parameters**

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

**Defaults**

No default behavior or values

**Command Modes**

ROUTER BGP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>pre-7.7.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Related Commands**

`router bgp` Enter ROUTER mode on the switch.

**distance bgp**

Configure three administrative distances for routes.

**Syntax**

```
distance bgp external-distance internal-distance local-distance
```

To return to default values, enter `no distance bgp`.
Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>external-distance</td>
<td>Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20</td>
</tr>
<tr>
<td>internal-distance</td>
<td>Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200</td>
</tr>
<tr>
<td>local-distance</td>
<td>Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200</td>
</tr>
</tbody>
</table>

Defaults

external-distance = 20; internal-distance = 200; local-distance = 200.

Command Modes

ROUTER BGP

Usage Information

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

Caution: Dell Force10 recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax

```
maximum-paths {ebgp | ibgp} number
```

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebgp</td>
<td>Enter the keyword ebgp to enable multipath support for External BGP routes.</td>
</tr>
<tr>
<td>ibgp</td>
<td>Enter the keyword ibgp to enable multipath support for Internal BGP routes.</td>
</tr>
<tr>
<td>number</td>
<td>Enter a number as the maximum number of parallel paths. Range: 1 to 16 Default: 1</td>
</tr>
</tbody>
</table>

Defaults

1

Command Modes

ROUTER BGP

Usage Information

If you enable this command, use the clear ip bgp ipv4 unicast soft * command to recompute the best path.
Command History

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**neighbor activate**

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier).

**Syntax**

```
neighbor [ip-address | peer-group-name] activate
```

To disable, use the `no neighbor [ip-address | peer-group-name] activate` command.

**Parameters**

- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name** (OPTIONAL) Enter the name of the peer group.
- **activate** Enter the keyword `activate` to enable the neighbor/peer group in the new AFI/SAFI.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

**Usage Information**

By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv4/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.

**Command History**

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**neighbor advertisement-interval**

Set the advertisement interval between BGP neighbors or within a BGP peer group.

**Syntax**

```
neighbor {ip-address | peer-group-name} advertisement-interval seconds
```

To return to the default value, use the `no neighbor {ip-address | peer-group-name} advertisement-interval` command.

**Parameters**

- **ip-address** Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name** Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- **seconds** Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

**Defaults**

`seconds = 5` seconds (internal peers); `seconds = 30` seconds (external peers)

**Command Modes**

ROUTER BGP
neighbor advertisement-start

Set the minimum interval before starting to send BGP routing updates.

Syntax

neighbor {ip-address} advertisement-start seconds

To return to the default value, use the no neighbor {ip-address} advertisement-start command.

Parameters

- **ip-address**: Enter the IP address of the neighbor in dotted decimal format.
- **seconds**: Enter a number as the time interval, in seconds, before BGP route updates are sent. Range: 0 to 3600 seconds.

Defaults

- **none**

Command Modes

- ROUTER BGP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

Syntax

neighbor {ip-address | peer-group-name} allowas-in number

To return to the default value, use the no neighbor {ip-address | peer-group-name} allowas-in command.

Parameters

- **ip-address**: Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name**: Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- **number**: Enter a number of times to allow this neighbor ID to use the AS path. Range: 1 to 10.

Defaults

- Not configured.

Command Modes

- ROUTER BGP

Related Commands

- bgp four-octet-as-support: Enable 4-Byte support for the BGP process.
neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Syntax:

```
neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
```

To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group to set the default route of all routers in that peer group.</td>
</tr>
<tr>
<td>route-map</td>
<td>(OPTIONAL) Enter the keyword <code>route-map</code> followed by the name of a configured route map.</td>
</tr>
</tbody>
</table>

Defaults: Not configured.

Command Modes: ROUTER BGP

Usage Information:

If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

Command History:

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

Syntax:

```
neighbor {ip-address | peer-group-name} description text
```

To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group.</td>
</tr>
<tr>
<td>text</td>
<td>Enter a continuous text string up to 80 characters.</td>
</tr>
</tbody>
</table>

Defaults: Not configured.

Command Modes: ROUTER BGP

Command History:

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series
neighbor distribute-list

Distribute BGP information via an established prefix list.

**Syntax**

```
neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}
```

To delete a neighbor distribution list, use the command:

```
no neighbor {ip-address | peer-group-name} distribute-list prefix-list-name {in | out}
```

**Parameters**

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group.
- `prefix-list-name`: Enter the name of an established prefix list.
  - If the prefix list is not configured, the default is `permit` (to allow all routes).
- `in`: Enter the keyword `in` to distribute only inbound traffic.
- `out`: Enter the keyword `out` to distribute only outbound traffic.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

**Related Commands**

- `ip as-path access-list`: Configure IP AS-Path ACL.
- `neighbor filter-list`: Assign a AS-PATH list to a neighbor or peer group.
- `neighbor route-map`: Assign a route map to a neighbor or peer group.

**Command History**

- Version 7.8.1.0: Introduced support on S-Series
- Version 7.7.1.0: Introduced support on C-Series

neighor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

**Syntax**

```
neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]
```

To disallow and disconnect connections, use the command:

```
no neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]
```

**Parameters**

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group.
- `ttl`: (OPTIONAL) Enter the number of hops as the Time to Live (ttl) value.
  - Range: 1 to 255.
  - Default: 255

**Defaults**

Disabled.
neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

Syntax

```
neighbor {ipv4-address | peer-group-name} fall-over
```

To disable, use the `no neighbor {ipv4-address | peer-group-name} fall-over` command.

Parameters

- `ipv4-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group.

Defaults

Disabled

Command Modes

ROUTER BGP

Usage Information

When fall-over is enabled, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (i.e., no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands

- `show ip bgp neighbors`: Display information on the BGP neighbors

Command History

- Version 7.8.1.0: Introduced support on S-Series
- Version 7.7.1.0: Introduced support on C-Series
- Version 7.4.1.0: Introduced

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

Syntax

```
neighbor {ip-address | peer-group-name} filter-list as-path-name {in | out}
```

To delete a BGP filter, use the `no neighbor {ip-address | peer-group-name} filter-list as-path-name {in | out}` command.

Parameters

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to apply the filter to all routers in the peer group.
ip as-path access-list

Use the `ip as-path access-list` command syntax in the `CONFIGURATION` mode to enter the AS-PATH ACL mode and configure AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute.

**Related Commands**

- `ip as-path access-list` - Enter AS-PATH ACL mode and configure AS-PATH filters.

**Command History**

- **Version 7.8.1.0** Introduced support on S-Series
- Increased name string to accept up to 140 characters. Prior to 7.8.1.0, ACL names are up to 16 characters long.
- **Version 7.7.1.0** Introduced support on C-Series

---

**neighbor graceful-restart**

Enable graceful restart on a BGP neighbor.

**Syntax**

```
neighbor {ip-address | peer-group-name} graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]
```

**Parameters**

- `ip-address` - Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` - Enter the name of the peer group to apply the filter to all routers in the peer group.
- `restart-time seconds` - Enter the keyword `restart-time` followed by the maximum number of seconds needed to restart and bring-up all the peers.
  - Range: 1 to 3600 seconds
  - Default: 120 seconds
- `stale-path-time seconds` - Enter the keyword `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer’s stale paths.
  - Default: 360 seconds
- `role receiver-only` - Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

**Defaults**

- as above

**Command Modes**

- ROUTER BGP
Usage Information
This feature is advertised to BGP neighbors through a capability advertisement. In receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

Command History
- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series

neighbor local-as
Configure Internal BGP (IBGP) routers to accept external routes from neighbors with a local AS number in the AS number path

Syntax
neighbor {ip-address | peer-group-name} local-as as-number [no-prepend]

Parameters
- ip-address: Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name: Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- as-number: Enter the AS number to reset all neighbors belonging to that AS.
  Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)
- no prepend: Specifies that local AS values are not prepended to announcements from the neighbor.

Defaults
Not configured.

Command Modes
ROUTER BGP

Related Commands
bgp four-octet-as-support : Enable 4-Byte support for the BGP process.

Command History
- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced command

neighbor maximum-prefix
Control the number of network prefixes received.

Syntax
neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]

Parameters
- maximum-prefix: Specify the maximum number of prefixes that can be received from the neighbor.
- threshold: Set the value of the threshold that triggers a warning message.
- warning-only: Enable or disable warning messages.

Defaults
No maximum or threshold is configured.

Command Modes
ROUTER BGP

Related Commands
bgp four-octet-as-support : Enable 4-Byte support for the BGP process.

Command History
- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced command
neighbor next-hop-self

Enables you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

Syntax

`neighbor {ip-address | peer-group-name} next-hop-self`

To return to the default setting, use the `no neighbor {ip-address | peer-group-name} next-hop-self` command.

Parameters

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group.

Defaults

Disabled.

Command Modes

ROUTER BGP

Usage Information

If the `set next-hop` command in the ROUTE-MAP mode is configured, its configuration takes precedence over the `neighbor next-hop-self` command.
neighbor password

Enable Message Digest 5 (MD5) authentication on the TCP connection between two neighbors.

**Syntax**

```plaintext
neighbor {ip-address | peer-group-name} password [encryption-type] password
```

To delete a password, use the `no neighbor {ip-address | peer-group-name} password` command.

**Parameters**

- `ip-address` Enter the IP address of the router to be included in the peer group.
- `peer-group-name` Enter the name of a configured peer group.
- `encryption-type` (OPTIONAL) Enter 7 as the encryption type for the `password` entered. 7 means that the password is encrypted and hidden.
- `password` Enter a text string up to 80 characters long. The first character of the `password` must be a letter. You cannot use spaces in the password.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the `peer-group-name` parameter, all the members of the peer group will inherit the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```plaintext
%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address] :179 to [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```plaintext
%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from [peer's IP address] : 11502 to [local router's IP address] :179
```

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series
neighbor peer-group (assigning peers)

Enables you to assign one peer to a existing peer group.

Syntax

```
neighbor ip-address peer-group peer-group-name
```

To delete a peer from a peer group, use the `no neighbor ip-address peer-group peer-group-name` command.

Parameters

- `ip-address` Enter the IP address of the router to be included in the peer group.
- `peer-group-name` Enter the name of a configured peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

You can assign up to 256 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group’s configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- `neighbor advertisement-interval`
- `neighbor distribute-list out`
- `neighbor filter-list out`
- `neighbor next-hop-self`
- `neighbor route-map out`
- `neighbor route-reflector-client`
- `neighbor send-community`

A neighbor may keep its configuration after it was added to a peer group if the neighbor’s configuration is more specific than the peer group’s, and the neighbor’s configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

Related Commands

- `clear ip bgp ipv4 unicast soft` Resets BGP sessions.
- `neighbor peer-group (creating group)` Create a peer group.
- `show ip bgp peer-group` View BGP peers.
- `show ip bgp neighbors` View BGP neighbors configurations.

Command History

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series

neighbor peer-group (creating group)

Enables you to create a peer group and assign it a name.

Syntax

```
neighbor peer-group-name peer-group
```
To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer-group-name</code></td>
<td>Enter a text string up to 16 characters long as the name of the peer group.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

When a peer group is created, it is disabled (shut mode).

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor peer-group passive</code></td>
<td>Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but will respond to one.</td>
</tr>
</tbody>
</table>

**Syntax**

`neighbor peer-group-name peer-group passive [match-af]`

To delete a passive peer-group, use the `no neighbor peer-group-name peer-group passive` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer-group-name</code></td>
<td>Enter a text string up to 16 characters long as the name of the peer group.</td>
</tr>
<tr>
<td><code>match-af</code></td>
<td>(Optional) Enter the keyword <code>match-af</code> to require that the address family of a peer matches the address family of the subnet assigned to the specified peer group before the peer’s adjacency is brought up.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

After you configure a peer group as passive, you must assign it a subnet using the `neighbor soft-reconfiguration inbound` command.

Use the keyword `match-af` to restrict the peer adjacency established with a passive peer group. Entering `match-af` requires that a peer’s address family matches the address family of the subnet assigned to the peer group before the peer’s adjacency is brought up. For example, if the address family of the peer group’s subnet is IPv6, only IPv6 neighbors in the subnet can be brought up in a peering session.

You can only specify the `match-af` option when you first enter the `neighbor peer-group passive` command to configure passive peering for a BGP group. An error message is displayed if you later try to add this option to an existing passive peer group by re-entering the command.
neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

**Syntax**

```
neighbor {ip-address | peer-group-name} remote-as number
```

To delete a remote AS entry, use the `no neighbor {ip-address | peer-group-name} remote-as number` command.

**Parameters**

- `ip-address`: Enter the IP address of the neighbor to enter the remote AS in its routing table.
- `peer-group-name`: Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
- `number`: Enter a number of the AS.
  
  Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte)

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

You must configure your system to accept 4-Byte formats before entering a 4-Byte AS Number. If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (shutdown).

**Related Commands**

- `router bgp`: Enter the ROUTER BGP mode and configure routes in an AS.
- `bgp four-octet-as-support`: Enable 4-Byte support for the BGP process.

**Command History**

- **Version 8.4.2.0**: Added support for the `match-as` keyword
- **Version 7.8.1.0**: Introduced support on S-Series
- **Version 7.7.1.0**: Introduced support on C-Series

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

**Syntax**

```
neighbor {ip-address | peer-group-name} remove-private-as
```

To return to the default, use the `no neighbor {ip-address | peer-group-name} remove-private-as` command.
neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax

`neighbor {ip-address | peer-group-name} route-map map-name {in | out}`

To remove the route map, use the `no neighbor {ip-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group.
- `map-name`: Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).
- `in`: Enter the keyword `in` to filter inbound routes.
- `out`: Enter the keyword `out` to filter outbound routes.

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.
If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
</tr>
</tbody>
</table>
neighbor route-reflector-client

Configure the router as a route reflector and the specified neighbors as members of the cluster.

Syntax

```
neighbor {ip-address | peer-group-name} route-reflector-client
```

To remove one or more neighbors from a cluster, use the `no neighbor {ip-address | peer-group-name} route-reflector-client` command. If you delete all members of a cluster, you also delete the route-reflector configuration on the router.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need not be fully meshed. By default, when no route reflector is used, internal BGP (IBGP) speakers in the network must be fully meshed.

The first time you enter this command the router is configured as a route reflector and the specified BGP neighbors are configured as clients in the route-reflector cluster.

When you remove all clients of a route reflector using the `no neighbor route-reflector-client` command, the router no longer functions as a route reflector.

If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the `no bgp client-to-client reflection` command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp client-to-client reflection</td>
<td>Enable route reflection between route reflector and clients.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced support on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>
neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

Syntax

neighbor {ip-address | peer-group-name} send-community

To disable sending a COMMUNITY attribute, use the no neighbor {ip-address | peer-group-name} send-community command.

Parameters

- `ip-address`: Enter the IP address of the peer router in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.

Defaults

Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes

ROUTER BGP

Usage Information

To configure a COMMUNITY attribute, use the set community command in the ROUTE-MAP mode.

Command History

Version 7.8.1.0 Introduced support on S-Series

Version 7.7.1.0 Introduced support on C-Series

neighbor shutdown

Disable a BGP neighbor or peer group.

Syntax

neighbor {ip-address | peer-group-name} shutdown

To enable a disabled neighbor or peer group, use the neighbor {ip-address | peer-group-name} no shutdown command.

Parameters

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults

Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes

ROUTER BGP

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The neighbor shutdown command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the show ip bgp summary command to confirm its status.

Related Commands

- `show ip bgp summary`: Displays the current BGP configuration.
- `show ip bgp neighbors`: Displays the current BGP neighbors.
### neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing inbound route updates.

**Syntax**
```plaintext
neighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound
```

**Parameters**
- `ipv4-address`: Enter the IP address of the neighbor for which you want to start storing inbound routing updates.
- `ipv6-address`: Enter the IP address of the neighbor for which you want to start storing inbound routing updates.
- `peer-group-name`: Enter the name of the peer group for which you want to start storing inbound routing updates.

**Defaults**
Disabled

**Command Modes**
ROUTER BGP

**Usage Information**
This command enables soft-reconfiguration for the specified BGP neighbor. BGP will store all updates for inbound IPv4 routes received by the neighbor but will not reset the peer-session.

**Caution:** Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.

**Related Commands**
- `show ip bgp neighbors`: Display routes received on a neighbor

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv4 multicast and IPv4 unicast address families</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
**neighbor subnet**

Enable passive peering so that the members of the peer group are dynamic.

**Syntax**

```
neighbor peer-group-name subnet subnet-number mask
```

To remove passive peering, use the `no neighbor peer-group-name subnet subnet-number mask` command.

**Parameters**

- `subnet-number` Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group.
  To allow all addresses, enter 0.0.0.0/0.

- `mask` Enter a prefix mask in / prefix-length format (/x).

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series

---

**neighbor timers**

Set keepalive and hold time timers for a BGP neighbor or a peer group.

**Syntax**

```
neighbor {ip-address | peer-group-name} timers keepalive holdtime
```

To return to the default values, use the `no neighbor {ip-address | peer-group-name} timers` command.

**Parameters**

- `ip-address` Enter the IP address of the peer router in dotted decimal format.

- `peer-group-name` Enter the name of the peer group to set the timers for all routers within the peer group.

- `keepalive` Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers.
  Range: 1 to 65535
  Default: 60 seconds

- `holdtime` Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead.
  Range: 3 to 65535
  Default: 180 seconds

**Defaults**

```
keepalive = 60 seconds; holdtime = 180 seconds.
```

**Command Modes**

ROUTER BGP

**Usage Information**

Timer values configured with the `neighbor timers` command override the timer values configured with the any other command.
When two neighbors, configured with different *keepalive* and *holdtime* values, negotiate for new values, the resulting values will be as follows:

- the lower of the *holdtime* values is the new *holdtime* value, and
- whichever is the lower value; one-third of the new *holdtime* value, or the configured *keepalive* value is the new *keepalive* value.

### Command Syntax

**neighbor update-source**

Enable the E-Series software to use Loopback interfaces for TCP connections for BGP sessions.

**Syntax**

```
neighbor {ip-address | peer-group-name} update-source interface
```

To use the closest interface, use the `no neighbor {ip-address | peer-group-name} update-source interface` command.

**Parameters**

- `ip-address`: Enter the IP address of the peer router in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to disable all routers within the peer group.
- `interface`: Enter the keyword `loopback` followed by a number of the loopback interface. Range: 0 to 16383.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

### Command History

- **Version 7.8.1.0**: Introduced support on S-Series
- **Version 7.7.1.0**: Introduced support on C-Series

### Command Syntax

**neighbor weight**

Assign a weight to the neighbor connection, which is used to determine the best path.

**Syntax**

```
neighbor {ip-address | peer-group-name} weight weight
```

To remove a weight value, use the `no neighbor {ip-address | peer-group-name} weight` command.

**Parameters**

- `ip-address`: Enter the IP address of the peer router in dotted decimal format.
### peer-group-name
Enter the name of the peer group to disable all routers within the peer group.

### weight
Enter a number as the weight.
- Range: 0 to 65535
- Default: 0

---

**Defaults**
0

**Command Modes**
ROUTER BGP

**Usage Information**
In the FTOS best path selection process, the path with the highest weight value is preferred.

**Note:**
Reset the neighbor connection (clear ip bgp ipv4 unicast soft * command) to apply the weight to the connection and recompute the best path.

If the `set weight` command is configured in a route map applied to this neighbor, the weight set in that command overrides the weight set in the `neighbor weight` command.

**Related Commands**
- `set weight` Assign a weight to all paths meeting the route map criteria.

---

**Command History**
- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series

### network
Specify the networks for the BGP process and enter them in the BGP routing table.

**Syntax**

```
network ip-address mask [route-map map-name]
```

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

**Parameters**
- **ip-address**
  - Enter an IP address in dotted decimal format of the network.
- **mask**
  - Enter the mask of the IP address in the slash prefix length format (for example, /24).
  - The mask appears in command outputs in dotted decimal format (A.B.C.D).
- **route-map map-name**
  - (OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map.

Only the following ROUTE-MAP mode commands are supported:
- `match ip address`
- `set community`
- `set local-preference`
- `set metric`
- `set next-hop`
- `set origin`
- `set weight`

If the route map is not configured, the default is deny (to drop all routes).

**Defaults**
Not configured.

**Command Modes**
ROUTER BGP
Dell Networking OS software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network</code></td>
<td>Specify this IGP route as the preferred route.</td>
</tr>
<tr>
<td><code>redistribute</code></td>
<td>Redistribute routes into BGP.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

### network backdoor

Specify this IGP route as the preferred route.

**Syntax**

```
network ip-address mask backdoor
```

To remove a network, use the `no network ip-address mask backdoor` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Enter an IP address in dotted decimal format of the network.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Usage Information**

Though Dell Networking OS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

### redistribute

Redistribute routes into BGP.

**Syntax**

```
redistribute {connected | static} [route-map map-name]
```

To disable redistribution, use the `no redistribution {connected | 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 <code>connected</code> to redistribute routes from physically connected interfaces.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Enter the keyword <code>static</code> to redistribute non-connected routes.</td>
</tr>
<tr>
<td><code>route-map map-name</code></td>
<td>Enter the keyword <code>route-map</code> followed by the name of the route-map.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `network` - Specify this IGP route as the preferred route.
- `redistribute` - Redistribute routes into BGP.
### redistribute isis

Redistribute IS-IS routes into BGP.

**Syntax**

```
redistribute isis [WORD] [level-1 [level-1-2] [level-2] [metric metric-value] [route-map map-name]]
```

To return to the default values, enter the no redistribute isis [WORD] [level-1 [level-1-2 | level-2] [metric metric-value] [route-map map-name] command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WORD</strong></td>
<td>ISO routing area tag</td>
</tr>
<tr>
<td><strong>level-1</strong></td>
<td>(OPTIONAL) Enter the keyword level-1 to independently redistributed into Level 1 routes only.</td>
</tr>
<tr>
<td><strong>level-1-2</strong></td>
<td>(OPTIONAL) Enter the keyword level-1-2 to independently redistributed into Level 1-2 routes only.</td>
</tr>
<tr>
<td><strong>level-2</strong></td>
<td>(OPTIONAL) Enter the keyword level-2 to independently redistributed into Level 2 routes only.</td>
</tr>
<tr>
<td><strong>metric</strong></td>
<td>(OPTIONAL) Enter the keyword metric followed by the metric-value to set the MED.</td>
</tr>
<tr>
<td><strong>route-map</strong></td>
<td>(OPTIONAL) Enter the keyword route-map followed by the name of an established route map.</td>
</tr>
</tbody>
</table>

### Related Commands

- `neighbor default-originateroute-map map-name`: Inject the default route.
**Command Modes**

ROUTER BGP

**Usage Information**

With Dell Networking OS version 8.3.1.0 and later, the redistribute command can be used to advertise the IGP cost as the MED on redistributed routes. When the route-map is set with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-group will have IGP cost set as MED.

IS-IS to BGP redistribution supports matching of **level-1** or **level-2** routes or all routes (default). More advanced match options can be performed using route maps. The metric value of redistributed routes can be set by the redistribution command.

**Command History**

| Version 8.3.1.0 | Introduced ability to substitute IGP cost for MED when a peer/peer-group outbound route-map is set as internal. |
| Version 6.3.1.0 | Introduced |

**redistribute ospf**

Redistribute OSPF routes into BGP.

**Syntax**

```
redistribute ospf process-id [[match external {1 | 2}] [match internal]] [route-map map-name]
```

To stop redistribution of OSPF routes, use the **no redistribute ospf process-id** command.
Parameters

- **process-id**: Enter the number of the OSPF process.
  Range: 1 to 65535

- **match external {1 | 2}**: (OPTIONAL) Enter the keywords match external to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.

- **match internal**: (OPTIONAL) Enter the keywords match internal to redistribute OSPF internal routes only.

- **route-map map-name**: (OPTIONAL) Enter the keywords route-map followed by the name of a configured Route map.

Defaults

- Not configured.

Command Modes

- ROUTER BGP

Usage Information

With Dell Networking OS version 8.3.1.0 and later, the redistribute command can be used to advertise the IGP cost as the MED on redistributed routes. When the route-map is set with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-group will have IGP cost set as MED.

When you enter redistribute isis *process-id* command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. This feature is not supported by an RFC.

Command History

- Version 8.3.1.0 Introduced ability to substitute IGP cost for MED when a peer/peer-group outbound route-map is set as internal.
- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series

**router bgp**

```
router bgp as-number
```

Enter ROUTER BGP mode to configure and enable BGP.

Syntax

```
router bgp as-number
```

To disable BGP, use the **no router bgp as-number** command.

Parameters

- **as-number**: Enter the AS number.
  Range: 1 to 65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)

Defaults

- Not enabled.

Command Modes

- CONFIGURATION

Example

```
Figure 12-4. Command Example: router bgp

(conf)#router bgp 3
(conf-router_bgp)#
```
show capture bgp-pdu neighbor

**Display BGP packet capture information for an IPv4 address on the system.**

**Syntax**

```
show capture bgp-pdu neighbor ipv4-address
```

**Parameters**

- `ipv4-address`: Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.

**Command Modes**

EXEC Privilege

**Example**

```
(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 4098758, 26 packet(s) captured using 680 bytes
PDU[1] : len 101, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00650100 00000000 00000000
  00000000 419ef06c 00000000
  00000000 00000000 00000000 00000000 0181a1e4 0181a25c 41af92c0
  00000000 00000000 00000000
  00000000 00000000 0181a1e4 0181a25c 41af9400 00000000
PDU[2] : len 19, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00130400
PDU[3] : len 19, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00130400

[... ]
```

```
Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 4098758, 27 packet(s) captured using 562 bytes
PDU[1] : len 41, captured 00:34:52 ago
  ffffffff ffffffff ffffffff ffffffff 00290104 000100b4 14141401
  0c020a01 04000100 01020800
PDU[2] : len 19, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00130400
PDU[3] : len 19, captured 00:34:50 ago
  ffffffff ffffffff ffffffff ffffffff 00130400
```

```
#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture bgp-pdu max-buffer-size</code></td>
<td>Specify a size for the capture buffer.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

At least one interface must be in Layer 3 mode for the router bgp command to be accepted. If no interfaces are enabled for Layer 3, an error message appears: `% Error: No router id configured.`
show config

View the current ROUTER BGP configuration.

Syntax

`show config`

Command Modes

`ROUTER BGP`

Example

Figure 12-6. show config Command Example

```
(conf-router_bgp)#show config
!
router bgp 45
neighbor suzanne peer-group
neighbor suzanne no shutdown
neighbor sara peer-group
neighbor sara shutdown
neighbor 13.14.15.20 peer-group suzanne
neighbor 13.14.15.20 shutdown
neighbor 123.34.55.123 peer-group suzanne
neighbor 123.34.55.123 shutdown
(conf-router_bgp)#
```

Command History

```
Version 7.8.1.0 Introduced support on S-Series
Version 7.7.1.0 Introduced support on C-Series
```

show ip bgp

View the current BGP IPv4 routing table for the system.

Syntax

`show ip bgp [vrf vrf-name] [ipv4 unicast] [network [network-mask] [longer-prefixes]]`

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- `ipv4 unicast` (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to ipv4 unicast routes.
- `network` (OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
- `network-mask` (OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
- `longer-prefixes` (OPTIONAL) Enter the keyword `longer-prefixes` to view all routes with a common prefix.

Command Modes

`EXEC`

`EXEC Privilege`

Usage Information

When you enable `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.
Example Figure 12-7. show ip bgp Command Example (Partial)

```
>show ip bgp
BGP table version is 847562, local router ID is 63.114.8.131
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>* 3.0.0.0/8</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td></td>
<td>209 701 80 1</td>
</tr>
<tr>
<td>* 3.3.0.0/16</td>
<td>0.0.0.0</td>
<td>22</td>
<td>18508</td>
<td>701</td>
<td>80 i</td>
</tr>
<tr>
<td>* 4.0.0.0/8</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td></td>
<td>701 1 i</td>
</tr>
<tr>
<td>* 4.2.49.12/30</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>209</td>
<td>1 i</td>
</tr>
<tr>
<td>* 4.17.250.0/24</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>1239</td>
<td>13716 1</td>
</tr>
<tr>
<td>* 4.21.132.0/23</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>701</td>
<td>1239 13716 1</td>
</tr>
<tr>
<td>* 4.24.118.16/30</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>209</td>
<td>1 i</td>
</tr>
<tr>
<td>* 4.24.145.0/30</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>209</td>
<td>1 i</td>
</tr>
<tr>
<td>* 4.24.187.12/30</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>209</td>
<td>1 i</td>
</tr>
<tr>
<td>* 4.24.202.0/30</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>209</td>
<td>1 i</td>
</tr>
<tr>
<td>* 4.25.88.0/30</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td>209</td>
<td>3561 3908 1</td>
</tr>
<tr>
<td>* 5.0.0.0/9</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td></td>
<td>7 i</td>
</tr>
<tr>
<td>* 5.0.0.0/10</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td></td>
<td>7 i</td>
</tr>
<tr>
<td>* 5.0.0.0/11</td>
<td>63.114.8.33</td>
<td>0</td>
<td>18508</td>
<td></td>
<td>7 i</td>
</tr>
</tbody>
</table>
```

Table 12-1 defines the information displayed in Figure 12-7

Table 12-1. show ip bgp Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Related Commands

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

show ip bgp community
View BGP communities.

neighbor maximum-prefix
Control number of network prefixes received.
show ip bgp cluster-list

View BGP neighbors in a specific cluster.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 unicast] cluster-list [cluster-id]
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- `ipv4 unicast` (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to ipv4 unicast routes.
- `cluster-id` (OPTIONAL) Enter the cluster id in dotted decimal format.

**Command Modes**

EXEC

EXEC Privilege

**Example**

Figure 12-8. Command Example: show ip bgp cluster-list (Partial)

```
#show ip bgp cluster-list
BGP table version is 6444683, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* I 10.10.10.1/32</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>* I 10.19.75.5/32</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 10.30.1.0/24</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I</td>
<td>192.68.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>
```

Table 12-2 defines the information displayed in Figure 12-8.

**Table 12-2. show ip bgp cluster-list Command Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>
show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 unicast] community [community-number] [local-as] [no-export] [no-advertise]
```

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- `ipv4 unicast` (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to ipv4 unicast routes.
- `community-number` Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
- `local-AS` Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
- `no-advertise` Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
- `no-export` Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

EXEC

EXEC Privilege

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.
Example Figure 12-9. show ip bgp community Command Example (Partial)

>show ip bgp community
BGP table version is 3762622, local router ID is 63.114.8.48
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* i 3.0.0.0/8</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>701 80 i</td>
</tr>
<tr>
<td>* i 4.2.49.12/30</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>4622 i</td>
</tr>
<tr>
<td>* i 4.23.132.0/23</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>6462 i</td>
</tr>
<tr>
<td>* i 4.24.118.16/30</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>831 i</td>
</tr>
<tr>
<td>* i 4.24.145.0/30</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>31 i</td>
</tr>
<tr>
<td>* i 4.24.187.12/30</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>31 i</td>
</tr>
<tr>
<td>* i 4.24.202.0/30</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>31 i</td>
</tr>
<tr>
<td>* i 4.25.88.0/30</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>3561 3908 i</td>
</tr>
<tr>
<td>* i 6.1.0.0/16</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.2.0.0/22</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.3.0.0/18</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.4.0.0/16</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.5.0.0/19</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.6.0.0/20</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.9.0.0/20</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.10.0.015</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.14.0.0/15</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.13.0.0/21</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
<tr>
<td>* i 6.151.0.0/16</td>
<td>205.171.0.16</td>
<td>100</td>
<td>0</td>
<td>209</td>
<td>7170 1455 i</td>
</tr>
</tbody>
</table>

--More--

The show ip bgp community command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the show ip bgp command output.

Table 12-3. Command Example Fields: show ip bgp community

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

show ip bgp community-list

C E S

View routes that are affected by a specific community list.

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 unicast] community-list community-list-name [exact-match]
```
**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.</td>
</tr>
<tr>
<td>ipv4 unicast</td>
<td>(OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.</td>
</tr>
<tr>
<td>community-list-name</td>
<td>Enter the name of a configured IP community list. (max 16 chars)</td>
</tr>
<tr>
<td>exact-match</td>
<td>Enter the keyword for an exact match of the communities.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

EXEC Privilege

**Example**

*Figure 12-10. Command Example: show ip bgp community-list*

```bash
#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Path source: I = internal, a = aggregate, c = confed-external, r = redistributed, n = network
Origin codes: i = IGP, e = EGP, ? = incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
</table>
```

The `show ip bgp community-list` command without any parameters lists BGP routes matching the Community List and the output is the same as for the `show ip bgp` command output.

**Table 12-4. show ip bgp community-list Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**show ip bgp dampened-paths**

View BGP routes that are dampened (non-active).

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 unicast] dampened-paths
```

**Command Modes**

EXEC

EXEC Privilege
**Example**

Figure 12-11. Command Example: show ip bgp dampened-paths

>show ip bgp damp
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>From</th>
<th>Reuse</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 12-5 defines the information displayed in Figure 12-11.

**Table 12-5. show ip bgp dampened-paths Command Example**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the network ID to which the route is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>Displays the IP address of the neighbor advertising the dampened route.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Displays the hour:minutes:seconds until the dampened route is available.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the dampened route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**show ip bgp detail**

Display BGP internal information for IPv4 Unicast address family.

**Syntax**

```
show ip bgp [ipv4 unicast] detail
```

**Defaults**

none

**Command Modes**

EXEC

EXEC Privilege
**Example**

**Figure 12-12. Command Example: show ip bgp detail**

```
R2#show ip bgp detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTrMrP 0x41a17004 : NdKATmrP 0x41a17014 : NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfDid 0 : NdMedMissVal -1 :
NdIgmrIldId 0 : NdRRC2C 1 : NdClstdId 33686273 : NdPatTbP 0x41a19088
NdASPTrp1 0x41a19090 : NdCommTbP 0x41a19098 : NhOptTransTbP 0x41a190a0 :
NdRRClslTbP 0x41a190b8
NdPktFPA 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25800 :
NdTmpCommP 0x41a25800
NdTmpRRCIP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHNP : NdOrigPAP 0
NdOrgNHNP 0 : NdModPathP 0x41a4f6cc0 : NdModASPAP 0x41a4c000 : NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHNP : NdComSortBnP 0x41a19110 : NdComSortHdP 0x41a195d04 :
NdUpdHdP 0x41a195e4 : NdUpdHdP 0x41a1a3e9 :

NumNHDfDr 0 : CfgHdrAFMask 1
AFCNhNetTmPr 0x41ee705c : AFTrtDamp 0 : AlwaysCmpMed 0 : LocRld 10 : LocRmt 10 :
softReconfig 0x41a1a8c
DefNet 0 : AutoSumm 1 : NhpP 0x41a1d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : Fata 0 : ConnExp 0 : HldExp 0 : KeepExp 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 : TxNotifs 0
BadEvts 0 : SynFails 0 : RxWdCodeP 0x41a1b6d8 : RxWdCodeP 0x41a1b6e4
RxUpdCodeP 0x41a1a7b7 : TxEcodeP 0x41a1b734 : TxEcodeP 0x41a1b750 : TxEcodeP 0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEv 0 : LocPref 0 : tmplPathP 0x41a1b7b8 : LogNbrChgs 1
RecursiveHN 1 : PgCfgId 0 : KeepAlive 0 : HldrTime 0 : DioHdl 0 : AggrValTmPrp 0x41ee7024

UpdNetTmPr 0 : RedistTmPr 0x41ee7094 : PeerChgTmPr 0 : CleanRibTmPr 0x41ce7104
PeerUpdTmPr 0x41ee70cc : DfrdNHtMPr 0x41ee7174 : DfrdRtseTmPr 0x41ee713c :
FastExtFallover 1 : FastIntFallover 0 : EnforcementAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAPI 0 : TcpioCtxCB 0 : RedistBlk 1
NextCBFurg 0x1101119536 : NumPeerToPurge 0 : PeerRBGPcnt 0 : NonDet 0 : DfrdPathSel 0
BGFRst 0 : NumGrCfg 0 : DfrdTmestmp 0 : SnmpTrps 0 : IgrnBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 : MaceorExtInt 361
FixedFarStc 1 : VarFarStc 1
Packet Capture max allowed length 40960000 : current length 0

Peer Grp List
Nbr List
Confed Peer List
Address Family specific Information
AFIndex 0
NdSpFlag 0x41a190b0 : AFRtTp 0x41a1d200 : NdRTMMKp 0x41a19d28 : NdRTMAFBlVer 0 :
NdRbDctxAddr 1101110688
NdRbDctxAddrLen 255 : NdAFpPfx 0 : NdAFNLRIp 0 : NdAFNLRI Len 0 : NdAFNPrtp 0
NdAFWLen 0 : NdAFNH 0 : NdAFredRtTp 0x41a1d400 : NdRccCtxAd 1101110880
NdRedCtxAddrLen 255 : NdAFredWrkP 0x41a19e88 : AFAggRtt 0x41a1d600 : AFAggCtxAddr 1101110828
NdNumAggPfx 0 : AFAggAggSet 0 : AFAggSuppMap 0 : AFAggValdPfx 0 :
AFAggPathRttP 0x41a1d700
MpathCtxAddr 110111140 : MpathCtxAd 255 : AfEorSet 0x41a1b7f8 : NumDfrdFpx 0
AfActPeerHd 0x41a1a344 : AExtDist 1101112312 : AInfDist 200 : ALocDist 200
AfnNumRtc 0 : AfnRr 0 : AfnNetRttP 0x41a1d300 : AfnNetCtxAd 1101112392 :
AfnNetCtxAd 255
AfnWcCtxAd 1101112443 : AfnWcCtxAd 255 : AfnNetKBkDrRttP 0x41a1d500 :
AfnNetKBkDrCtn 0 : AfnDampHl 0 : AfnDampSupp 0 : AfnDampMaxHld 0 : AfnDampCeiling 0 :
AfnDampMapP

| Command History |
|-----------------|-----------------|-----------------|
| **Version 7.8.1.0** | Introduced support on S-Series |
| **Version 7.7.1.0** | Introduced support on C-Series |
| **Version 7.5.1.0** | Introduced |

---

378 | Border Gateway Protocol IPv4 (BGPv4)
show ip bgp extcommunity-list

View information on all routes with Extended Community attributes.

Syntax

show ip bgp [vrf vrf-name] [ipv4 unicast] extcommunity-list [list name]

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.
ipv4 unicast  (OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.
list name  Enter the extended community list name you wish to view.

Command Modes

EXEC
EXEC Privilege

Usage Information

To view the total number of COMMUNITY attributes found, use the show ip bgp summary command. The text line above the route table states the number of COMMUNITY attributes found.

The show ip bgp community command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the show ip bgp command output.

Command History

Version 8.4.6.0  Added support for VRF.
Version 7.8.1.0  Introduced support on S-Series
Version 7.7.1.0  Introduced support on C-Series

show ip bgp filter-list

View the routes that match the filter lists.

Syntax

show ip bgp [vrf vrf-name] [ipv4 unicast] filter-list as-path-name

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.
ipv4 unicast  (OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.
as-path-name  Enter the name of an AS-PATH.

Command Modes

EXEC
EXEC Privilege
Figure 12-13. Command Example: show ip bgp filter-list

```
#show ip bgp filter-list hello
BGP table version is 80227, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Path source codes: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* I 6.1.5.0/24</td>
<td>192.100.11.2</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.10.0/24</td>
<td>192.100.8.2</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.20.0/24</td>
<td>192.100.9.2</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.20.1</td>
<td>192.100.10.2</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.5.1</td>
<td>6.1.5.1</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.6.1</td>
<td>6.1.6.1</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.20.1</td>
<td>6.1.20.1</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.20.0/24</td>
<td>6.1.20.0/24</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.20.1</td>
<td>6.1.20.1</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>* I 6.1.20.0/24</td>
<td>6.1.20.0/24</td>
<td>20000</td>
<td>9999</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>
#```

Table 12-6 defines the information displayed in Figure 12-13.

**Table 12-6. Command Example fields: show ip bgp filter-list**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path source codes</td>
<td>Lists the path sources shown to the right of the last AS number in the Path column:</td>
</tr>
<tr>
<td></td>
<td>i = internal route entry</td>
</tr>
<tr>
<td></td>
<td>a = aggregate route entry</td>
</tr>
<tr>
<td></td>
<td>c = external confederation route entry</td>
</tr>
<tr>
<td></td>
<td>n = network route entry</td>
</tr>
<tr>
<td></td>
<td>r = redistributed route entry</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>
show ip bgp flap-statistics

View flap statistics on BGP routes.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 unicast] flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-expression]
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- `ipv4 unicast` (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to ipv4 unicast routes.
- `ip-address` (OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
- `mask` (OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
- `filter-list as-path-name` (OPTIONAL) Enter the keyword `filter-list` followed by the name of a configured AS-PATH ACL.
- `regexp regular-expression` Enter a regular expression then use one or a combination of the following characters to match:
  - `.` (period) any single character (including a white space)
  - `*` (asterisk) the sequences in a pattern (0 or more sequences)
  - `+` (plus) the sequences in a pattern (1 or more sequences)
  - `?` (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
  - `[ ]` (brackets) a range of single-character patterns.
  - `( )` (parenthesis) groups a series of pattern elements to a single element
  - `{ }` (braces) minimum and the maximum match count
  - `^` (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - `$` (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege

**Example**

**Figure 12-14. Command Example: show ip bgp flap-statistics**

```
> show ip bgp flap
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

>   Network     From     Flaps Duration Reuse   Path
```
Table 12-7 defines the information displayed in Figure 12-14.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the network ID to which the route is flapping.</td>
</tr>
<tr>
<td>From</td>
<td>Displays the IP address of the neighbor advertising the flapping route.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Displays the number of times the route flapped.</td>
</tr>
<tr>
<td>Duration</td>
<td>Displays the hours:minutes:seconds since the route first flapped.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Displays the hours:minutes:seconds until the flapped route is available.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the flapping route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Version 8.4.6.0 Added support for VRF.
Version 7.8.1.0 Introduced support on S-Series
Version 7.7.1.0 Introduced support on C-Series

show ip bgp inconsistent-as

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 unicast] inconsistent-as
```

Command Modes

EXEC

EXEC Privilege

Example

```
>show ip bgp inconsistent-as
BGP table version is 280892, local router ID is 10.1.2.100
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network       Next Hop       Metric LocPrf Weight Path
* 3.0.0.0/8    63.114.8.33   0 18508 209 7018 80 i
* 63.114.8.34   0 18508 209 7018 80 i
* 63.114.8.60   0 18508 209 7018 80 i
>* 63.114.8.33   0 18508 701 80  i
>* 3.18.135.0/24 63.114.8.60   0 18508 209 7018 80 i
* 63.114.8.34   0 18508 209 7018 80 i
* 63.114.8.33   0 18508 209 7018 80 i
>* 4.0.0.0/8     63.114.8.60   0 18508 209 1  i
* 63.114.8.34   0 18508 209 1  i
* 63.114.8.33   0 18508 209 1  i
* 6.0.0.0/20    63.114.8.60   0 18508 209 3549 1 i
* 63.114.8.34   0 18508 209 3549 1 i
>* 63.114.8.33   0 18508 209 3549 1 i
* 9.2.0.0/16    63.114.8.60   0 18508 209 701 i
* 63.114.8.34   0 18508 209 701 i
```

--More--
**Table 12-8. show ip bgp inconsistent-as Command Example Fields**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**show ip bgp neighbors**

Displays routing information exchanged by BGP neighbors.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 unicast] neighbors [ipv4-neighbor-addr | ipv6-neighbor-addr] [advertised-routes | dampened-routes | detail | flap-statistics | routes | received-routes [network network-mask] | denied-routes [network network-mask]]]
```

**Parameters**

- **vrf vrf-name**
  (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- **ipv4 unicast**
  (OPTIONAL) Enter the `ipv4 unicast` keywords to view information only related to IPv4 unicast routes.
- **ipv4-neighbor-addr**
  (OPTIONAL) Enter the IP address of the neighbor to view only BGP route information exchanged with that neighbor.
- **advertised-routes**
  (OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
- **dampened-routes**
  (OPTIONAL) Enter the keyword `dampened-routes` to view information on dampened routes from the BGP neighbor.
- **detail**
  (OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv4 Unicast address family.
- **flap-statistics**
  (OPTIONAL) Enter the keyword `flap-statistics` to view flap statistics on the neighbor’s routes.
- **routes**
  (OPTIONAL) Enter the keywords `routes` to view only the neighbor’s feasible routes.
Command Modes

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.6.0</td>
</tr>
<tr>
<td>Version 7.8.1.0</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
</tr>
<tr>
<td>Version 7.2.1.0</td>
</tr>
<tr>
<td>Version 6.3.10</td>
</tr>
</tbody>
</table>

Example 1

**Figure 12-16. Command Example: show ip bgp neighbors (Partial)**

```
#show ip bgp neighbors

BGP neighbor is 100.10.10.2, remote AS 200, external link
BGP version 4, remote router ID 192.168.2.101
BGP state ESTABLISHED, in this state for 00:16:12
Last read 00:00:12, last write 00:00:03
Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
  3 opens, 1 notifications, 1394 updates
  Sent 48 messages, 0 in queue
  3 opens, 2 notifications, 0 updates
  43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv4 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv4 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  ROUTE_REFRESH(2)
  GRACEFUL_RESTART(64)
  CISCO_ROUTE_REFRESH(128)

Route map for incoming advertisements is test
Maximum prefix set to 4 with threshold 75

For address family: IPv4 Unicast
BGP table version 34, neighbor version 34
5 accepted prefixes consume 20 bytes
Prefix advertised 0, denied 4, withdrawn 0

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer

Connections established 2; dropped 1
Last reset 00:18:21, due to Maximum prefix limit reached
```
Example 2  Figure 12-17.  Command Example: show ip bgp neighbors advertised-routes

```bash
>show ip bgp neighbors 192.14.1.5 advertised-routes

BGP table version is 74103, local router ID is 33.33.33.33
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed,
 n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*r 1.10.1.0/24</td>
<td>0.0.0.0</td>
<td>5000</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*r 1.11.0.0/16</td>
<td>0.0.0.0</td>
<td>5000</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*r 223.94.249.0/24</td>
<td>223.100.4.249</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>*r 223.94.250.0/24</td>
<td>223.100.4.250</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>*r 223.100.0.0/16</td>
<td>223.100.255.254</td>
<td>0</td>
<td>100</td>
<td>?</td>
<td></td>
</tr>
</tbody>
</table>
```

Total number of prefixes: 74102

Example 3  Figure 12-18.  Command Example: show ip bgp neighbors received-routes

```bash
#show ip bgp neighbors 100.10.10.2 received-routes

BGP table version is 13, local router ID is 120.10.10.1
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
 n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 70.70.21.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.22.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.23.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.24.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>*&gt; 70.70.25.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>*&gt; 70.70.26.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>*&gt; 70.70.27.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>*&gt; 70.70.28.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>*&gt; 70.70.29.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
</tbody>
</table>

```

Example 4  Figure 12-19.  Command Example: show ip bgp neighbors denied-routes

```bash
#show ip bgp neighbors 100.10.10.2 denied-routes
4 denied paths using 205 bytes of memory
BGP table version is 34, local router ID is 100.10.10.2
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
 n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 70.70.21.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.22.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.23.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>D 70.70.24.0/24</td>
<td>100.10.10.2</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>200</td>
</tr>
</tbody>
</table>
```

# Table 12-9. Command Example fields: show ip bgp neighbors

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version (always version 4) and the remote router ID.</td>
</tr>
</tbody>
</table>
### Table 12-9. Command Example fields: show ip bgp neighbors

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP state</td>
<td>Displays the neighbor’s BGP state and the amount of time in hours:minutes:seconds it has been in that state.</td>
</tr>
<tr>
<td>Last read</td>
<td>This line displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• last read is the time (hours:minutes:seconds) the router read a message from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• hold time is the number of seconds configured between messages from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.</td>
</tr>
<tr>
<td>Received messages</td>
<td>This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Sent messages</td>
<td>The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Received updates</td>
<td>This line displays the number of BGP updates received and sent.</td>
</tr>
<tr>
<td>Soft reconfiguration</td>
<td>This line indicates that soft reconfiguration inbound is configured.</td>
</tr>
<tr>
<td>Minimum time</td>
<td>Displays the minimum time, in seconds, between advertisements.</td>
</tr>
<tr>
<td>(list of inbound and outbound</td>
<td>Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.</td>
</tr>
<tr>
<td>policies)</td>
<td>For address family:</td>
</tr>
<tr>
<td></td>
<td>Displays IPv4 Unicast as the address family.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the which version of the primary BGP routing table the router and the neighbor are using.</td>
</tr>
<tr>
<td>accepted prefixes</td>
<td>Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.</td>
</tr>
<tr>
<td>Prefix advertised</td>
<td>Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session.</td>
</tr>
<tr>
<td></td>
<td>If the peering session was never reset, the word never is displayed.</td>
</tr>
<tr>
<td>Local host:</td>
<td>Displays the peering address of the local router and the TCP port number.</td>
</tr>
<tr>
<td>Foreign host:</td>
<td>Displays the peering address of the neighbor and the TCP port number.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show ip bgp` View the current BGP routing table.
**show ip bgp next-hop**

View all next hops (via learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

**Syntax**

```
show ip bgp next-hop
```

**Command Modes**

EXEC

EXEC Privilege

**Example**

```
Figure 12-20. Command Example: show ip bgp next-hop

>show ip bgp next-hop
Next-hop        Via                       RefCount  Cost  Flaps Time Elapsed
63.114.8.33     63.114.8.33, Gi 12/22       240984     0      0 00:18:25
63.114.8.34     63.114.8.34, Gi 12/22       135152     0      0 00:18:13
63.114.8.35     63.114.8.35, Gi 12/22            1       0      0 00:18:07
63.114.8.60     63.114.8.60, Gi 12/22       135155     0      0 00:18:11
>
```

**Table 12-10. Command Example fields: show ip bgp next-hop**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-hop</td>
<td>Displays the next-hop IP address.</td>
</tr>
<tr>
<td>Via</td>
<td>Displays the IP address and interface used to reach the next hop.</td>
</tr>
<tr>
<td>RefCount</td>
<td>Displays the number of BGP routes using this next hop.</td>
</tr>
<tr>
<td>Cost</td>
<td>Displays the cost associated with using this next hop.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Displays the number of times the next hop has flapped.</td>
</tr>
<tr>
<td>Time Elapsed</td>
<td>Displays the time elapsed since the next hop was learned. If the route is down, then this field displays time elapsed since the route went down.</td>
</tr>
</tbody>
</table>

**Command History**

- **Version 7.8.1.0** Introduced support on S-Series
- **Version 7.7.1.0** Introduced support on C-Series

**show ip bgp paths**

View all the BGP path attributes in the BGP database.

**Syntax**

```
show ip bgp [vrf vrf-name] paths [regexp regular-expression]
```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF. Range: 1 to 63.</td>
</tr>
<tr>
<td>regexp</td>
<td>Enter a regular expression then use one or a combination of the following characters to match: . = (period) any single character (including a white space) *= (asterisk) the sequences in a pattern (0 or more sequences) += (plus) the sequences in a pattern (1 or more sequences) ? = (question mark) sequences in a pattern (either 0 or 1 sequences). <strong>You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.</strong></td>
</tr>
<tr>
<td>regular-expression</td>
<td>[ ] = (brackets) a range of single-character patterns. () = (parenthesis) groups a series of pattern elements to a single element { } = (braces) minimum and the maximum match count ^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. $ = (dollar sign) the end of the output string.</td>
</tr>
</tbody>
</table>

Command Modes

- EXEC
- EXEC Privilege

Example

**Figure 12-21. Command Example: show ip bgp paths (Partial)**

```
#show ip bgp path
Total 16 Paths
Address Hash Refcount Metric Path
0x1efe?e5c 15 10000 32 ?
0x1efe?e1c 71 10000 23 ?
0x1efe?d9c 239 10000 42 ?
0x1efe?d9c 283 6 {102 103} ?
0x1efe?b1c 287 336 20000 ?
0x1efe?d1c 295 10000 13 ?
0x1efe?c5c 339 6 {92 93} ?
0x1efe?d6c 351 10000 12 ?
0x1efe?c1c 395 6 {82 83} ?
0x1efe?d6c 451 6 {72 73} ?
0x1efe?b5c 491 78 0 ?
0x1efe?adc 883 2 120 i
0x1efe?adr 983 10000 33 ?
0x1efe?b9c 1003 6 0 1
```

Table 12-11. Command Example fields: show ip bgp paths

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Displays the total number of BGP path attributes.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using this path attribute.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the MED attribute for this path attribute.</td>
</tr>
<tr>
<td>Path</td>
<td>Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.</td>
</tr>
</tbody>
</table>
show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

Syntax

show ip bgp [vrf vrf-name] paths as-path

Command Modes

EXEC

EXEC Privilege

Example

Figure 12-22. Command Example: show ip bgp paths as-path (Partial)

```
#show ip bgp paths as-path
Total 13 AS-Paths
Address Hash Refcount AS-Path
0x1ea3c1ec 251 1 42
0x1ea3c25c 251 1 22
0x1ea3c1b4 507 1 13
0x1ea3c304 507 1 33
0x1ea3c10c 763 1 {92 93}
0x1ea3c144 763 1 {102 103}
0x1ea3c17c 763 1 12
0x1ea3c2cc 763 1 32
0x1ea3c09c 764 1 {72 73}
0x1ea3c0d4 764 1 {82 83}
0x1ea3c224 1019 1 43
0x1ea3c294 1019 1 23
0x1ea3c02c 1021 4
```

Table 12-12. Command Example fields: show ip bgp paths community

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using these AS-Paths.</td>
</tr>
<tr>
<td>AS-Path</td>
<td>Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.</td>
</tr>
</tbody>
</table>

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

Syntax

show ip bgp [vrf vrf-name] paths community

Command History

<table>
<thead>
<tr>
<th>Version 8.4.6.0</th>
<th>Added support for VRF.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

Border Gateway Protocol IPv4 (BGPv4) | 389
Command Modes

EXEC
EXEC Privilege

Example

Figure 12-23. Command Example: show ip bgp paths community (Partial)

E1200-BGP>show ip bgp paths community
Total 293 Communities
Address Hash Refcount Community
0x1ec88a5c 3 4 209:209 209:6059 209:31272 390:8900 19092:300
0xe0f10ec 15 4 209:209 209:3039 209:31272 390:8900 19092:300
0x1c90233 37 2 209:209 209:7193 209:21362 390:8900 19092:300
0x1f588cd4 41 24 209:209 209:6253 209:21362 390:8900 19092:300
0x1e805884 46 2 209:209 209:21226 286:777 286:3033 1899:3033
64675:21092
0xe143f4c 46 8 209:209 209:5097 209:21362 390:8900 19092:300
0x1f173294 48 16 209:209 209:21226 286:40 286:777 286:3040 5606:40
12955:5606
0x1c9f8e24 50 6 209:209 209:4069 209:21362 390:8900 19092:300
0x1c9f8e4 53 4 209:209 209:3193 209:21362 390:8900 19092:300
0x1f58a944 57 6 209:209 209:2073 209:21362 390:8900 19092:300
0x1c6e2374 80 2 209:209 209:999 209:40832
0x1f58ad6c 57 6 209:209 209:41528
0x1c6e2064 83 2 209:777 209:40832
0x1f58a6cc 85 570 209:209 209:40832
0x1f57cc0c 98 2 209:209 209:21226 286:3031 13646:1044 13646:1124
13646:1234 13646:1244 13646:1254 13646:1264 13646:1300
0x1d65b2ac 117 6 209:209 209:31272
517:5104

Table 12-13. Command Example fields: show ip bgp paths community

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using these communities.</td>
</tr>
<tr>
<td>Community</td>
<td>Displays the community attributes in this BGP path.</td>
</tr>
</tbody>
</table>

Command History

Version 8.4.6.0  Added support for VRF.
Version 7.8.1.0  Introduced support on S-Series
Version 7.7.1.0  Introduced support on C-Series

show ip bgp peer-group

Enables you to view information on the BGP peers in a peer group.

Syntax

show ip bgp [vrf vrf-name] [ipv4 unicast] peer-group [peer-group-name [detail | summary]]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.</td>
</tr>
<tr>
<td>ipv4 unicast</td>
<td>(OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>(OPTIONAL) Enter the name of a peer group to view information about that peer group only.</td>
</tr>
</tbody>
</table>
**Example**

**Figure 12-24. Command Example: show ip bgp peer-group (Partial)**

```
#show ip bgp peer-group

Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
  12.1.1.2*
  12.1.1.3*
  12.1.1.4*
  12.1.1.5*
  12.1.1.6*
  12.2.1.2*
  12.2.1.3*
  12.2.1.4*
  12.2.1.5*
  12.2.1.6*
  12.3.1.2*
  12.3.1.3*
  12.3.1.4*
  12.3.1.5*
  12.3.1.6*
  12.4.1.2*
  12.4.1.3*
  12.4.1.4*
  12.4.1.5*
  12.4.1.6*
```

**Table 12-14. Command Example fields: show ip bgp peer-group**

<table>
<thead>
<tr>
<th>Line beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer-group</td>
<td>Displays the peer group’s name.</td>
</tr>
<tr>
<td>Administratively shut</td>
<td>Displays the peer group’s status if the peer group is not enabled.</td>
</tr>
<tr>
<td></td>
<td>If the peer group is enabled, this line is not displayed.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version supported.</td>
</tr>
<tr>
<td>Minimum time</td>
<td>Displays the time interval between BGP advertisements.</td>
</tr>
<tr>
<td>For address family</td>
<td>Displays IPv4 Unicast as the address family.</td>
</tr>
<tr>
<td>BGP neighbor</td>
<td>Displays the name of the BGP neighbor.</td>
</tr>
<tr>
<td>Number of peers</td>
<td>Displays the number of peers currently configured for this peer group.</td>
</tr>
<tr>
<td>Peer-group members:</td>
<td>Lists the IP addresses of the peers in the peer group.</td>
</tr>
<tr>
<td></td>
<td>If the address is outbound optimized, a * is displayed next to the IP address.</td>
</tr>
</tbody>
</table>
### show ip bgp regexp

Display the subset of BGP routing table matching the regular expressions specified.

**Syntax**

```plaintext
show ip bgp [vrf vrf-name] regexp regular-expression [character]
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- `regular-expression [character]` Enter a regular expression then use one or a combination of the following characters to match:
  - `.` (period) any single character (including a white space)
  - `*` (asterisk) the sequences in a pattern (0 or more sequences)
  - `+` (plus) the sequences in a pattern (1 or more sequences)
  - `?` (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
  - `[]` (brackets) a range of single-character patterns.
  - `()` (parenthesis) groups a series of pattern elements to a single element.
  - `{}` (braces) minimum and the maximum match count.
  - `^` (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - `$` (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege
Example Figure 12-25. Command Example: show ip bgp regexp (Partial)

#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*+I 3.0.0.0/8 1.1.1.2 0 100 0 2914 1239 80 i
*+I 4.0.0.0/8 1.1.1.2 0 100 0 2914 3356 i
*+I 4.17.225.0/24 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 6496
*+I 4.17.226.0/23 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 6496
*+I 4.17.251.0/24 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 6496
*+I 4.17.252.0/23 1.1.1.2 0 100 0 2914 11853 11853 11853 11853 11853 6496
*+I 4.19.2.0/23 1.1.1.2 0 100 0 2914 701 6167 6167 6167 6167 i
*+I 4.19.16.0/22 1.1.1.2 0 100 0 2914 174 4200 16559 i
*+I 4.21.80.0/22 1.1.1.2 0 100 0 2914 174 4200 16559 i
*+I 4.21.82.0/24 1.1.1.2 0 100 0 2914 174 4200 16559 i
*+I 4.21.252.0/23 1.1.1.2 0 100 0 2914 701 6389 19198 i
*+I 4.23.180.0/24 1.1.1.2 0 100 0 2914 3561 6128 30576 i
*+I 4.36.200.0/21 1.1.1.2 0 100 0 2914 14742 11854 14135 11854 14135 i
*+I 4.47.64.0/22 1.1.1.2 0 100 0 2914 11608 19281 i
*+I 4.78.32.0/21 1.1.1.2 0 100 0 2914 3491 29748 i
*+I 4.8.10.0/16 1.1.1.2 0 100 0 2914 701 668 i
*+I 6.2.0.0/22 1.1.1.2 0 100 0 2914 701 668 i
*+I 6.3.0.0/18 1.1.1.2 0 100 0 2914 701 668 i

Table 12-15. Command Example fields: show ip bgp regexp

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP router’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the AS paths the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Command History

Version 8.4.6.0 Added support for VRF.
Version 7.8.1.0 Introduced support on S-Series
Version 7.7.1.0 Introduced support on C-Series

show ip bgp summary

Enables you to view the status of all BGP connections.

Syntax

show ip bgp [vrf vrf-name] [ipv4 unicast] summary

Command Modes

EXEC
EXEC Privilege
### Table 12-16. Command Example fields: show ip bgp summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP router identifier</td>
<td>Displays the local router ID and the AS number.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the BGP table version and the main routing table version.</td>
</tr>
<tr>
<td>network entries</td>
<td>Displays the number of network entries and route paths and the amount of</td>
</tr>
<tr>
<td></td>
<td>memory used to process those entries.</td>
</tr>
<tr>
<td>paths</td>
<td>Displays the number of paths and the amount of memory used.</td>
</tr>
<tr>
<td>denied paths</td>
<td>Displays the number of denied paths and the amount of memory used.</td>
</tr>
<tr>
<td>BGP path attribute entries</td>
<td>Displays the number of BGP path attributes and the amount of memory used</td>
</tr>
<tr>
<td></td>
<td>to process them.</td>
</tr>
<tr>
<td>BGP AS-PATH entries</td>
<td>Displays the number of BGP AS-PATH attributes processed and the amount of</td>
</tr>
<tr>
<td></td>
<td>memory used to process them.</td>
</tr>
<tr>
<td>BGP community entries</td>
<td>Displays the number of BGP COMMUNITY attributes processed and the amount of</td>
</tr>
<tr>
<td></td>
<td>memory used to process them. The show ip bgp community</td>
</tr>
<tr>
<td></td>
<td>command provides more details on the COMMUNITY attributes.</td>
</tr>
<tr>
<td>Dampening enabled</td>
<td>Displayed only when dampening is enabled. Displays the number of paths</td>
</tr>
<tr>
<td></td>
<td>designated as history, dampened, or penalized.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Displays the BGP neighbor address.</td>
</tr>
<tr>
<td>AS</td>
<td>Displays the AS number of the neighbor.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Displays the number of BGP messages that neighbor received.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Displays the number of BGP messages that neighbor sent.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Displays the version of the BGP table that was sent to that neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Displays the number of messages from that neighbor waiting to be processed.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Displays the number of messages waiting to be sent to that neighbor.</td>
</tr>
<tr>
<td></td>
<td>If a number appears in parentheses, the number represents the number of</td>
</tr>
<tr>
<td></td>
<td>messages waiting to be sent to the peer group.</td>
</tr>
</tbody>
</table>
**show running-config bgp**

Use this feature to display the current BGP configuration.

**Syntax**

```
show running-config bgp
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**timers bgp**

Adjust BGP Keep Alive and Hold Time timers.

**Syntax**

```
timers bgp keepalive holdtime
```

To return to the default, enter `no timers bgp`.
MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). Dell Networking OS MBGP is implemented as per IETF RFC 1858.

Dell Networking OS version 7.8.1.0 and later support MBGP for IPv6 on E-Series and C-Series platforms.

Dell Networking OS version 7.8.1.0 and later supports MBGP for IPv4 Multicast only on the S-Series platform.

Dell Networking OS version 8.2.1.0 and later support MBGP on the E-Series ExaScale platform.

The MBGP commands are:

- address family ipv4 multicast (MBGP)
- aggregate-address
- bgp dampening
- bgp soft-reconfig-backup
- clear ip bgp dampening
- clear ip bgp flap-statistics
- clear ip bgp ipv4 multicast soft
- debug ip bgp dampening
- debug ip bgp dampening
- debug ip bgp peer-group updates
- debug ip bgp ipv4 unicast soft-reconfiguration
- debug ip bgp updates
- distance bgp
- neighbor activate

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **keepalive** | Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers.  
**Range:** 1 to 65535  
**Default:** 60 seconds |
| **holdtime** | Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead.  
**Range:** 3 to 65535  
**Default:** 180 seconds |

Defaults

No default values or behavior

Command Modes

- ROUTER BGP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>E-Series</td>
</tr>
</tbody>
</table>
• neighbor advertisement-interval
• neighbor default-originate
• neighbor distribute-list
• neighbor filter-list
• neighbor maximum-prefix
• neighbor next-hop-self
• neighbor remove-private-as
• neighbor route-map
• neighbor route-reflector-client
• neighbor soft-reconfiguration inbound
• network
• redistribute
• redistribute ospf
• show ip bgp ipv4 multicast
• show ip bgp cluster-list
• show ip bgp community
• show ip bgp community-list
• show ip bgp dampened-paths
• show ip bgp filter-list
• show ip bgp flap-statistics
• show ip bgp inconsistent-as
• show ip bgp ipv4 multicast
• show ip bgp ipv4 multicast neighbors
• show ip bgp peer-group
• show ip bgp summary

address family ipv4 multicast (MBGP)

This command changes the context to SAFI (Subsequent Address Family Identifier).

**Syntax**
address family ipv4 multicast

To remove SAFI context, use the no address family ipv4 multicast command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Enter the keyword ipv4 to specify the address family as IPV4.</td>
</tr>
<tr>
<td>multicast</td>
<td>Enter the keyword multicast to specify multicast as SAFI.</td>
</tr>
</tbody>
</table>

**Defaults**
IPv4 Unicast

**Command Modes**
ROUTER BGP (conf-router_bgp)

**Usage Information**
All subsequent commands will apply to this address family once this command is executed. You can exit from this AFI/SAFI to the IPv4 Unicast (the default) family by entering exit and returning to the Router BGP context.
aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

**Syntax**

```
aggregate-address ip-address mask [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]
```

**Parameters**

- `ip-address mask`:
  - Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in / prefix format (/x).

- `advertise-map map-name`:
  - (OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.

- `as-set`:
  - (OPTIONAL) Enter the keyword `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

- `attribute-map map-name`:
  - (OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.

- `summary-only`:
  - (OPTIONAL) Enter the keyword `summary-only` to advertise only the aggregate address. Specific routes will not be advertised.

- `suppress-map map-name`:
  - (OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP Address Family (conf-router_bgp_af)

**Usage Information**

- At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

- Do not add the `as-set` parameter to the aggregate. If routes within the aggregate are constantly changing, the aggregate will flap to keep track of the changes in the AS_PATH.

- In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppressed; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

- If the route is injected via the `network` command, that route will still appear in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

- The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.
**bgp dampening**

Enable MBGP route dampening.

**Syntax**

```
bgp dampening [half-life time] [route-map map-name]
```

To disable route dampening, use the **no bgp dampening [half-life time] [route-map map-name]** command.

**Parameters**

- **half-life time** (OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires.
  
  - Range: 1 to 45.
  - Default: 15 minutes

- **route-map map-name** (OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map.
  
  Only match commands in the configured route map are supported.

**Defaults**

Disabled.

**Command Modes**

ROUTER BGP Address Family (conf-router_bgp_af)

**Usage Information**

When soft-reconfiguration is enabled for a neighbor and the **clear ip bgp soft in** is executed, the update database stored in the router is replayed and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (upon execution of **clear ip bgp soft in**), then BGP sends a route-refresh request to the neighbor and receives all of the peer’s updates.

**Version 7.8.1.0** Introduced support on S-Series

**Version 7.7.1.0** Introduced support on C-Series

---

**bgp soft-reconfig-backup**

Use this command **only** when route-refresh is **not** negotiated between peers to avoid having a peer resend BGP updates.

**Syntax**

```
bgp soft-reconfig-backup
```

To return to the default setting, use the **no bgp soft-reconfig-backup** command.

**Defaults**

Off

**Command Modes**

ROUTER BGP ADDRESS FAMILY (conf-router_bgp_af)

**Usage Information**

When soft-reconfiguration is enabled for a neighbor and the **clear ip bgp soft in** is executed, the update database stored in the router is replayed and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (upon execution of **clear ip bgp soft in**), then BGP sends a route-refresh request to the neighbor and receives all of the peer’s updates.

**Version 7.8.1.0** Introduced support on S-Series

**Version 7.7.1.0** Introduced support on C-Series

**Version 7.6.1.0** Introduced IPv6 MGBP support for E-Series
clear ip bgp dampening

Clear information on route dampening.

test wrong

clear ip bgp dampening ipv4 multicast network network-mask

dampening

Enter the keyword dampening to clear route flap dampening information.

network

(Optional) Enter the network address in dotted decimal format (A.B.C.D).

network-mask

(Optional) Enter the network mask in slash prefix format (/x).

Command Modes

EXEC Privilege

Command History

Version 8.4.1.0 Added support for IPv4 multicast and IPv6 unicast address families
Version 7.8.1.0 Introduced support on S-Series
Version 7.7.1.0 Introduced support on C-Series
Version 7.2.1.0 Introduced

clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

clear ip bgp ipv4 multicast flap-statistics network | filter-list list | regexp regexp

Network

(Optional) Enter the network address to clear flap statistics in dotted decimal format (A.B.C.D).
**filter-list list**  
(Optional) Enter the keyword `filter-list` followed by the name of a configured AS-PATH list (max 16 characters).

**regexp regexp**  
(Optional) Enter the keyword `regexp` followed by regular expressions. Use one or a combination of the following:

- `*` = (period) any single character (including a white space)
- `*` = (asterisk) the sequences in a pattern (0 or more sequences)
- `*` = (plus) the sequences in a pattern (1 or more sequences)
- `*` = (question mark) sequences in a pattern (either 0 or 1 sequences). You must enter an escape sequence (CTRL+\+) prior to entering the ? regular expression.
- `[]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element
- `{}` = (braces) minimum and the maximum match count
- `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

**Command Modes**  
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

**clear ip bgp ipv4 multicast soft**  
Clear and reapply policies for IPv4 multicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

**Syntax**

```
clear ip bgp [* | as-number | ipv4-neighbor-addr | ipv6-neighbor-addr | peer-group name] ipv4 multicast soft [in | out]
```

**Parameters**

- `*`  
  Clear and reapply policies for all BGP sessions.

- `as-number`  
  Clear and reapply policies for all neighbors belonging to the AS.
  Range: 0-65535 (2-Byte) or 1-4294967295 (4-Byte) or 0.1-65535.65535 (Dotted format)

- `ipv4-neighbor-addr`  
  Clear and reapply policies for a neighbor.

- `ipv6-neighbor-addr`  
  Clear and reapply policies for a neighbor.

- `peer-group name`  
  Clear and reapply policies for all BGP routers in the specified peer group.

- `ipv4 multicast`  
  Clear and reapply policies for all IPv4 multicast routes.

- `in`  
  Reapply only inbound policies. **Note:** If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.

- `out`  
  Reapply only outbound policies. **Note:** If you enter `soft`, without an `in` or `out` option, both inbound and outbound policies are reset.

**Command Modes**  
EXEC Privilege
**debug ip bgp dampening**

View information on routes being dampened.

**Syntax**

```
debug ip bgp dampening
```

To disable debugging, enter `no debug ip bgp dampening`

**Parameters**

- `dampening`
  - Enter the keyword `dampening` to clear route flap dampening information.

**Command Modes**

- EXEC Privilege

**Command History**

- Version 8.4.1.0 Added BGP Soft Reconfiguration support for IPv4 unicast and IPv6 routes
- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series
- Version 7.2.1.0 Introduced

---

**debug ip bgp ipv4 multicast soft-reconfiguration**

Enable soft-reconfiguration debugging for IPv4 multicast routes.

**Syntax**

```
debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv4 multicast soft-reconfiguration
```

To disable debugging, use the `no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv4 multicast soft-reconfiguration` command.

**Parameters**

- `ipv4-address`
  - Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.

- `ipv6-address`
  - Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.

- `peer-group-name`
  - Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.

- `ipv4 multicast`
  - Debug soft reconfiguration for IPv4 multicast routes.

**Defaults**

Disabled

**Command Modes**

- EXEC Privilege

**Usage Information**

This command turns on BGP soft-reconfiguration inbound debugging for IPv4 multicast routes. If no neighbor is specified, debug is turned on for all neighbors.
debug ip bgp peer-group updates

View information about BGP peer-group updates.

ddebug ip bgp peer-group peer-group-name updates [in | out]

To disable debugging, enter no debug ip bgp peer-group peer-group-name updates [in | out] command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group</td>
<td>Enter the keyword peer-group followed by the name of the peer-group.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td></td>
</tr>
<tr>
<td>updates</td>
<td>Enter the keyword updates to view BGP update information.</td>
</tr>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword in to view only BGP updates received from neighbors.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword out to view only BGP updates sent to neighbors.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced support for IPv4 multicast and IPv6 unicast routes</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

debug ip bgp updates

View information about BGP updates.

ddebug ip bgp updates [in | out]

To disable debugging, enter no debug ip bgp updates [in | out] command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>updates</td>
<td>Enter the keyword updates to view BGP update information.</td>
</tr>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword in to view only BGP updates received from neighbors.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword out to view only BGP updates sent to neighbors.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Defaults

Disabled.
distance bgp

C E T S

Define an administrative distance for routes.

Syntax
distance bgp external-distance internal-distance local-distance

To return to default values, enter no distance bgp.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>external-distance</td>
<td>Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20</td>
<td></td>
</tr>
<tr>
<td>internal-distance</td>
<td>Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200</td>
<td></td>
</tr>
<tr>
<td>local-distance</td>
<td>Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200</td>
<td></td>
</tr>
</tbody>
</table>

Defaults

external-distance = 20; internal-distance = 200; local-distance = 200.

Command Modes

ROUTER BGP (conf-router_bgp_af)

Caution: Dell Force10 recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

Usage Information

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

neighbor activate

C E T S

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Syntax

neighbor [ip-address | peer-group-name] activate

To disable, use the no neighbor [ip-address | peer-group-name] activate command.
Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>(OPTIONAL) Enter the name of the peer group</td>
</tr>
<tr>
<td>activate</td>
<td>Enter the keyword activate to enable the neighbor/peer group in the new</td>
</tr>
<tr>
<td></td>
<td>AFI/SAFI.</td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information

By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv4/Unicast AFI/SAFI. By using activate in the new context, the neighbor/peer group is enabled for AFI/SAFI.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address family ipv4 multicast (MBGP)</td>
<td>Changes the context to SAFI</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax

neighbor {ip-address | peer-group-name} advertisement-interval seconds

to return to the default value, use the no neighbor {ip-address | peer-group-name} advertisement-interval command.

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group to set the advertisement interval for all routers in the peer group.</td>
</tr>
<tr>
<td>seconds</td>
<td>Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.</td>
</tr>
</tbody>
</table>

Defaults

seconds = 5 seconds (internal peers); seconds = 30 seconds (external peers)

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>
neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Syntax

```
neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
```

To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

Parameters

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to set the default route of all routers in that peer group.
- `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 BGP Address Family (conf-router_bgp_af)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

neighbor distribute-list

Distribute BGP information via an established prefix list.

Syntax

```
neighbor [ip-address | peer-group-name] distribute-list prefix-list-name [in | out]
```

To delete a neighbor distribution list, use the `no neighbor [ip-address | peer-group-name] distribute-list prefix-list-name [in | out]` command.

Parameters

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
- `prefix-list-name`: Enter the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).
- `in`: Enter the keyword `in` to distribute only inbound traffic.
- `out`: Enter the keyword `out` to distribute only outbound traffic.

Defaults

Not configured.

Command Modes

- ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information

Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

Related Commands

- `ip as-path access-list`: Configure IP AS-Path ACL.
neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

**Syntax**

neighbor [ip-address | peer-group-name] filter-list aspath access-list-name [in | out]

To delete a BGP filter, use the no neighbor [ip-address | peer-group-name] filter-list aspath access-list-name [in | out] command.

**Parameters**

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

- **peer-group-name**
  Enter the name of the peer group to apply the filter to all routers in the peer group.

- **access-list-name**
  Enter the name of an established AS-PATH access list (up to 140 characters).

  If the AS-PATH access list is not configured, the default is permit (to allow routes).

- **in**
  Enter the keyword in to filter inbound BGP routes.

- **out**
  Enter the keyword out to filter outbound BGP routes.

**Defaults**

Not configured.

**Command Modes**

- ROUTER BGP Address Family (conf-router_bgp_af)

**Usage Information**

Use the `ip as-path access-list` command syntax in the CONFIGURATION mode to enter the AS-PATH ACL mode and configure AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute.

**Related Commands**

- `ip as-path access-list` Enter AS-PATH ACL mode and configure AS-PATH filters.

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series
- Version 7.6.1.0 Introduced IPv6 MGBP support for E-Series
neighbor maximum-prefix

Control the number of network prefixes received.

Syntax

```
neighbor ip-address | peer-group-name maximum-prefix maximum [threshold] [warning-only]
```

To return to the default values, use the `no neighbor ip-address | peer-group-name maximum-prefix maximum` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>(OPTIONAL) Enter the name of the peer group.</td>
</tr>
<tr>
<td><code>maximum</code></td>
<td>Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.</td>
</tr>
<tr>
<td><code>threshold</code></td>
<td>(OPTIONAL) Enter a number to be used as a percentage of the <code>maximum</code> value. When the number of prefixes reaches this percentage of the <code>maximum</code> value, Dell Networking OS sends a message. Range: 1 to 100 percent. Default: 75</td>
</tr>
<tr>
<td><code>warning-only</code></td>
<td>(OPTIONAL) Enter the keyword <code>warning-only</code> to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.</td>
</tr>
</tbody>
</table>

Defaults

`threshold` = 75

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced</td>
<td>Support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced</td>
<td>Support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced</td>
<td>IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

neighbor next-hop-self

Enables you to configure the router as the next hop for a BGP neighbor.

Syntax

```
neighbor ip-address | peer-group-name next-hop-self
```

To return to the default setting, use the `no neighbor ip-address | peer-group-name next-hop-self` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>(OPTIONAL) Enter the name of the peer group.</td>
</tr>
</tbody>
</table>

Defaults

Disabled.

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information

If the `set next-hop` command in the ROUTE-MAP mode is configured, its configuration takes precedence over the `neighbor next-hop-self` command.
**neighbor remove-private-as**

Remove private AS numbers from the AS-PATH of outgoing updates.

**Syntax**

```
neighbor ip-address | peer-group-name remove-private-as
```

To return to the default, use the `no neighbor ip-address | peer-group-name remove-private-as` command.

**Parameters**

- `ip-address` (OPTIONAL) Enter the IP address of the neighbor to remove the private AS numbers.
- `peer-group-name` (OPTIONAL) Enter the name of the peer group to remove the private AS numbers.

**Defaults**

Disabled (that is, private AS number are not removed).

**Command Modes**

ROUTER BGP Address Family (conf-router_bgp_af)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

**neighbor route-map**

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

**Syntax**

```
neighbor [ip-address | peer-group-name] route-map map-name [in | out]
```

To remove the route map, use the `no neighbor [ip-address | peer-group-name] route-map map-name [in | out]` command.

**Parameters**

- `ip-address` (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` (OPTIONAL) Enter the name of the peer group.
- `map-name` Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).
- `in` Enter the keyword `in` to filter inbound routes.
- `out` Enter the keyword `out` to filter outbound routes.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP Address Family (conf-router_bgp_af)
Usage Information
When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

Command History

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

Syntax
neighbor ip-address | peer-group-name route-reflector-client

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the no neighbor ip-address | peer-group-name route-reflector-client command.

Parameters

| ip-address | (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format. |
| peer-group-name | (OPTIONAL) Enter the name of the peer group. All routers in the peer group receive routes from a route reflector. |

Defaults
Not configured.

Command Modes
ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information
The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

Command History

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv4 multicast routes.

Syntax
neighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound
network

Specify the networks for the BGP process and enter them in the BGP routing table.

**Syntax**

```
network ip-address mask [route-map map-name]
```

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

**Parameters**

<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 of the network.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).</td>
</tr>
<tr>
<td>route-map</td>
<td>(OPTIONAL) Enter the keyword <strong>route-map</strong> followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported:</td>
</tr>
<tr>
<td>map-name</td>
<td>• match ip address</td>
</tr>
<tr>
<td></td>
<td>• set community</td>
</tr>
<tr>
<td></td>
<td>• set local-preference</td>
</tr>
<tr>
<td></td>
<td>• set metric</td>
</tr>
<tr>
<td></td>
<td>• set next-hop</td>
</tr>
<tr>
<td></td>
<td>• set origin</td>
</tr>
<tr>
<td></td>
<td>• set weight</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.
Command Modes
ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information
Dell Networking OS resolves the network address configured by the network command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

Related Commands
redistribute Redistribute routes into BGP.

Command History
Version 7.8.1.0 Introduced support on S-Series
Version 7.7.1.0 Introduced support on C-Series
Version 7.6.1.0 Introduced IPv6 MGBP support for E-Series

redistribute
Redistribute routes into BGP.

Syntax
redistribute [connected | static] [route-map map-name]

To disable redistribution, use the no redistribution [connected | static] [route-map map-name] command.

Parameters
- **connected**: Enter the keyword connected to redistribute routes from physically connected interfaces.
- **static**: Enter the keyword static to redistribute manually configured routes. These routes are treated as incomplete routes.
- **route-map map-name**: (OPTIONAL) Enter the keyword route-map followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported:
  - match ip address
  - set community
  - set local-preference
  - set metric
  - set next-hop
  - set origin
  - set weight

If the route map is not configured, the default is deny (to drop all routes).

Defaults
Not configured.

Command Modes
ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information
If you do not configure default-metric command, in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0.0.0.0/0) configure the neighbor default-originate command.

Related Commands
neighbor default-originate Inject the default route.
**Command History**

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

**redistribute ospf**

Redistribute OSPF routes into BGP.

**Syntax**

```plaintext
redistribute ospf process-id [[match external {1 | 2}] [match internal]] [route-map map-name]
```

To stop redistribution of OSPF routes, use the `no redistribute ospf process-id` command.

**Parameters**

- `process-id` Enter the number of the OSPF process. Range: 1 to 65535
- `match external {1 | 2}` (OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
- `match internal` (OPTIONAL) Enter the keywords `match internal` to redistribute OSPF internal routes only.
- `route-map map-name` (OPTIONAL) Enter the keywords `route-map` followed by the name of a configured Route map.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP Address Family (conf-router_bgp_af)

**Usage Information**

When you enter `redistribute ospf process-id` command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

This feature is not supported by an RFC.

**Command History**

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced support on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

**show ip bgp cluster-list**

View BGP neighbors in a specific cluster.

**Syntax**

```plaintext
show ip bgp ipv4 multicast cluster-list [cluster-id]
```

**Parameters**

- `cluster-id` (OPTIONAL) Enter the cluster id in dotted decimal format.

**Command Modes**

EXEC

EXEC Privilege
show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

**Syntax**

```
show ip bgp ipv4 multicast community [community-number] [local-as] [no-export] [no-advertise]
```

**Parameters**

- `community-number` Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.

- `local-AS` Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.

- `no-advertise` Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.

- `no-export` Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

**Command Modes**

- EXEC
- EXEC Privilege

**Usage Information**

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series
- Version 7.6.1.0 Introduced IPv6 MGBP support for E-Series

show ip bgp community-list

View routes that are affected by a specific community list.

**Syntax**

```
show ip bgp ipv4 multicast community-list community-list-name
```
Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community-list-name</td>
<td>Enter the name of a configured IP community list.</td>
</tr>
</tbody>
</table>

Command Modes

<table>
<thead>
<tr>
<th>mode</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>version</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
</tbody>
</table>

**show ip bgp dampened-paths**

View BGP routes that are dampened (non-active).

Syntax

```
show ip bgpipv4 multicast dampened-paths
```

Command Modes

<table>
<thead>
<tr>
<th>mode</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>version</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

**show ip bgp filter-list**

View the routes that match the filter lists.

Syntax

```
show ip bgpipv4 multicast filter-listas-path-name
```

Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-path-name</td>
<td>Enter the name of an AS-PATH.</td>
</tr>
</tbody>
</table>

Command Modes

<table>
<thead>
<tr>
<th>mode</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>version</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>

**show ip bgp flap-statistics**

View flap statistics on BGP routes.

Syntax

```
show ip bgpipv4 multicast flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexpregular-expression]
```

Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter the IP mask.</td>
</tr>
<tr>
<td>filter-list</td>
<td>Enter the name of a configured IP community list.</td>
</tr>
<tr>
<td>as-path-name</td>
<td>Enter the name of an AS-PATH.</td>
</tr>
<tr>
<td>regexp regular-expression</td>
<td>Enter the regular expression for the route.</td>
</tr>
</tbody>
</table>
**show ip bgp inconsistent-as**

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

**Syntax**

```
show ip bgp ipv4 multicast inconsistent-as
```

**Parameters**

- `ip-address` (OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
- `mask` (OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
- `filter-list as-path-name` (OPTIONAL) Enter the keyword `filter-list` followed by the name of a configured AS-PATH ACL.
- `regexp regular-expression` Enter a regular expression then use one or a combination of the following characters to match:
  - `.` (period) any single character (including a white space)
  - `*` (asterisk) the sequences in a pattern (0 or more sequences)
  - `+` (plus) the sequences in a pattern (1 or more sequences)
  - `?` (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+^) prior to entering the ? regular expression.**
  - `[]` (brackets) a range of single-character patterns.
  - `( )` (parenthesis) groups a series of pattern elements to a single element
  - `{ }` (braces) minimum and the maximum match count
  - `^` (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - `$` (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series
- Version 7.6.1.0 Introduced IPv6 MGBP support for E-Series
**show ip bgp ipv4 multicast**

View the current MBGP routing table for the system.

**Syntax**

```
show ip bgp ipv4 multicast [detail | network [network-mask] [length]]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(OPTIONAL) Enter the keyword <code>detail</code> to display BGP internal information for the IPv4 Multicast address family.</td>
</tr>
<tr>
<td>network</td>
<td>(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.</td>
</tr>
<tr>
<td>network-mask</td>
<td>(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.</td>
</tr>
<tr>
<td>longer-prefixes</td>
<td>(OPTIONAL) Enter the keyword <code>longer-prefixes</code> to view all routes with a common prefix.</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege

**Example**

```
#show ip bgp ipv4 multicast
BGP table version is 14, local router ID is 100.10.10.1
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network            Next Hop            Metric     LocPrf Weight Path
*>I 25.1.0.0/16     25.25.25.25              0        100      0 i
*>I 25.2.0.0/16     25.25.25.26              0        100      0 ?
*>I 25.3.0.0/16     211.1.1.165              0        100      0 ?
*>r 144.1.0.0/16    0.0.0.0                  0             32768 ?
*>r 144.2.0.0/16    100.10.10.10             0             32768 ?
*>r 144.3.0.0/16    211.1.1.135              0             32768 ?
*>n 145.1.0.0/16    0.0.0.0                  0             32768 i
#
```

**Table 12-17. show ip bgp Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show ip bgp community` View BGP communities.

**Command History**

- Version 7.8.1.0 Introduced support on S-Series
- Version 7.7.1.0 Introduced support on C-Series
show ip bgp ipv4 multicast neighbors

Displays information on IPv4 multicast routes exchanged by BGP neighbors.

Syntax

show ip bgp ipv4 multicast neighbors [ipv4-neighbor-addr | ipv6-neighbor-addr] [advertised-routes | dampened-routes | detail | flap-statistics | routes | received-routes [network [network-mask]]] [denied-routes [network [network-mask]]]

Parameters

ipv4 multicast

Enter the ipv4 multicast keywords to view information only related to IPv4 multicast routes.

ipv4-neighbor-addr | ipv6-neighbor-addr

(OPTIONAL) Enter the IP address of the neighbor to view only BGP route information exchanged with that neighbor.

advertised-routes

(OPTIONAL) Enter the keywords advertised-routes to view only the routes the neighbor sent.

dampened-routes

(OPTIONAL) Enter the keyword dampened-routes to view information on dampened routes from the BGP neighbor.

detail

(OPTIONAL) Enter the keyword detail to view neighbor-specific internal information for the IPv4 Unicast address family.

flap-statistics

(OPTIONAL) Enter the keyword flap-statistics to view flap statistics on the neighbor’s routes.

routes

(OPTIONAL) Enter the keywords routes to view only the neighbor’s feasible routes.

received-routes [network [network-mask]]

(OPTIONAL) Enter the keywords received-routes followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. Note: neighbor soft-reconfiguration inbound must be configured prior to viewing all the information received from the neighbors.

Version 8.4.1.0 Added support for the display of configured IPv4 multicast address families

Version 7.8.1.0 Introduced support on S-Series

Version 7.7.1.0 Introduced support on C-Series

Version 7.5.1.0 Added detail option and output now displays default MED value

Version 7.2.1.0 Added received and denied route options

Version 6.3.10 The output is changed to display the total number of advertised prefixes
Figure 12-28. Command Example: show ip bgp ipv4 multicast neighbors

```
#show ip bgp ipv4 multicast neighbors

BGP neighbor is 25.25.25.25, remote AS 6400, internal link
BGP version 4, remote router ID 25.25.25.25
BGP state ESTABLISHED, in this state for 00:02:18
Last read 00:00:16, hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
3 opens, 1 notifications, 1394 updates
6 keepalives, 0 route refresh requests
Sent 48 messages, 0 in queue
3 opens, 2 notifications, 0 updates
43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 5 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv4 unicast:
MULTIPROTO_EXT(1)
ROUTE_REFRESH(2)
CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv4 Multicast:
MULTIPROTO_EXT(1)
ROUTE_REFRESH(2)
CISCO_ROUTE_REFRESH(128)

Update source set to Loopback 0
For address family: IPv4 Multicast
BGP table version 14, neighbor version 14
3 accepted prefixes consume 12 bytes

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 2; dropped 1
Last reset 00:03:17, due to user reset

Notification History
'Connection Reset' Sent : 1 Recv: 0

Local host: 100.10.10.1, Local port: 179
Foreign host: 25.25.25.25, Foreign port: 2290

BGP neighbor is 211.1.1.129, remote AS 640, external link
BGP version 4, remote router ID 0.0.0.0
BGP state ACTIVE, in this state for 00:00:36
Last read 00:00:41, hold time is 180, keepalive interval is 60 seconds
Received 28 messages, 0 notifications, 0 in queue
Sent 6 messages, 3 notifications, 0 in queue
Received 18 updates, Sent 6 updates
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Multicast
BGP table version 14, neighbor version 0
0 accepted prefixes consume 0 bytes
Prefix advertised 0, rejected 0, withdrawn 0

Connections established 3; dropped 3
Last reset 00:00:37, due to user reset

Notification History
'Connection Reset' Sent : 3 Recv: 0
```

Table 12-18. Command Example fields: show ip bgp ipv4 multicast neighbors

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version (always version 4) and the remote router ID.</td>
</tr>
<tr>
<td>Lines beginning with</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>BGP state</td>
<td>Displays the neighbor’s BGP state and the amount of time in hours:minutes:seconds it has been in that state.</td>
</tr>
</tbody>
</table>
| Last read            | This line displays the following information:  
  • last read is the time (hours:minutes:seconds) the router read a message from its neighbor  
  • hold time is the number of seconds configured between messages from its neighbor  
  • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive. |
| Received messages    | This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing. |
| Sent messages        | The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing. |
| Received updates     | This line displays the number of BGP updates received and sent. |
| Soft reconfiguration | This line indicates that soft reconfiguration inbound is configured. |
| Minimum time         | Displays the minimum time, in seconds, between advertisements. |
| (List of inbound and outbound policies) | Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy. |
| For address family:  | Displays IPv4 Multicast as the address family. |
| BGP table version    | Displays the which version of the primary BGP routing table the router and the neighbor are using. |
| Prefixes accepted    | Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes. |
| Prefixes advertised  | Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table. |
| Connections established | Displays the number of TCP connections established and dropped between the two peers to exchange BGP information. |
| Last reset           | Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed. |
| Local host:          | Displays the peering address of the local router and the TCP port number. |
| Foreign host:        | Displays the peering address of the neighbor and the TCP port number. |

**Related Commands**

show ip bgp peer-group  
Enables you to view information on the BGP peers in a peer group.

**Syntax**

```
show ip bgp ipv4 multicast peer-group [peer-group-name [detail | summary]]
```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>(OPTIONAL) Enter the name of a peer group to view information about that peer group only.</td>
</tr>
<tr>
<td>detail</td>
<td>(OPTIONAL) Enter the keyword detail to view detailed status information of the peers in that peer group.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword summary to view status information of the peers in that peer group. The output is the same as that found in show ip bgp summary command</td>
</tr>
</tbody>
</table>

Command Modes

- EXEC
- EXEC Privilege

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor peer-group (assigning peers)</td>
<td>Assign peer to a peer-group.</td>
</tr>
<tr>
<td>neighbor peer-group (creating group)</td>
<td>Create a peer group.</td>
</tr>
<tr>
<td>show ip bgp peer-group</td>
<td>View information on the BGP peers in a peer group.</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Modified: added detail option</td>
</tr>
</tbody>
</table>

show ip bgp summary

Enables you to view the status of all BGP connections.

Syntax

show ip bgp ipv4 multicast summary

Command Modes

- EXEC
- EXEC Privilege

Example

**Figure 12-29. Command Example: show ip bgp ipv4 multicast summary**

```
#sho ip bgp ipv4 multicast summary
BGP router identifier 100.10.10.1, local AS number 6400
BGP table version is 14, main routing table version 14
7 network entrie(s) and 7 paths using 972 bytes of memory
2 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 35 bytes of memory

 Neighbor        AS     MsgRcvd  MsgSent     TblVer  InQ  OutQ Up/Down  State/Pfx
25.25.25.25     6400        21        9         14    0     0 00:02:04         3
211.11.1.129     640 28       6          0    0     0 00:00:21 Active
```

Table 12-19. Command Example fields: show ip bgp ipv4 multicast summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP router identifier</td>
<td>Displays the local router ID and the AS number.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the BGP table version and the main routing table version.</td>
</tr>
</tbody>
</table>
Table 12-19. Command Example fields: show ip bgp ipv4 multicast summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network entries</td>
<td>Displays the number of network entries and route paths and the amount of memory used to process those entries.</td>
</tr>
<tr>
<td>BGP path attribute entries</td>
<td>Displays the number of BGP path attributes and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP AS-PATH entries</td>
<td>Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP community entries</td>
<td>Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The show ip bgp community command provides more details on the COMMUNITY attributes.</td>
</tr>
<tr>
<td>Dampening enabled</td>
<td>Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Displays the BGP neighbor address.</td>
</tr>
<tr>
<td>AS</td>
<td>Displays the AS number of the neighbor.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Displays the number of BGP messages that neighbor received.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Displays the number of BGP messages that neighbor sent.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Displays the version of the BGP table that was sent to that neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Displays the number of messages from that neighbor waiting to be processed.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Displays the number of messages waiting to be sent to that neighbor.</td>
</tr>
<tr>
<td></td>
<td>If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage.</td>
</tr>
<tr>
<td></td>
<td>If the neighbor has never moved into the Established stage, the word never is displayed.</td>
</tr>
<tr>
<td>State/Pfx</td>
<td>If the neighbor is in Established stage, the number of network prefixes received.</td>
</tr>
<tr>
<td></td>
<td>If a maximum limit was configured with the neighbor maximum-prefix command, (prfxd) appears in this column.</td>
</tr>
<tr>
<td></td>
<td>If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm) When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column.</td>
</tr>
<tr>
<td></td>
<td>If the neighbor is disabled, the phrase (Admin shut) appears in this column.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for the display of configured IPv4 multicast address families</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for E-Series</td>
</tr>
</tbody>
</table>
BGP Extended Communities (RFC 4360)

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute. It provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new “Type” field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

The BGP Extended Community commands are:

- deny
- deny regex
- description
- ip extcommunity-list
- match extcommunity
- permit
- permit regex
- set extcommunity rt
- set extcommunity soo
- show ip bgp ipv4 extcommunity-list
- show ip bgp paths extcommunity
- show ip extcommunity-list
- show running-config extcommunity-list

**deny**

Use this feature to reject (deny) from the two types of extended communities, Route Origin (rt) or Site-of-Origin (soo).

**Syntax**

deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}

To remove (delete) the rule, use the no deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN} command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>rt</strong></td>
<td>Enter the keyword <em>rt</em> to designate a Route Origin community</td>
</tr>
<tr>
<td><strong>soo</strong></td>
<td>Enter the keyword <em>soo</em> to designate a Site-of-Origin community (also known as Route Origin).</td>
</tr>
<tr>
<td><strong>as4 ASN4:NN</strong></td>
<td>Enter the keyword <em>as4</em> followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-Byte AS number:2-Byte community value).</td>
</tr>
<tr>
<td><strong>ASN:NNNN</strong></td>
<td>Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-Byte AS number:4-Byte community value).</td>
</tr>
<tr>
<td><strong>IPADDR:NN</strong></td>
<td>Enter the IP address specific extended community in the format IPADDR:NN (4-Byte IPv4 Unicast Address:2-Byte community value).</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured

**Command Modes**

CONFIGURATION (conf-ext-community-list)
**deny regex**

This feature enables you to specify an extended communities to reject (deny) using a regular expressions (regex).

**Syntax**

```plaintext
deny regex {regex}
```

To remove, use the `no deny regex {regex}` command.

**Parameters**

- **regex**: Enter a regular expression.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION (conf-ext-community-list)

**Usage Information**

Duplicate commands are silently accepted.

**Example**

```plaintext
Figure 12-30. Commands Example: deny regexp
```

```plaintext
(conf-ext-community-list)#deny regexp 123
(conf-ext-community-list)#
```

**Related Commands**

- **permit**: Configure to add (permit) rules
- **show ip extcommunity-list**: Display the Extended Community list

**Command History**

- **Version 7.8.1.0**: Introduced on S-Series
- **Version 7.7.1.0**: Introduced on C-Series
- **Version 7.6.1.0**: Introduced on E-Series

**description**

Use this feature to designate a meaningful description to the extended community.

**Syntax**

```plaintext
description {line}
```

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

**Parameters**

- **line**: Enter a description (maximum 80 characters).

**Defaults**

Not configured
ip extcommunity-list

Use this feature to enter the Extended Community-list mode.

**Syntax**
```
ip extcommunity-list word
```

To exit from this mode, use the `exit` command.

**Parameters**
- `word`: Enter a community list name (maximum 16 characters).

**Defaults**
No defaults values or behavior

**Command Modes**
CONFIGURATION (conf-ext-community-list)

**Usage Information**
This new mode will change the prompt. See the example below.

**Example**

```
(config)#ip extcommunity-list test
(config-ext-community-list)#
```

**Command History**
- Version 7.8.1.0 Introduced on S-Series
- Version 7.7.1.0 Introduced on C-Series
- Version 7.6.1.0 Introduced on E-Series

**match extcommunity**

Use this feature to match an extended community in the Route Map mode.

**Syntax**
```
match extcommunity {extended community list name}
```

To change the match, use the `no match extcommunity {extended community list name}` command.

**Parameters**
- `extended community list name`: Enter the name of the extended community list.

**Defaults**
No defaults values or behavior

**Command Modes**
ROUTE MAP (config-route-map)

**Usage Information**
Like standard communities, extended communities can be used in route-map to match the attribute.
permit

Use this feature to add rules (permit) from the two types of extended communities, Route Origin (rt) or Site-of-Origin (soo).

Syntax

`permit \{rt \| soo\} \{as4 ASN4:NN | ASN:NNNN | IPADDR:NN\}`

To change the rules, use the `no permit \{rt \| soo\} \{as4 ASN4:NN | ASN:NNNN | IPADDR:NN\}` command.

Parameters

- **rt**: Enter the keyword `rt` to designate a Route Origin community.
- **soo**: Enter the keyword `soo` to designate a Site-of-Origin community (also known as Route Origin).
- **as4 ASN4:NN**: Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-Byte AS number:2-Byte community value).
- **ASN:NNNN**: Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-Byte AS number:4-Byte community value).
- **IPADDR:NN**: Enter the IP address specific extended community in the format IPADDR:NN (4-Byte IPv4 Unicast Address:2-Byte community value).

Default

Not Configured

Command Modes

`CONFIGURATION (conf-ext-community-list)`

Related Commands

- `deny`: Configure to delete (deny) rules
- `show ip extcommunity-list`: Display the Extended Community list

Command History

- **Version 7.8.1.0**: Introduced on S-Series
- **Version 7.7.1.0**: Introduced on C-Series
- **Version 7.6.1.0**: Introduced on E-Series

permit regex

This feature enables you specify an extended communities to forward (permit) using a regular expressions (regex).

Syntax

`permit regex \{regex\}`

To remove, use the `no permit regex \{regex\}` command.
Parameters

**regex**
Enter a regular expression.

Defaults
Not configured

Command Modes
CONFIGURATION (conf-ext-community-list)

Usage
Duplicate commands are silently accepted.

Example
**Figure 12-33. Command Example: permit regexp**

```plaintext
(conf-ext-community-list)#permit regexp 123
(conf-ext-community-list)#
```

Related Commands

- **deny regexp**
  Deny a community using a regular expression

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**set extcommunity rt**

Use this feature to set Route Origin community attributes in Route Map.

Syntax

```
set extcommunity rt |as4 ASN4:NN [non-trans] | ASN:NNNN [non-trans] | IPADDR:NN [non-trans] | [additive]
```

To delete the Route Origin community, use the **no set extcommunity** command.

Parameters

- **as4 ASN4:NN**
Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-Byte AS number:2-Byte community value).

- **ASN:NNNN**
Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-Byte AS number:4-Byte community value).

- **IPADDR:NN**
Enter the IP address specific extended community in the format IPADDR:NN (4-Byte IPv4 Unicast Address:2-Byte community value).

- **additive**
  (OPTIONAL) Enter the keyword `additive` to add to the existing extended community.

- **non-trans**
  (OPTIONAL) Enter the keyword `non-trans` to indicate a non-transitive BGP extended community.

Defaults
No default values or behavior

Command Modes
ROUTE MAP (config-route-map)

Usage
If the set community `rt` and `soo` are in the same route-map entry, we can define the behavior as:

- If `rt` option comes before `soo`, with or without `additive` option, then `soo` overrides the communities set by `rt`
set extcommunity soo

Use this feature to set extended community site-of-origin in Route Map.

Syntax

```
set extcommunity soo {as4 ASN4:NN | ASN:NNNN | IPADDR:NN [non-trans]}
```

To delete the site-of-origin community, use the `no set extcommunity` command.

Parameters

- **as4 ASN4:NN**: Enter the keyword `as4` followed by the 4-octet AS specific extended community number in the format ASN4:NN (4-Byte AS number:2-Byte community value).
- **ASN:NNNN**: Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-Byte AS number:4-Byte community value).
- **IPADDR:NN**: Enter the IP address specific extended community in the format IPADDR:NN (4-Byte IPv4 Unicast Address:2-Byte community value)
- **non-trans**: (OPTIONAL) Enter the keyword `non-trans` to indicate a non-transitive BGP extended community.

Defaults

No default behavior or values

Command Modes

ROUTE MAP (config-route-map)

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, we can define the behavior as:

- If `rt` option comes before `soo`, with or without `additive` option, then `soo` overrides the communities set by `rt`
- If `rt` options comes after `soo`, without the `additive` option, then `rt` overrides the communities set by `soo`
- If `rt` with `additive` option comes after `soo`, then `rt` adds the communities set by `soo`

Related Commands

```
set extcommunity rt
```

Set extended community route origins via the route-map

Command History

- Version 7.8.1.0: Introduced on S-Series
- Version 7.7.1.0: Introduced on C-Series
- Version 7.6.1.0: Introduced on E-Series
**show ip bgp ipv4 extcommunity-list**

Use this feature to display IPv4 routes matching the extended community list name.

**Syntax**

```
show ip bgp [ipv4 [multicast | unicast] | ipv6 unicast] extcommunity-list name
```

**Parameters**

- **multicast** Enter the keyword `multicast` to display the multicast route information.
- **unicast** Enter the keyword `unicast` to display the unicast route information.
- **ipv6 unicast** Enter the keywords `ipv6 unicast` to display the IPv6 unicast route information.
- **name** (OPTIONALLY) Enter the name of the extcommunity-list.

**Defaults**

No default values or behavior

**Command Modes**

- EXEC
- EXEC Privilege

**Usage Information**

If there is a type or sub-type that is not well-known, it will be displayed as:

```
TTSS:XX:YYYY
```

Where TT is type, SS is sub-type displayed in hexadecimal format, XX:YYYY is the value divided into 2-Byte and 4-Byte values in decimal format. This format is consistent with other vendors.

For example, if the extended community has type 0x04, sub-type 0x05, value 0x20 00 00 00 10 00, it will be displayed as:

```
0x0405:8192:4096
```

Non-transitive extended communities are marked with an asterisk, as shown in the figure below.

**Example**

```
#show ip bgp ipv4 multicast extcommunity-list
BGP routing table entry for 192.168.1.0/24, version 2
Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer
Received from :
  100.100.1.2  (2.4.0.1)    Best
    AS_PATH :  200
    Next-Hop : 100.100.1.2, Cost : 0
    Origin IGP, Metric  4294967295 (Default), LocalPref 100, Weight 0,
    external
    Communities :
      300:400
      500:600
    Extended Communities :
      SoO:38:50529045 SoO:0.0.0.2:33 SoO:506.62106:34 0x0303:254:11223*
#
```

**Command History**

- **Version 7.8.1.0** Introduced on S-Series
- **Version 7.7.1.0** Introduced on C-Series
- **Version 7.6.1.0** Introduced on E-Series
show ip bgp paths extcommunity

Use this feature to display all BGP paths having extended community attributes.

Syntax

show ip bgp paths extcommunity

Command Modes

EXEC

EXEC Privilege

Example

Figure 12-35. Command Example: show ip bgp paths community (Partial)

#show ip bgp paths extcommunity
Total 1 Extended Communities

<table>
<thead>
<tr>
<th>Address</th>
<th>Hash</th>
<th>Refcount</th>
<th>Extended Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x41d57024</td>
<td>12272</td>
<td>1</td>
<td>RT:7:200 SoO:5:300 SoO:0.0.0.3:1285</td>
</tr>
</tbody>
</table>

Table 12-20. Command Example fields: show ip bgp paths community

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using these extended communities.</td>
</tr>
<tr>
<td>Community</td>
<td>Displays the extended community attributes in this BGP path.</td>
</tr>
</tbody>
</table>

Command History

- Version 7.8.1.0 Introduced on S-Series
- Version 7.7.1.0 Introduced on C-Series
- Version 7.6.1.0 Introduced on E-Series

show ip extcommunity-list

Display the IP extended community list.

Syntax

show ip extcommunity-list [word]

Parameters

word Enter the name of the extended community list you want to view.

Defaults

Defaults.

Command Modes

EXEC

EXEC Privilege
**Example**

Figure 12-36. Command Example: show ip extcommunity-list

```
#show ip extcommunity-list test
ip extcommunity-list test
deny RT:1234:12
permit regexp 123
deny regexp 234
deny regexp 123
#
```

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**show running-config extcommunity-list**

Use this feature to display the current configuration of the extended community lists.

**Syntax**

```
show running-config extcommunity-list [word]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>word</td>
<td>Enter the name of the extended community list you want to view.</td>
</tr>
</tbody>
</table>

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Example**

Figure 12-37. Command Example: show running-config extcommunity-list

```
#show running-config extcommunity-list test
ip extcommunity-list test
 permit rt 65033:200
 deny soo 101.11.11.2:23
 permit rt as4 110212:340
 deny regex '^((65001_)&' 
#
```

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
Content Addressable Memory (CAM)

Overview

Content Addressable Memory (CAM) commands are supported C-Series, E-Series TeraScale and S-Series, as indicated by the symbols under each command heading: C E T S

This chapter includes information relating to the E-Series TeraScale platform. Refer to Chapter 13, Content Addressable Memory (CAM) for ExaScale for information on the commands for the E-Series ExaScale platform.

Note: Not all CAM commands are supported on all platforms. Be sure to note the platform symbol when looking for a command.

Warning: If you are using these features for the first time, contact the Dell Networking Technical Assistance Center (TAC) for guidance. For information on contacting Dell Networking TAC, visit the Dell Networking website at www.force10networks.com/support

This chapter includes the following sections:

- CAM Profile Commands
- CAM IPv4flow Commands
- CAM Layer 2 ACL Commands

CAM Profile Commands

The CAM profiling feature enables you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 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 ACLs (when IPv6 is not employed).
- Hash MPLS packets based on source and destination IP addresses for LAGs.
- Hash based on bidirectional flow for LAGs.
- Optimize the VLAN ACL Group feature, which permits group VLANs for IP egress ACLs.
Important Points to Remember

- CAM Profiles are available on Dell Networking OS versions 6.3.1.1 and later for the E-Series TeraScale. Refer to Chapter 13, Content Addressable Memory (CAM) for ExaScale for information on the commands for the E-Series ExaScale platform.
- Dell Networking OS versions 7.8.1.0 and later support CAM allocations on the C-Series and S-Series.
- All line cards within a single system must have the same CAM profile (including CAM sub-region configurations); this profile must match the system CAM profile (the profile on the primary RPM).
- Dell Networking OS automatically reconfigures the CAM profile on line cards and the secondary RPM to match the system CAM profile by saving the correct profile on the card and then rebooting it.
- 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 QoS configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, TCP and UDP rules with port range options might require more than one CAM entry.
- After you install a secondary RPM, copy the running-configuration to the startup-configuration so that the new RPM has the correct CAM profile.
- 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-acl (EXEC Privilege)
- cam-optimization
- cam-profile (Config)
- show cam-acl
- show cam-profile
- show cam-usage
- test cam-usage
cam-acl (Configuration)
Allocate CAM for IPv4 and IPv6 ACLs

Syntax
```
cam-acl {default | l2acl number ipv4acl number ipv6acl number, ipv4qos number l2qos number, l2pt number imac acl number ecfmacl number [vman-qos | vman-dual-qos number] [vrfv4acl number]}
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Use the default CAM profile settings, and set the CAM as follows.</td>
</tr>
<tr>
<td>l2acl number</td>
<td>Allocate space to each CAM region.</td>
</tr>
<tr>
<td>ipv4acl number</td>
<td>Enter the CAM profile name followed by the amount to be allotted.</td>
</tr>
<tr>
<td>ipv6acl number</td>
<td>The total space allocated must equal 13.</td>
</tr>
<tr>
<td>ipv4qos number</td>
<td>The ipv6acl range must be a factor of 2.</td>
</tr>
<tr>
<td>l2qos number</td>
<td>Allocate space to each CAM region.</td>
</tr>
<tr>
<td>l2pt number</td>
<td>Enter the CAM profile name followed by the amount to be allotted.</td>
</tr>
<tr>
<td>imac acl number</td>
<td>The total space allocated must equal 13.</td>
</tr>
<tr>
<td>ecfmacl number</td>
<td>The ipv6acl range must be a factor of 2.</td>
</tr>
<tr>
<td>vman-qos</td>
<td>Allocate space to each CAM region.</td>
</tr>
<tr>
<td>vman-dual-qos</td>
<td>Enter the CAM profile name followed by the amount to be allotted.</td>
</tr>
<tr>
<td>vrfv4acl number</td>
<td>The total space allocated must equal 13.</td>
</tr>
</tbody>
</table>

Command Modes

- `CONFIGURATION`

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added <code>ecfmacl</code>, <code>vman-qos</code>, and <code>vman-dual-qos</code> keywords.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
</tbody>
</table>

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 3 blocks and these cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

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 2 (2, 4, 6, 8, 10).
cam-acl (EXEC Privilege)

Adjust line card CAM setting to match chassis settings.

This command is deprecated as of Dell Networking OS 8.3.1.0

Syntax

```plaintext
cam-acl {chassis | linecard}
```

Command Modes

```
EXEC Privilege
```

Command History

```
<table>
<thead>
<tr>
<th>Version 8.3.1.0</th>
<th>COMMAND DEPRECATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
</tbody>
</table>
```

cam-optimization

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

Syntax

```plaintext
cam-optimization [qos]
```

Parameters

```
| qos                      | Optimize CAM usage for Quality of Service (QoS) |
```

Command Modes

```
CONFIGURATION
```

Defaults

```
Disabled
```

Command History

```
<table>
<thead>
<tr>
<th>Version 8.2.1.0</th>
<th>Introduced on the s-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on the C-Series and S-Series</td>
</tr>
</tbody>
</table>
```

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 1 FP entry will be used).

Note that an ACL itself may still require more that a single FP entry, regardless of the number of interfaces. Refer to IP Access Control Lists, Prefix Lists, and Route-map in the Dell Networking OS Configuration Guide for complete discussion.
cam-profile (Config)

Set the default CAM profile and the required microcode.

**Syntax**

```
cam-profile profile microcode microcode
```

**Parameters**

- **profile** Choose one of the following CAM profiles:
  - Enter the keyword `default` to specify the default CAM profile.
  - Enter the keyword `eg-default` to specify the default CAM profile for EG (dual-CAM) line cards.
  - Enter the keyword `ipv4-320k` to specify the CAM profile that provides 320K entries for the IPv4 Forwarding Information Base (FIB).
  - Enter the keyword `ipv4-egacl-16k` to specify the CAM profile that provides 16K entries for egress ACLs.
  - Enter the keyword `ipv6-extacl` to specify the CAM profile that provides IPv6 functionality.
  - Enter the keyword `l2-ipv4-inacil` to specify the CAM profile that provides 32K entries for ingress ACLs.
  - Enter the keyword `unified-default` to specify the CAM profile that maintains the CAM allocations for the IPv6 and IPv4 FIB while allocating more CAM space for the Ingress and Egress Layer 2 ACL, and IPv4 ACL regions.
  - Enter the keyword `ipv4-vrf` to specify the CAM profile that maintains the CAM allocations for the IPv4 FIB while allocating CAM space for VRF.
  - Enter the keyword `ipv4-v6-vrf` to specify the CAM profile that maintains the CAM allocations for the IPv4 and IPv6 FIB while allocating CAM space for VRF.
  - Enter the keyword `ipv4-64k-ipv6` to specify the CAM profile that provides an alternate to ipv6-extacl that redistributes CAM space from the IPv4 FIB to IPv4Flow and IPv6FIB.

- **microcode** Choose a microcode based on the CAM profile you chose. Not all microcodes are available to be paired with a CAM profile.
  - Enter the keyword `default` to select the microcode that distributes CAM space for a typical deployment.
  - Enter the keyword `lag-hash-align` to select the microcode for applications that require the same hashing for bi-directional traffic.
  - Enter the keyword `lag-hash-mpls` to select the microcode for hashing based on MPLS labels (up to five labels deep).
  - Enter the keyword `ipv6-extacl` to select the microcode for IPv6.
  - Enter the keyword `acl-group` to select the microcode for applications that need 16k egress IPv4 ACLs.
  - Enter the keyword `ipv4-vrf` to select the microcode for IPv4 VRF applications.
  - Enter the keyword `ipv4-v6-vrf` to select the microcode for IPv4 and IPv6 VRF applications.
  - E-Series TeraScale only: Select `l2-switched-pbr` microcode if you apply a PBR redirect list to a VLAN interface and want to prevent Layer 2 traffic from being redirected and dropped. `l2-switched-pbr` (IPv4-LDA) microcode allows only Layer 3 traffic to be redirected while Layer 2 traffic is switched within the VLAN.

**Defaults**

- `cam-profile default microcode default`

**Command Modes**

- `CONFIGURATION`
You must save the running configuration using the command `copy running-config startup-config` after changing the CAM profile from CONFIGURATION mode. CAM profile changes take effect after the next chassis reboot.

⚠️ **Note:** Do not use the ipv4-egacl-16 CAM profile for Layer 2 egress ACLs.

⚠️ **Note:** Do not make any changes to the CAM profile after you change the profile to ipv4-320K and save the configuration until after you reload the chassis; any changes lead to unexpected behavior. After you reload the chassis, you may make changes to the IPv4 Flow partition.

### show cam-acl

Display the details of the CAM profiles on the chassis and all line cards.

**Syntax**

```
show cam-acl
```

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The display reflects the settings implemented with the `cam-acl` command.
show cam-profile

Display the details of the CAM profiles on the chassis and all line cards.

Syntax

```
show cam-profile [profile microcode microcode | summary]
```
### Parameters

<table>
<thead>
<tr>
<th>profile</th>
<th>(OPTIONAL) Choose a single CAM profile to display:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enter the keyword <strong>default</strong> to specify the default CAM profile.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>eg-default</strong> to specify the default CAM profile for EG (dual-CAM) line cards.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv4-320k</strong> to specify the CAM profile that provides 320K entries for the IPv4 Forwarding Information Base (FIB).</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv4-egacl-16k</strong> to specify the CAM profile that provides 16K entries for egress ACLs.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv6-extacl</strong> to specify the CAM profile that provides IPv6 functionality.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>l2-ipv4-inacl</strong> to specify the CAM profile that provides 32K entries for ingress ACLs.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>unified-default</strong> to specify the CAM profile that maintains the CAM allocations for the IPv6 and IPv4 FIB while allocating more CAM space for the Ingress and Egress Layer 2 ACL, and IPv4 ACL regions.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv4-vrf</strong> to specify the CAM profile that maintains the CAM allocations for the IPv4 FIB while allocating CAM space for VRF.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv4-v6-vrf</strong> to specify the CAM profile that maintains the CAM allocations for the IPv4 and IPv6FIB while allocating CAM space for VRF.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>microcode</th>
<th>Choose the microcode to display. Not all microcodes are available to be paired with a CAM profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enter the keyword <strong>default</strong> to select the microcode that distributes CAM space for a typical deployment.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>lag-hash-align</strong> to select the microcode for applications that require the same hashing for bi-directional traffic.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>lag-hash-mpls</strong> to select the microcode for hashing based on MPLS labels (up to five labels deep).</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv6-extacl</strong> to select the microcode for IPv6.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>acl-group</strong> to select the microcode for applications that need 16k egress IPv4 ACLs.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv4-vrf</strong> to select the microcode for IPv4 VRF applications.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv4-v6-vrf</strong> to select the microcode forIPv4 and IPv6 VRF applications.</td>
<td></td>
</tr>
<tr>
<td>• Enter the keyword <strong>ipv4-64k-ipv6</strong> to specify the CAM profile that provides an alternate to ipv6-extacl that redistributes CAM space from the IPv4FIB to IPv4Flow and IPv6FIB.</td>
<td></td>
</tr>
</tbody>
</table>

| summary | (OPTIONAL) Enter this keyword to view a summary listing of the CAM profile and microcode on the chassis and all line cards. |

### Defaults

None

### Command Modes

EXEC Privilege

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for <strong>(optional)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td><strong>ipv4-64k-ipv6</strong> profile</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Added support for VRF protocols.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

If the CAM profile has been changed, this command displays the current CAM profile setting in one column and in the other column displays the CAM profile and the microcode that will be configured for the chassis and all online line cards *after the next reboot.*
Example 1  Figure 13-3. Command Output: show cam-profile summary

FTOS#show cam-profile summary
-- Chassis CAM Profile --
  Profile Name : Default          : Default
  MicroCode Name : Default          : Default
-- Line card 1 --
  Profile Name : Default          : Default
  MicroCode Name : Default          : Default
-- Line card 6 --
  Profile Name : Default          : Default
  MicroCode Name : Default          : Default
FTOS#

Example 2  Figure 13-4. Command Output: show cam-profile

FTOS#show cam-profile
-- Chassis Cam Profile --
  CamSize          : 18-Meg
  Profile Name     : DEFAULT          : DEFAULT
  L2FIB            : 32K entries      : 32K entries
  L2ACL            : 1K entries       : 1K entries
  IPv4FIB          : 256K entries     : 256K entries
  IPv4ACL          : 1K entries       : 1K entries
  IPv4Flow         : 24K entries      : 24K entries
  EgIPv4ACL        : 1K entries       : 1K entries
  IPv6FIB          : 0 entries       : 0 entries
  IPv6ACL          : 0 entries       : 0 entries
  IPv6Flow         : 0 entries       : 0 entries
  EgIPv6ACL        : 0 entries       : 0 entries
  MicroCode Name   : Default          : Default
-- Line card 0 --
  CamSize          : 18-Meg
  Profile Name     : DEFAULT          : DEFAULT
  L2FIB            : 32K entries      : 32K entries
  L2ACL            : 1K entries       : 1K entries
  IPv4FIB          : 256K entries     : 256K entries
  IPv4ACL          : 1K entries       : 1K entries
  IPv4Flow         : 24K entries      : 24K entries
  EgIPv4ACL        : 1K entries       : 1K entries
  IPv6FIB          : 0 entries       : 0 entries
  IPv6ACL          : 0 entries       : 0 entries
  IPv6Flow         : 0 entries       : 0 entries
  EgIPv6ACL        : 0 entries       : 0 entries
  MicroCode Name   : Default          : Default
FTOS#

show cam-usage

Display Layer 2, Layer 3, ACL, or all CAM usage statistics.

Syntax  show cam-usage [acl | router | switch]
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>(OPTIONAL) Enter this keyword to display Layer 2 and Layer 3 ACL CAM usage.</td>
</tr>
<tr>
<td>router</td>
<td>(OPTIONAL) Enter this keyword to display Layer 3 CAM usage.</td>
</tr>
<tr>
<td>switch</td>
<td>(OPTIONAL) Enter this keyword to display Layer 2 CAM usage.</td>
</tr>
</tbody>
</table>

### Defaults

None

### Command Modes

EXEC Privilege

### Command History

Version 6.5.1.0 Introduced on E-Series

### Example

**Figure 13-5. Command Example: show cam-usage**

```plaintext
FTOS#show cam-usage
Linecard|Portpipe| CAM Partition   | Total CAM | Used CAM | Available CAM
-------|--------|=================|-----------|----------|----------------
 1   | 0      | IN-L2 ACL       | 1008      | 320      | 688            |
    |        | IN-L2 FIB       | 32768     | 1132     | 31636         |
    |        | IN-L3 ACL       | 12288     | 2        | 12286         |
    |        | IN-L3 FIB       | 262141    | 14       | 262127        |
    |        | IN-L3-SysFlow   | 2878      | 45       | 2833          |
    |        | IN-L3-TrcList   | 1024      | 0        | 1024          |
    |        | IN-L3-McastFib  | 9215      | 0        | 9215          |
    |        | IN-L3-Qos       | 8192      | 0        | 8192          |
    |        | IN-L3-PBR       | 1024      | 0        | 1024          |
    |        | IN-V6 ACL       | 0         | 0        | 0             |
    |        | IN-V6 FIB       | 0         | 0        | 0             |
    |        | IN-V6-SysFlow   | 0         | 0        | 0             |
    |        | IN-V6-McastFib  | 0         | 0        | 0             |
    |        | OUT-L2 ACL      | 1024      | 0        | 1024          |
    |        | OUT-L3 ACL      | 1024      | 0        | 1024          |
    |        | OUT-V6 ACL      | 0         | 0        | 0             |
 1   | 1      | IN-L2 ACL       | 320       | 0        | 320            |
    |        | IN-L2 FIB       | 32768     | 1136     | 31632         |
    |        | IN-L3 ACL       | 12288     | 2        | 12286         |
    |        | IN-L3 FIB       | 262141    | 14       | 262127        |
    |        | IN-L3-SysFlow   | 2878      | 44       | 2834          |
```

--More--

**Figure 13-6. Command Example: show cam-usage acl**

```plaintext
FTOS#show cam-usage acl
Linecard|Portpipe| CAM Partition   | Total CAM | Used CAM | Available CAM
-------|--------|=================|-----------|----------|----------------
 11   | 0      | IN-L2 ACL       | 1008      | 0        | 1008          |
    |        | IN-L3 ACL       | 12288     | 2        | 12286         |
    |        | OUT-L2 ACL      | 1024      | 0        | 1024          |
    |        | OUT-L3 ACL      | 1024      | 0        | 1024          |
FTOS#
```
Example Figure 13-7. Command Example: show cam-usage router

```
FTOS#show cam-usage router

Linecard|Portpipe| CAM Partition   | Total CAM | Used CAM | Available CAM
---------|--------|-----------------|-----------|----------|----------------
  11     |   0    | IN-L3 ACL       | 8192      | 3        | 8189
  |        | IN-L3 FIB       | 196607    | 1        | 196606
  |        | IN-L3-SysFlow   | 2878      | 0        | 2878
  |        | IN-L3-TrcList   | 1024      | 0        | 1024
  |        | IN-L3-McastFib  | 9215      | 0        | 9215
  |        | IN-L3-Qos       | 8192      | 0        | 8192
  |        | IN-L3-PBR       | 1024      | 0        | 1024
  |        | OUT-L3 ACL      | 16384     | 0        | 16384

FTOS#
```

Example Figure 13-8. Command Example: show cam-usage switch

```
FTOS#show cam-usage switch

Linecard|Portpipe| CAM Partition   | Total CAM | Used CAM | Available CAM
---------|--------|-----------------|-----------|----------|----------------
  11     |   0    | IN-L2 ACL       | 7152      | 0        | 7152
  |        | IN-L2 FIB       | 32768     | 1081     | 31687
  |        | OUT-L2 ACL      | 0         | 0        | 0

FTOS#
```

test cam-usage

```
C E S
```

Verify that enough CAM space is available for the IPv6 ACLs you have created.

**Syntax**

```
test cam-usage service-policy input input policy name linecard {number | all}
```

**Parameters**

- **policy-map name**
  - Enter the name of the policy-map to verify.
- **number**
  - Enter `all` to get information for all the linecards/stack-units, or enter the linecard/stack-unit `number` to get information for a specific card.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

- **Version 7.8.1.0** Introduced

**Usage Information**

This command applies to both IPv4 and IPv6 CAM Profiles, but is best used when verifying QoS optimization for IPv6 ACLs.
QoS Optimization for IPv6 ACLs does not impact the CAM usage for applying a policy on a single (or the first of several) interfaces. It is most useful when a policy is applied across multiple interfaces; it can reduce the impact to CAM usage across subsequent interfaces.

**Example**

The following examples show some sample output when using the `test cam-usage` command.

**Figure 13-9. Command Example: test cam-usage (C-Series)**

```plaintext
FTOS#test cam-usage service-policy input LauraMapTest linecard all
Linecard | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port | Status
---------------------------------------------------------------
  2 |        1 | IPv4Flow      |           232 |                      0 | Allowed
  2 |        1 | IPv6Flow      |             0 |                      0 | Allowed
  4 |        0 | IPv4Flow      |           232 |                      0 | Allowed
  4 |        0 | IPv6Flow      |             0 |                      0 | Allowed
FTOS#
```

```plaintext
FTOS#test cam-usage service-policy input LauraMapTest linecard 4 port-set 0
Linecard | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port | Status
---------------------------------------------------------------
  4 |        0 | IPv4Flow      |           232 |                      0 | Allowed
  4 |        0 | IPv6Flow      |             0 |                      0 | Allowed
FTOS#
```

```plaintext
FTOS#test cam-usage service-policy input LauraMapTest linecard 2 port-set 1
Linecard | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port | Status
---------------------------------------------------------------
  2 |        1 | IPv4Flow      |           232 |                      0 | Allowed
  2 |        1 | IPv6Flow      |             0 |                      0 | Allowed
FTOS#
```

**Table 13-1. Output Explanations: test cam-usage (C-Series)**

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linecard</td>
<td>Lists the line card or linecards that are checked. Entering <strong>all</strong> shows</td>
</tr>
<tr>
<td></td>
<td>the status for linecards in the chassis</td>
</tr>
<tr>
<td>Portpipe</td>
<td>Lists the portpipe (port-set) or port pipes (port-sets) that are checked.</td>
</tr>
<tr>
<td></td>
<td>Entering <strong>all</strong> shows the status for linecards and port-pipes in the</td>
</tr>
<tr>
<td></td>
<td>chassis.</td>
</tr>
<tr>
<td>CAM Partition</td>
<td>Shows the CAM profile of the CAM</td>
</tr>
<tr>
<td>Available CAM</td>
<td>Identifies the amount of CAM space remaining for that profile</td>
</tr>
<tr>
<td>Estimated CAM per Port</td>
<td>Estimates the amount of CAM space the listed policy will require.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether or not the policy will be allowed in the CAM</td>
</tr>
</tbody>
</table>
CAM IPv4flow Commands

IPv4Flow sub-partitions are supported on E-Series TeraScale platform.

The 18-megabit user configurable CAM is divided into multiple regions such as Layer 2 FIB, Layer 3 FIB, IPv4Flow, IPv4 Ingress ACL, etc. The IPv4Flow region is further sub-divided into 5 regions: System Flow, QoS, PBR, Trace-lists, Multicast FIB & ACL.

You can change the amount of CAM space allocated to each sub-region. You can configure the IPv4Flow region in both EtherScale and TeraScale. In EtherScale, these commands allocate CAM space for IPv4Flow sub-regions and the IPv4 ACL region.

Like CAM profiles, you can configure the IPv4Flow region from EXEC Privilege and CONFIGURATION mode.

The CAM IPv4flow commands are:

- cam ipv4flow (EXEC Privilege)
- cam-ipv4flow (CONFIGURATION)
- show cam-ipv4flow
**cam ipv4flow (EXEC Privilege)**

Configure the amount of CAM space in IPv4flow sub-regions.

**This command is deprecated as of Dell Networking OS 8.3.1.0**

**Syntax**

```
cam ipv4flow {chassis all | linecard number} {default | acl value multicast-fib value pbr value qos value system-flow value trace-list value}
```

**Command Modes**

- EXEC Privilege

**Command History**

- Version 8.3.1.0 COMMAND DEPRECATED
- Version 6.3.1.0 Introduced on E-Series

**cam-ipv4flow (CONFIGURATION)**

Configure the amount of CAM space in IPv4flow sub-regions.

**Syntax**

```
cam-ipv4flow {default | multicast-fib value pbr value qos value system-flow value trace-list value}
```

**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 reset the IPV4Flow CAM region to its default setting.</td>
</tr>
<tr>
<td>multicast-fib value</td>
<td>Enter the keyword <code>multicast-fib</code> followed by the number of entries for the multicast FIB sub-region in 1K increments. Range: 1 to 32 KB Default: 9 KB</td>
</tr>
<tr>
<td>pbr value</td>
<td>Enter the keyword <code>pbr</code> followed by the number of entries for the PBR sub-region in 1K increments. Range: 1 to 32 KB Default: 1 KB</td>
</tr>
<tr>
<td>qos value</td>
<td>Enter the keyword <code>qos</code> followed by the number of entries for the QoS sub-region in 1K increments. Range: 1 to 32 KB Default: 8 KB</td>
</tr>
<tr>
<td>system-flow value</td>
<td>Enter the keyword <code>system-flow</code> followed by the number of entries for the system-flow sub-region in 1K increments. Range: 4 to 32 KB Default: 5 KB</td>
</tr>
<tr>
<td>trace-list value</td>
<td>Enter the keyword <code>trace-list</code> followed by the number of entries for the trace-list sub-region in 1K increments. Range: 1 to 32 KB Default: 1 KB</td>
</tr>
</tbody>
</table>

**Defaults**

See Parameters

**Command Modes**

- CONFIGURATION
show cam-ipv4flow

Display details about the IPv4Flow sub-regions.

Syntax

show cam-ipv4flow

Command Modes

EXEC Privilege

Example

Figure 13-11. Command Example: show cam-ipv4flow

```
FTOS#show cam-ipv4flow

-- Chassis Cam Ipv4Flow --
  Current Settings   Next Boot
Acl                  : 8K          5K
Multicast Fib/Acl    : 9K          12K
Pbr                  : 1K          1K
Qos                  : 8K          8K
System Flow          : 5K          5K
Trace Lists          : 1K          1K

-- Line card 2 --
  Current Settings   Next Boot
Acl                  : 5K          0K
Multicast Fib/Acl    : 9K          12K
Pbr                  : 1K          1K
Qos                  : 8K          8K
System Flow          : 5K          5K
Trace Lists          : 1K          1K

-- Line card 8 --
  Current Settings   Next Boot
Acl                  : 5K          0K
Multicast Fib/Acl    : 9K          12K
Pbr                  : 1K          1K
Qos                  : 8K          8K
System Flow          : 5K          5K
Trace Lists          : 1K          1K

-- Line card 13 --
  Current Settings   Next Boot
Acl                  : 5K          0K
Multicast Fib/Acl    : 9K          12K
Pbr                  : 1K          1K
Qos                  : 8K          8K
System Flow          : 5K          5K
Trace Lists          : 1K          1K

FTOS#
```

Usage Information

If the IPv4Flow sub-region has been changed, this command displays the current IPv4Flow configuration in one column and in the other column displays the IPv4Flow configuration that will be loaded after the next reboot.
CAM Layer 2 ACL Commands

IPv4Flow sub-partitions are supported on the E-Series TeraScale platform.

The CAM Layer 2 ACL commands are:
- `cam l2acl (EXEC Privilege)
- `cam-l2acl (CONFIGURATION)
- `show cam-l2acl

The 18-megabit user configurable CAM is divided into multiple regions such as Layer 2 FIB, Layer 3 FIB, IPv4Flow, IPv4 Ingress ACL, etc. The Layer 2 ACL region is further sub-divided into 6 regions: Sysflow, L2ACL, PVST, QoS, L2PT, FRRP.

You can change the amount of CAM space, in percentage, allocated to each sub-region. The amount of space that you can distribute to the sub-partitions is equal to the amount of CAM space that the selected CAM profile allocates to the Layer 2 ACL partition. Dell Networking OS requires that you specify the amount of CAM space for all sub-partitions and that the sum of all sub-partitions is 100%.

Like CAM profiles, you can configure the Layer 2 ACL partition from EXEC Privilege mode or CONFIGURATION mode.

**cam l2acl (EXEC Privilege)**

Re-allocate the amount of space, in percentage, for each Layer 2 ACL CAM sub-partition.

**This command is deprecated as of Dell Networking OS 8.3.1.0**

**Syntax**
```
cam l2acl {chassis all | linecard number} {default | system-flow percentage l2acl
percentage pvst percentage qos percentage l2pt percentage frrp percentage}
```

**Command Modes**
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version 8.3.1.0</th>
<th>COMMAND DEPRECATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**cam-l2acl (CONFIGURATION)**

Re-allocate the amount of space, in percentage, for each Layer 2 ACL CAM sub-partition.

**Syntax**
```
cam-l2acl {default | system-flow percentage l2acl percentage pvst percentage qos percentage l2pt percentage frrp percentage}
```
The PVST sub-partition requires a minimum number of entries when employing PVST+. See the CAM chapter of the Dell Networking OS Configuration Guide for the E-Series.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Display the percentage of the Layer 2 ACL CAM partition that is allocated to each Layer 2 ACL CAM sub-partition.</td>
</tr>
</tbody>
</table>

### show cam-l2acl

Display the percentage of the Layer 2 ACL CAM partition that is allocated to each Layer 2 ACL CAM sub-partition. If configuration has changed, the command displays the current configuration and the configuration that Dell Networking OS will write to the CAM after the next chassis reboot.

**Syntax**

```
show cam-l2acl
```

**Command Modes**

- EXEC Privilege

**Command History**

- Version 7.7.1.0 Introduced on E-Series
Example

Figure 13-12. Command Example: show cam-l2acl

FTOS#show cam-l2acl

-- Chassis Cam L2-ACL --
  Current Settings (in percent)
  Sysflow : 6
  L2Ac1 : 14
  Pvoi : 50
  Qos : 12
  L2pt : 13
  Frrp : 5

-- Line card 1 --
  Current Settings (in percent)
  Sysflow : 6
  L2Ac1 : 14
  Pvoi : 50
  Qos : 12
  L2pt : 13
  Frrp : 5

-- Line card 5 --
  Current Settings (in percent)
  Sysflow : 6
  L2Ac1 : 14

--More--

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cam-l2acl</td>
<td>Re-allocate the amount of space, in percentage, for each Layer 2 ACL CAM</td>
</tr>
<tr>
<td>(CONFIGURATION)</td>
<td>sub-partition.</td>
</tr>
</tbody>
</table>
Configuration Rollback

Overview

The Configuration Rollback feature is enabled on the C-Series and E-Series. Configuration Rollback enables you to archive your running configurations for future use. This feature also enables you to replace your running configuration with an archived running configuration without rebooting the chassis. Once you load an archived configuration, you have the option to confirm the replacement or revert (roll back) to your previous configuration. This rollback feature enables you to view and test a configuration before completing the configuration change.

Note: Archive files are stored on the internal flash in a hidden directory named CFGARCH. You may have to reboot the chassis when rolling back to a feature that explicitly requires it, like CAM profiles.

Commands

The Configuration Rollback commands are:

- archive
- archive backup
- archive config
- archive delete
- configure confirm
- configure replace
- configure terminal
- configuration mode exclusive
- debug rollback
- maximum number
- show archive
- show config
- show configuration lock
- show run diff
- time-period
**archive**

Enter the CONFIGURATION ARCHIVE mode.

**Syntax**

```
archive
```

To exit the CONFIGURATION ARCHIVE mode, use the `exit` command at the CONFIGURATION ARCHIVE mode prompt (conf-archive).

**Defaults**

No default values or behavior

**Command Modes**

CONFIGURATION ARCHIVE (conf-archive)

**Command History**

Version 7.6.1.0 Introduced on C-Series and E-Series.

**Example**

```
FTOS#conf
FTOS(conf)#archive
FTOS(conf-archive)#
FTOS#
```

---

**archive backup**

Copy an archive file to another location.

**Syntax**

```
archive backup {flash://CFGARCH_DIR/filename} {flash://filepath | ftp://userid:password@hostip/filepath}
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>flash://CFGARCH_DIR/filename</code></td>
<td>Enter the path directory <code>flash://CFGARCH_DIR/</code> followed by the name of the file.</td>
</tr>
<tr>
<td><code>flash://filepath</code></td>
<td>Enter the path <code>flash://</code> followed by the file path of the local file system to copy your file to the local location.</td>
</tr>
<tr>
<td><code>ftp://userid:password@hostip/filepath</code></td>
<td>Enter the path <code>ftp://</code> followed by the FTP remote file system to copy your file to the remote location.</td>
</tr>
</tbody>
</table>

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

Version 7.6.1.0 Introduced on C-Series and E-Series

**Related Commands**

- `show archive` Display the archive

---

**archive config**

Archive a running configuration.

**Syntax**

```
archive config [comment comment]
```

---
Parameters

- **comment comment**
  - Describe the configuration that you are archiving using up to 30 characters.

Defaults

- No default values or behavior

Command Modes

- EXEC Privilege

Command History

- **Version 7.7.1.0** Comment option added
- **Version 7.6.1.0** Introduced on C-Series and E-Series

Usage Information

- Archive files are stored on flash in a hidden directory named CFGARCH. This directory name is an acronym for **Configure Archive**. A maximum of 15 archive files can be stored in this directory.

Example

**Figure 14-1. archive config Command Example**

```plaintext
R4_C300#archive config comment 30 characters
3d2h5m: %RPM0-P:CP %CFGARCHIVE-5-RUNNING_CFG_ARCHIVED: Archived
running-config as archive_0
configuration archived as archive_0
R4_C300#
```

**archive delete**

Delete an archived configuration.

**Syntax**

```plaintext
archive delete {number | all}
```

**Parameters**

<table>
<thead>
<tr>
<th><strong>number</strong></th>
<th>Specify which archived configuration you want to delete.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Enter this keyword to delete all archived configurations.</td>
</tr>
</tbody>
</table>

Defaults

- None

Command Modes

- CONFIG ARCHIVE

Command History

- **Version 7.7.1.0** Introduced on C-Series and E-Series

Example

**Figure 14-2. archive delete Command Example**

```plaintext
FTOS#archive delete all
Please confirm if you want to proceed [yes/no]:yes
all archives have been removed.
FTOS#
```

**configure confirm**

Confirm the replacement of the running configuration when **time** option is used with the **configure replace** command.

**Syntax**

```plaintext
configure confirm
```

**Defaults**

- No default values or behavior
**configure replace**

Replace the running configuration with a specified file.

**Syntax**

```
configure replace {flash://filepath | startup-config [force | time seconds]}
```

**Parameters**

- `flash://filepath`: Enter the path `flash://` followed by the file path of the local file system to copy your file to the local location.
- `startup-config force`: Enter the keyword `startup-config` to replace with the startup configuration and force the replacement without confirmation.
- `force`: Enter the keyword `force` to replace the startup configuration without confirmation.
- `time seconds`: Enter the keyword `time` to replace with the startup configuration and designate the time with which you have to confirm the replacement of the running configuration. Range: 60 to 1800 seconds

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

Version 7.6.1.0 Introduced on C-Series and E-Series

**Related Commands**

- `show archive`: Display the archive

---

**configure terminal**

Enter the exclusive configuration mode when the configuration mode is set to manual.

**Syntax**

```
configure terminal [lock]
```

To undo the lock, use the `exit` command.

**Parameters**

- `lock` (OPTIONAL) Enter the keyword `lock` to lock the confirmation in an exclusive mode.

**Defaults**

Unlocked

**Command Modes**

EXEC Privilege

**Usage Information**

Archiving/replacing a configuration automatically locks CONFIGURATION mode. Use this command when you want exclusive control of CONFIGURATION mode when making configuration changes.

**Command History**

Version 7.6.1.0 Introduced on C-Series and E-Series
configuration mode exclusive

configuration mode exclusive {auto | manual}

To negate the configuration, use the no configuration mode exclusive {auto | manual} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Enter auto to set the exclusive mode to auto.</td>
</tr>
<tr>
<td>manual</td>
<td>Enter manual to set the exclusive mode to manual (the default).</td>
</tr>
</tbody>
</table>

Defaults

CONFIGURATION mode does not lock by default.

Command Modes

EXEC Privilege

Command History

Version 7.6.1.0 Introduced on C-Series and E-Series

Usage Information

If you choose the manual option, you must enter set the lock each time before entering CONFIGURATION mode.

If you choose the auto option, you can exit to EXEC Privilege mode and re-enter CONFIGURATION mode without setting the lock again.

If another user attempts to enter the CONFIGURATION mode while a lock is in place, the following message is generated:

% Error: User "" on line console0 is in exclusive configuration mode

If a user is already in CONFIGURATION mode when a lock is executed, the following message is generated:

% Error: Can't lock configuration mode exclusively since the following users are currently configuring the system:

User "admin" on line vty1 ( 10.1.1.1 )

Note: The CONFIGURATION mode lock corresponds to a VTY session, not to a user. If you set a lock and then exit the CONFIGURATION mode and another user enters CONFIGURATION mode, you will be denied access when you attempt to re-enter CONFIGURATION mode.
Example

```
FTOS(conf)#configuration mode exclusive auto
FTOS(conf)#exit
3d23h35m: %RPM0-P:CP %SYS-5-CONFIG_I: Configured from console by console
FTOS#config! Locks configuration mode exclusively.
FTOS(conf)#
```

Note: When your session times out and you return to EXEC mode, the lock is no longer set.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>When configuration is set to manual, use this command to set the exclusive mode.</td>
</tr>
</tbody>
</table>

**debug rollback**

Enable debugging for the configuration replace and rollback feature.

Syntax

```
debug rollback
```

Disable debugging using the command `undebug all`.

Defaults

Debugging is disabled for all features by default.

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and E-Series</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>undebug all</td>
<td>Disable all debug operations on the system.</td>
</tr>
</tbody>
</table>

**maximum number**

Set the maximum number of archives.

Syntax

```
maximum {number}
```

To return to the default, use the `no maximum {number}` command.

Parameters

- `number` Enter the maximum number of files to archive.
  - Range: 2 to 15
  - Default: 10

Defaults

No default values or behavior

Command Modes

CONFIGURATION (conf-archive)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and E-Series</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show archive</td>
<td>Display the archive</td>
</tr>
</tbody>
</table>
show archive

Display the content of the archive.

Syntax:
```
show archive
```

Defaults:
No default values or behavior

Command Modes:
EXEC Privilege

Command History:
Version 7.6.1.0  Introduced on C-Series and E-Series

Example:
```
Figure 14-3.  show archive Command Output

FTOS#show archive
Archive directory: flash:/CFGARCH_DIR
#    Archive        Date        Time      Size        Comment
0    -             -           -          -           
1    -             -           -          -           
2    -             -           -          -           
3    -             -           -          -           
4    -             -           -          -           
5    -             -           -          -           
6    -             -           -          -           Deleted
7    *archive_7    12/13/2007  20:51:24  5640        Archived
8    archive_8     12/13/2007  20:51:44  5645        Archived
9    archive_9     12/16/2007  21:43:44  5677        Most recently archived
10   -             -           -          -           
11   -             -           -          -           Deleted
12   -             -           -          -           Deleted
13   -             -           -          -           Deleted
14   -             -           -          -           
FTOS#
```

Usage Information:
The most recent archived configuration is marked with an asterisk in the output of this command.

show config

Display the contents of the archive configuration.

Syntax:
```
show config
```

Defaults:
No default values or behavior

Command Modes:
CONFIGURATION (conf-archive)

Command History:
Version 7.6.1.0  Introduced on C-Series and E-Series

Example:
```
FTOS#(conf-archive)#show config
! archive
maximum 3
FTOS#(conf-archive)#
```
show configuration lock

Syntax
show configuration lock

Defaults
None

Command Modes
EXEC Privilege

Command History
Version 7.7.1.0  Introduced on C-Series and E-Series

Example
Figure 14-4. show configuration lock Command Output

FTOS# show configuration lock
Configure exclusively locked by the following line:
Line : vty 0
Line number : 2
User : admin
Type : AUTO
State : LOCKED
Ip address : 10.11.9.97

Usage Information
The type may be auto, manual, or rollback. When set to auto, Dell Networking OS automatically
denies access to CONFIGURATION mode to all other users every time the user on the listed VTY line
enters CONFIGURATION mode. When set to manual, the user on the listed VTY line must explicitly
set the lock each time before entering CONFIGURATION mode. Rollback indicates that Dell
Networking OS is in a rollback process. The line number shown in the output can be used to send the
messages to that session or release a lock on a VTY line.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear line</td>
<td>Reset a terminal line.</td>
</tr>
<tr>
<td>configuration mode exclusive</td>
<td>Enable exclusive configuration mode.</td>
</tr>
<tr>
<td>send</td>
<td>Send messages to one or all terminal line users.</td>
</tr>
</tbody>
</table>

show run diff

Syntax
show run diff {flash: | startup-config}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash:</td>
<td>Enter the archive configuration file using the path [flash://]filename</td>
</tr>
<tr>
<td>startup-config</td>
<td>Enter the keywords startup-config to compare the contents of the startup configuration.</td>
</tr>
</tbody>
</table>

Defaults
No default values or behavior

Command Modes
EXEC Privilege

Command History
Version 7.6.1.0  Introduced on C-Series and E-Series
**Example**

**Figure 14-5.  show run diff archive Command Example**

```
FTOS#show run diff archive_7
running-config
-------
< policy-map-input test
running-config
-------
< archive
< maximum 3
flash:/CFGARCH_DIR/archive_7
-------
> archive
FTOS#
```

**time-period**

Set a time period to automatically save an archive file.

**Syntax**

```
time-period {minutes}
```

To stop the auto-save, use the **no time-period {minutes}** command.

**Parameters**

- **minutes**
  - Enter the time, in minutes to automatically save an archive file.
  - Range: 5 to 1440 minutes

**Defaults**

Disabled, that is no automatically saving is configured

**Command Modes**

CONFIGURATION (conf-archive)

**Command History**

- **Version 7.6.1.0**
  - Introduced on C-Series and E-Series
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.

- Commands to Configure the System to be a DHCP Server
- Commands to Configure Secure DHCP

Commands to Configure the System to be a DHCP Server

- clear ip dhcp
- client-identifier
- debug ip dhcp server
- default-router
- disable
- dns-server
- domain-name
- excluded-address
- hardware-address
- host
- ip dhcp bootp
- ip dhcp relay information
- disable
- lease
- netbios-name-server
- netbios-node-type
- network
- pool
- show ip dhcp binding
- show ip dhcp configuration
- show ip dhcp conflict
- show ip dhcp database
- show ip dhcp server
clear ip dhcp

Syntax: clear ip dhcp [binding {address} | conflicts | 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.
- conflicts: 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 8.2.1.0 Introduced on C-Series and S-Series.

Usage Information:
- Entering <CR> after clear ip dhcp binding, clears all the IPs from the binding table.

client-identifier

Syntax: client-identifier unique-identifier

Parameters:
- unique-identifier: Enter the client identifier for a Microsoft.

Command Mode: DHCP

Default: None

Command History:
- Version 8.2.1.0 Introduced on C-Series and S-Series.

Usage Information:
- Microsoft clients require a client identifier instead of a hardware addresses. The client identifier is formed by concatenating the media type and the MAC address of the client. Refer to the “Address Resolution Protocol Parameters” section of RFC 1700—Assigned Numbers, for a list of media type codes.

debug ip dhcp server

Syntax: debug ip dhcp server [events | packets]
**default-router**

Assign a default gateway to clients based on address pool.

**Syntax**

```
default-router address [address2...address8]
```

**Parameters**

- `address`: Enter 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>

**Default**

None

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.

**disable**

Disable 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**

CONFIGURATION

**Default**

Disabled

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.

**dns-server**

Assign a DNS server to clients based on address pool.

**Syntax**

```
dns-server address [address2...address8]
```
Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Enter the a list of DNS servers that may service clients on the subnet. You may list up to 8 servers, in order of preference.</td>
</tr>
</tbody>
</table>

Command Mode

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

Default

<table>
<thead>
<tr>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**domain-name**

Assign a domain to clients based on address pool.

Syntax

```
domain-name name
```

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Give a name to the group of addresses in a pool.</td>
</tr>
</tbody>
</table>

Command Mode

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

Default

<table>
<thead>
<tr>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**excluded-address**

Prevent the server from leasing an address or range of addresses in the pool.

Syntax

```
excluded-address [address | low-address high-address]
```

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Enter a single address to be excluded from the pool.</td>
</tr>
<tr>
<td>low-address</td>
<td>Enter the lowest address in a range of addresses to be excluded from the pool.</td>
</tr>
<tr>
<td>high-address</td>
<td>Enter the highest address in a range of addresses to be excluded from the pool.</td>
</tr>
</tbody>
</table>

Command Mode

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>DHCP</td>
</tr>
</tbody>
</table>

Default

<table>
<thead>
<tr>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**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 8.2.1.0 Introduced on C-Series and S-Series.

---

**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 8.2.1.0 Introduced on C-Series and S-Series.

---

**ip dhcp bootp**

Allow the DHCP server to respond to BOOTP messages, or direct the server to ignore them.

**Syntax**

```
ip dhcp bootp [automatic | ignore]
```

**Parameters**

- `automatic` Enter this keyword to instruct the server to respond to BOOTP messages.
- `ignore` Enter this keyword to instruct the server to ignore all BOOTP messages.

**Command Mode**

DHCP

**Default**

automatic

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.

---

**ip dhcp relay information**

**Syntax**

```
ip dhcp relay information [check | option | policy]
```

**Parameters**

- `check`
### lease

Specify a lease time for the addresses in a pool.

**Syntax**

```plaintext
lease {days [hours] [minutes] | infinite}
```

**Parameters**

- `days`
  - Enter the number of days of the lease.
  - Range: 0-31
- `hours`
  - Enter the number of hours of the lease.
  - Range: 0-23
- `minutes`
  - Enter the number of minutes of the lease.
  - Range: 0-59
- `infinite`
  - Specify that the lease never expires.

**Command Mode**

- `DHCP <POOL>`

**Default**

- 24 hours

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.

### 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**

```plaintext
netbios-name-server address [address2...address8]
```

**Parameters**

- `address`
  - Enter the address of the NetBIOS name server. You may enter up to 8, in order of preference.

**Command Mode**

- `DHCP <POOL>`

**Default**

- None

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.
**netbios-node-type**

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking recommends specifying clients as hybrid.

**Syntax**

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

**Parameters**

- `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**

DHCP <POOL>

**Default**

Hybrid

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.

**network**

Specify the range of addresses in an address pool.

**Syntax**

```
network network /prefix-length
```

**Parameters**

- `network` Specify a range of addresses.
- `prefix-length` Prefix-length Range: 17-31

**Command Mode**

DHCP <POOL>

**Default**

None

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.

**pool**

Create an address pool.

**Syntax**

```
pool name
```

**Parameters**

- `name` Enter the address pool’s identifying name

**Command Mode**

DHCP

**Default**

None

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.
show ip dhcp binding  
Display the DHCP binding table.

Syntax  show ip dhcp binding

Command Mode  EXEC Privilege

Default  None

Command History  Version 8.2.1.0  Introduced on C-Series and S-Series.

show ip dhcp configuration  
Display the DHCP configuration.

Syntax  show ip dhcp configuration [global | pool name]

Parameters  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool name</td>
<td>Display the configuration for a DHCP pool.</td>
</tr>
<tr>
<td>global</td>
<td>Display the DHCP configuration for the entire system.</td>
</tr>
</tbody>
</table>

Command Mode  EXEC Privilege

Default  None

Command History  Version 8.2.1.0  Introduced on C-Series and S-Series.

show ip dhcp conflict  
Display the address conflict log.

Syntax  show ip dhcp conflict address

Parameters  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Display a particular conflict log entry.</td>
</tr>
</tbody>
</table>

Command Mode  EXEC Privilege

Default  None

Command History  Version 8.2.1.0  Introduced on C-Series and S-Series.

show ip dhcp database  
Display the DHCP database.

Syntax  show ip dhcp database
show ip dhcp server

Display the DHCP server statistics.

Syntax

show ip dhcp server statistics

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
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 8.3.1.0 Introduced on E-Series.
- Version 8.2.1.0 Introduced on C-Series and S-Series

**Related Commands**
- `arp inspection-trust` Specify a port as trusted so that ARP frames are not validated against the binding table.

**clear ip dhcp snooping**

Clear the DHCP binding table.

**Syntax**
```
clear ip dhcp snooping binding
```

**Command Modes**
- EXEC Privilege

**Default**
None

**Command History**
- Version 8.3.1.0 Introduced on E-Series.
- Version 7.8.1.0 Introduced on C-Series and S-Series

**Related Commands**
- `show ip dhcp snooping` Display the contents of the DHCP binding table.

**ip dhcp snooping**

Enable DHCP Snooping globally.

**Syntax**
```
[no] ip dhcp snooping
```
When enabled, no learning takes place until snooping is enabled on a VLAN. Upon disabling DHCP Snooping the binding table is deleted, and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

Introduced in Dell Networking OS version 7.8.1.0, DHCP Snooping was available for Layer 3 only and dependent on DHCP Relay Agent (ip helper-address). Dell Networking OS 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>Enable 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**

- Version 8.3.1.0: Introduced on E-Series.
- Version 7.8.1.0: Introduced on C-Series and S-Series on Layer 3 interfaces.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

**Syntax**

```
[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number
```

**Parameters**

- **mac address**
  - Enter the keyword mac followed by the MAC address of the host to which the server is leasing the IP address.

- **vlan-id vlan-id**
  - Enter the keyword vlan-id followed by the VLAN to which the host belongs. Range: 2-4094

- **ip ip-address**
  - Enter the keyword ip followed by the IP address that the server is leasing.
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 8.4.6.0 Added support for the keyword fortyGigE.
Version 8.3.1.0 Introduced on E-Series.
Version 7.8.1.0 Introduced on C-Series and S-Series

Related Commands

show ip dhcp snooping Display the contents of the DHCP binding table.
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
Untrusted

Command History
Version 8.3.1.0 Introduced on E-Series.
Version 8.2.1.0 Added keyword ipmac.
Version 7.8.1.0 Introduced on C-Series and S-Series

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 8.3.1.0 Introduced on E-Series.
Version 7.8.1.0 Introduced on C-Series and S-Series

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.
Dynamic Host Configuration Protocol (DHCP)

**ip dhcp relay**

Enable Option 82.

**Syntax**

```
ip dhcp relay information-option [trust-downstream]
```

**Parameters**

- `trust-downstream`: Configure the system to trust Option 82 when it is received from the previous-hop router.

**Command Modes**

CONFIGURATION

**Default**

Disabled

**Command History**

- Version 8.3.1.0: Introduced on E-Series.
- Version 7.8.1.0: Introduced on C-Series and S-Series

**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]
```

**Parameters**

- `binding`: Display the binding table.
- `source-address-validation`: Display the interfaces configured with IP Source Guard.

**Command Modes**

EXEC

EXEC Privilege

**Default**

None

**Command History**

- Version 8.3.1.0: Introduced on E-Series.
- Version 7.8.1.0: Introduced on C-Series and S-Series

**Related Commands**

- `clear ip dhcp snooping`: Clear 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
```

**Related Commands**

- `ip dhcp snooping trust`: Configure an interface as trusted.
<table>
<thead>
<tr>
<th>Command Modes</th>
<th>CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.3.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
</tbody>
</table>
Equal Cost Multi-Path

Overview

The characters that appear below command headings indicate support for the associated Dell Networking platform, as follows:

- C-Series: C
- E-Series: E
- S-Series: S

Commands

The ECMP commands are:

- hash-algorithm
- hash-algorithm ecmp
- hash-algorithm seed
- ip ecmp-deterministic
- ipv6 ecmp-deterministic

hash-algorithm

Change the hash algorithm used to distribute traffic flows across a Port Channel. The ECMP, LAG, and line card options are supported only on the E-Series TeraScale and ExaScale chassis.

Syntax

```
hash-algorithm {algorithm-number | {ecmp {checksum| crc | xor} [number] lag {checksum| crc | xor} [number] nh-ecmp {checksum| crc | xor} [number] linecard number ip-sa-mask value ip-da-mask value}
```

To return to the default hash algorithm, use the `no hash-algorithm` command.

To return to the default the Equal-cost Multipath Routing (ECMP) hash algorithm, use the `no hash-algorithm ecmp algorithm-value` command.

To remove the hash algorithm on a particular line card, use the `no hash-algorithm linecard number` command.
Equal Cost Multi-Path

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>algorithm-number</code></td>
<td>Enter the algorithm number. Range: 0 to 47</td>
</tr>
<tr>
<td><code>ecmp hash algorithm value</code></td>
<td>TeraScale and ExaScale Only: Enter the keyword <code>ecmp</code> followed by the ECMP hash algorithm value. Range: 0 to 47</td>
</tr>
<tr>
<td><code>lag hash algorithm value</code></td>
<td>TeraScale and ExaScale Only: Enter the keyword <code>lag</code> followed by the LAG hash algorithm value. Range: 0 to 47</td>
</tr>
<tr>
<td><code>nh-ecmp hash algorithm value</code></td>
<td>(OPTIONAL) Enter the keyword <code>nh-ecmp</code> followed by the ECMP hash algorithm value.</td>
</tr>
<tr>
<td><code>linecard number</code></td>
<td>(OPTIONAL) TeraScale and ExaScale Only: Enter the keyword <code>linecard</code> followed by the line card slot number. Range: 0 to 13 on an E1200/E1200i, 0 to 6 on an E600/E600i, and 0 to 5 on an E300</td>
</tr>
<tr>
<td><code>ip-sa-mask value</code></td>
<td>(OPTIONAL) Enter the keyword <code>ip-sa-mask</code> followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF</td>
</tr>
<tr>
<td><code>ip-da-mask value</code></td>
<td>(OPTIONAL) Enter the keyword <code>ip-da-mask</code> followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF</td>
</tr>
</tbody>
</table>

Defaults

0 for hash-algorithm value on TeraScale and ExaScale
IPSA and IPDA mask value is FF for line card

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added nh-ecmp option</td>
</tr>
<tr>
<td>7.7.1.1</td>
<td>Added nh-ecmp option</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Added support for the line card option on TeraScale only</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added the support for ECMP and LAG on TeraScale only</td>
</tr>
</tbody>
</table>

Usage Information

Set the default hash-algorithm method on ExaScale systems to ensure CRC is not used for LAG. For example, `hash-algorithm ecmp xor lag checksum nh-ecmp checksum`

To achieve the functionality of hash-align on the ExaScale platform, do not use CRC as a hash-algorithm method.

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The hash algorithm command with the line card option changes the hash for a particular line card by applying the mask specified in the IPSA and IPDA fields.

The line card option is applicable with the lag-hash-align microcode only (refer to `cam-profile (Config)`). Any other microcode returns an error message as follows:
FTOS(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff

% Error: This command is not supported in the current microcode configuration.

In addition, the linecard number ip-sa-mask value ip-da-mask value option has the following behavior to maintain bi-directionality:

- When hashing is done on both IPSA and IPDA, the ip-sa-mask and ip-da-mask values must be equal. (Single Linecard)
- When hashing is done only on IPSA or IPDA, Dell Networking OS maintains bi-directionality with masks set to XX 00 for line card 1 and 00 XX for line card 2 (ip-sa-mask and ip-da-mask). The mask value must be the same for both line cards when using multiple line cards as ingress (where XX is any value from 00 to FF for both line cards). For example, assume traffic is flowing between linecard 1 and linecard 2:

  hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00
  hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, then use the hash-algorithm command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

On TeraScale if the keyword ECMP or LAG is not entered, Dell Networking OS assumes it to be common for both. If the keyword ECMP or LAG is entered separately, both should fall in the range of 0 to 23 or 24 to 47 since compression enable/disable is common for both.

TeraScale and ExaScale support the range 0-47. The default for ExaScale is 24.

For EtherScale, only the range 0 to 15 is valid; 16 to 47 is considered as 15.

<table>
<thead>
<tr>
<th>Range</th>
<th>Compression Status</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-11</td>
<td>Compression Enabled</td>
<td>rotate [0 - 11]</td>
</tr>
<tr>
<td>12-23</td>
<td>Compression Enabled</td>
<td>shift [0 - 11]</td>
</tr>
<tr>
<td>24-35</td>
<td>Compression Disabled</td>
<td>rotate [0 - 11]</td>
</tr>
<tr>
<td>36-47</td>
<td>Compression Disabled</td>
<td>shift [0 - 11]</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>load-balance (E-Series)</td>
<td>Change the traffic balancing method.</td>
</tr>
</tbody>
</table>
hash-algorithm ecmp

Change the hash algorithm used to distribute traffic flows across an ECMP (equal-cost multipath routing) group.

Syntax

hash-algorithm ecmp {crc-upper} | {dest-ip} | {lsb}

To return to the default hash algorithm, use the no hash-algorithm ecmp command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>crc-upper</td>
<td>Uses the upper 32 bits of the key for the hash computation</td>
<td>crc-lower</td>
</tr>
<tr>
<td>dest-ip</td>
<td>Uses the destination IP for ECMP hashing</td>
<td>enabled</td>
</tr>
<tr>
<td>lsb</td>
<td>Returns the LSB of the key as the hash</td>
<td>crc-lower</td>
</tr>
</tbody>
</table>

Defaults
crc-lower, dest-ip enabled

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

Usage Information

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The default ECMP hash configuration is crc-lower. This takes the lower 32 bits of the hash key to compute the egress port and is the “fall-back” configuration if the user hasn’t configured anything else.

The different hash algorithms are based on the number of ECMP group members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide satisfactory distribution of traffic, then use this command to designate another algorithm.

When a member leaves or is added to the ECMP group, the hash algorithm is recalculated to balance traffic across the members.

Related Commands

load-balance (C-Series and S-Series)

hash-algorithm seed

Select the seed value for the ECMP, LAG, and NH hashing algorithm.

Syntax

hash-algorithm seed value [linecard slot] [port-set number]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range/Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>seed value</td>
<td>Enter the keyword followed by the seed value.</td>
<td>0 - 4095</td>
</tr>
<tr>
<td>linecard slot</td>
<td>Enter the keyword followed by the line card slot number.</td>
<td></td>
</tr>
<tr>
<td>port-set number</td>
<td>Enter the keyword followed by the line card port-pipe number.</td>
<td></td>
</tr>
</tbody>
</table>

Defaults

None
Deterministic ECMP sorts ECMPs in order even though RTM provides them in a random order. However, the hash algorithm uses as a seed the lower 12 bits of the chassis MAC, which yields a different hash result for every chassis. This means that for a given flow, even though the prefixes are sorted, two unrelated chassis will select different hops.

Dell Networking OS provides a CLI-based solution for modifying the hash seed to ensure that on each configured system, the ECMP selection is same. When configured, the same seed is set for ECMP, LAG, and NH, and is used for incoming traffic only.

**Note:** While the seed is stored separately on each port-pipe, the same seed is used across all CAMs. 
**Note:** You cannot separate LAG and ECMP, but you can use different algorithms across chassis with the same seed. If LAG member ports span multiple port-pipes and line cards, set the seed to the same value on each port-pipe to achieve deterministic behavior. 
**Note:** If the hash algorithm configuration is removed. Hash seed will not go to original factory default setting.

**ip ecmp-deterministic**

Deterministic ECMP Next Hop arranges all ECMPs in order before writing them into the CAM. For example, suppose the RTM learns 8 ECMPs in the order that the protocols and interfaces came up. In this case, the FIB and CAM sort them so that the ECMPs are always arranged. This implementation ensures that every chassis having the same prefixes orders the ECMPs the same.

With 8 or less ECMPs, the ordering is lexicographic and deterministic. With more than 8 ECMPs, ordering is deterministic, but it is not in lexicographic order.

**Syntax**

```
ip ecmp-deterministic
```

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

| Version 8.3.1.0 | Introduced on E-Series. |

**Usage Information**

After enabling IPv6 Deterministic ECMP, traffic loss occurs for a few milliseconds while Dell Networking OS sorts the CAM entries.

**ipv6 ecmp-deterministic**

Deterministic ECMP Next Hop arranges all ECMPs in order before writing them into the CAM. For example, suppose the RTM learns 8 ECMPs in the order that the protocols and interfaces came up. In this case, the FIB and CAM sort them so that the ECMPs are always arranged. This implementation ensures that every chassis having the same prefixes orders the ECMPs the same.
With 8 or less ECMPs, the ordering is lexicographic and deterministic. With more than 8 ECMPs, ordering is deterministic, but it is not in lexicographic order.

**Syntax**  
`ipv6 ecmp-deterministic`

**Defaults**  
Disabled

**Command Modes**  
CONFIGURATION

**Command History**  
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**  
After enabling IPv6 Deterministic ECMP, traffic loss occurs for a few milliseconds while Dell Networking OS sorts the CAM entries.
Far-End Failure Detection (FEFD)

Overview

FTOS supports Far-End Failure Detection (FEFD) on the Ethernet interfaces of the E-Series, as indicated by the \( e \) character that appears below each command heading. This feature detects and reports far-end link failures.

- FEFD is not supported on the Management interface.
- During an RPM failover, FEFD is operationally disabled for approximately 8-10 seconds.
- By default, FEFD is disabled.

Commands

The FEFD commands are:

- debug fefd
- fefd
- fefd mode
- fefd-global
- fefd disable
- fefd interval
- fefd-global interval
- fefd reset
- show fefd

**debug fefd**

Enable debugging of FEFD.

**Syntax**

```
debug fefd {events | packets} [interface]
```

To disable debugging of FEFD, use the `no debug fefd {events | packets} [interface]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>events</code></td>
<td>Enter the keyword <code>events</code> to enable debugging of FEFD state changes.</td>
</tr>
</tbody>
</table>
**Command Modes**

**EXEC Privilege**

**fefd**

Enable Far-End Failure Detection on an interface.

**Syntax**

```plaintext
fefd
```

To disable FEFD on an interface, enter `no fefd`.

**Defaults**

Disabled.

**Command Modes**

INTERFACE

**Usage Information**

When you enter `no fefd` for an interface and `fefd-global`, FEFD is enabled on the interface because the `no fefd` command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the `fefd disable` command.

**fefd mode**

Change the FEFD mode on an interface.

**Syntax**

```plaintext
fefd mode {normal | aggressive}
```

To return the FEFD mode to the default of normal, enter `no fefd mode`.

**Parameters**

- **normal**
  
  (OPTIONAL) Enter the keyword `normal` to change the link state to “unknown” when a far-end failure is detected by the software on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol.

- **aggressive**
  
  (OPTIONAL) Enter the keyword `aggressive` to change the link state to “error-disabled” when a far-end failure is detected by the software on that interface. When an interface is placed in “error-disabled” state, you must enter the `fefd reset` command to reset the interface state.

**Defaults**

normal

**Command Modes**

INTERFACE
**fefd-global**

Enable FEFD globally on the system.

**Syntax**

```
fe.fd-global [mode {normal | aggressive}]
```

To disable FEFD globally, use the `no fefd-global [mode {normal | aggressive}]` command syntax.

**Parameters**

- **mode normal** (OPTIONAL) Enter the keywords `mode normal` to change the link state to “unknown” when a far-end failure is detected by the software on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol. Normal mode is the default.

- **mode aggressive** (OPTIONAL) Enter the keyword `mode aggressive` to change the link state to “error-disabled” when a far-end failure is detected by the software on that interface. When an interface is placed in “error-disabled” state, you must enter the `fefd reset` command to reset the interface state.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Usage Information**

If you enter only the `fe.fd-global` syntax, the mode is normal and the default interval is 15 seconds.

If you disable FEFD globally (`no fefd-global`), the system does not remove the FEFD interface configuration.

**fefd disable**

Disable FEFD on an interface only. This command overrides the `fe.fd-global` command for the interface.

**Syntax**

```
fefd disable
```

To re-enable FEFD on an interface, enter `no fefd disable`.

**Default**

Not configured.

**Command Modes**

INTERFACE

**fefd interval**

Set an interval between control packets.

**Syntax**

```
fefd interval seconds
```

To return to the default value, enter `no fefd interval`. 
Parameters

<table>
<thead>
<tr>
<th>seconds</th>
<th>Enter a number as the time between FEFD control packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range: 3 to 300 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 15 seconds</td>
</tr>
</tbody>
</table>

Defaults

15 seconds

Command Modes

INTERFACE

**fefd-global interval**

Configure an interval between FEFD control packets.

Syntax

```
fefd-global interval seconds
```

To return to the default value, enter `no fefd-global interval`.

Parameters

<table>
<thead>
<tr>
<th>seconds</th>
<th>Enter a number as the time between FEFD control packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range: 3 to 300 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 15 seconds</td>
</tr>
</tbody>
</table>

Defaults

15 seconds

Command Modes

CONFIGURATION

**fefd reset**

Reset all interfaces or a single interface that was in “error-disabled” mode.

Syntax

```
fefd reset [interface]
```

Parameters

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

Defaults

Not configured.

Command Modes

EXEC Privilege

**show fefd**

View FEFD status globally or on a specific interface.

Syntax

```
show fefd [interface]
```


Far-End Failure Detection (FEFD) | 487

**Parameters**

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

**Command Modes**

- EXEC
- EXEC Privilege

**Example**

**Figure 17-1. Command Example: show fefd**

```
FTOS#sh fefd
FEFD is globally 'ON', interval is 10 seconds, mode is 'Aggressive'.

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>MODE</th>
<th>INTERVAL (second)</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 5/0</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/1</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/2</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/3</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/4</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/5</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/6</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/7</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/8</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/9</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/10</td>
<td>NA</td>
<td>NA</td>
<td>Locally disabled</td>
</tr>
<tr>
<td>Gi 5/11</td>
<td>Aggressive</td>
<td>10</td>
<td>Err-disabled</td>
</tr>
</tbody>
</table>

FTOS#
```

**Table 17-1. Description of show fefd display**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the interfaces type and number.</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the mode (aggressive or normal) or NA if the interface contains <code>fefd disable</code> in its configuration.</td>
</tr>
<tr>
<td>Interval</td>
<td>Displays the interval between FEFD packets.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the interface and can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• bi-directional (interface is up and connected and seeing neighbor’s echo)</td>
</tr>
<tr>
<td></td>
<td>• err-disabled (only found when the FEFD mode is aggressive and when the interface has not seen its neighbor’s echo for 3 times the message interval. To reset an interface in this state, use the <code>fefd reset</code> command.)</td>
</tr>
<tr>
<td></td>
<td>• unknown (only found when FEFD mode is normal)</td>
</tr>
<tr>
<td></td>
<td>• locally disabled (interface contains the <code>fefd disable</code> command in its configuration)</td>
</tr>
<tr>
<td></td>
<td>• Admin Shutdown (interface is disabled with the <code>shutdown</code> command)</td>
</tr>
</tbody>
</table>
Dell Networking OS Resilient Ring Protocol (FRRP)

Overview

Dell Networking OS Resilient Ring Protocol (FRRP) is supported on platforms C E S.

FRRP is a proprietary protocol for that offers fast convergence in a Layer 2 network without having to run the Spanning Tree Protocol. The Resilient Ring Protocol is an efficient protocol that transmits a high-speed token across a ring to verify the link status. All the intelligence is contained in the master node with practically no intelligence required of the transit mode.

Commands

The FRRP commands are:

- clear frrp
- debug frrp
- description
- disable
- interface
- member-vlan
- mode
- protocol frrp
- show frrp
- timer

Important Points to Remember

- FRRP is media- and speed-independent.
- FRRP is a Dell Networking proprietary protocol that does not interoperate with any other vendor.
- Spanning Tree must be disabled on both primary and secondary interfaces before Resilient Ring protocol is enabled.
- A VLAN configured as control VLAN for a ring cannot be configured as control or member VLAN for any other ring.
- Member VLANs across multiple rings are not supported in Master nodes.
- If multiple rings share one or more member VLANs, they cannot share any links between them.
- Each ring can have only one Master node; all others are Transit nodes.

**clear frrp**

Clear the FRRP statistics counters.

**Syntax**

clear frrp [ring-id]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ring-id</td>
<td>(Optional) Enter the ring identification number.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 255</td>
</tr>
</tbody>
</table>

**Defaults**

No default values or behavior

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced for the C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

**Figure 18-1. clear frrp Command Examples**

```
FTOS#clear frrp clears the frrp counters for all the available rings

Clear frrp statistics counter on all ring [confirm] yes confirmation required

FTOS#clear frrp 4 clears the frrp counters on the specified ring

Clear frrp statistics counter for ring 4 [confirm] yes confirmation required

FTOS#
```

**Usage Information**

Executing this command, without the optional `ring-id`, will clear statistics counters on all the available rings. Dell Networking OS requires a command line confirmation before the command is executed. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

**Related Commands**

- `show frrp` Display the Resilient Ring Protocol configuration

**debug frrp**

Enable FRRP debugging.

**Syntax**

debug frrp {event | packet | detail} [ring-id] [count number]

To disable debugging, use the `no debug frrp {event | packet | detail} {ring-id} [count number]` command.
### Parameters

<table>
<thead>
<tr>
<th><strong>event</strong></th>
<th>Enter the keyword <code>event</code> to display debug information related to ring protocol transitions.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>packet</strong></td>
<td>Enter the keyword <code>packet</code> to display brief debug information related to control packets.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>Enter the keyword <code>detail</code> to display detailed debug information related to the entire ring protocol packets.</td>
</tr>
<tr>
<td><strong>ring-id</strong></td>
<td>(Optional) Enter the ring identification number. Range: 1 to 255</td>
</tr>
<tr>
<td><strong>count number</strong></td>
<td>Enter the keyword <code>count</code> followed by the number of debug outputs. Range: 1 to 65534</td>
</tr>
</tbody>
</table>

### Defaults

Disabled

### Command Modes

CONFIGURATION (conf-frrp)

### Command History

<table>
<thead>
<tr>
<th>Version 8.2.1.0</th>
<th>Introduced for the C-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### Usage Information

Since the Resilient Ring Protocol can potentially transmit 20 packets per interface, debug information must be restricted.

### description

Enter an identifying description of the ring.

**Syntax**

```
description Word
```

To remove the ring description, use the `no description [Word]` command.

**Parameters**

<table>
<thead>
<tr>
<th><strong>Word</strong></th>
<th>Enter a description of the ring. Maximum: 255 characters</th>
</tr>
</thead>
</table>

### Defaults

No default values or behavior

### Command Modes

CONFIGURATION (conf-frrp)

### Command History

<table>
<thead>
<tr>
<th>Version 8.2.1.0</th>
<th>Introduced for the C-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### disable

Disable the Resilient Ring Protocol.

**Syntax**

```
disable
```

To enable the Resilient Ring Protocol, use the `no disable` command.

**Defaults**

Disabled
interface

Configure the primary, secondary, and control-vlan interfaces.

Syntax

```
interface {primary interface secondary interface control-vlan vlan-id}
```

To return to the default, use the `no interface {primary interface secondary interface control-vlan vlan-id}` command.

Parameters

- **primary interface**
  - Enter the keyword `primary` to configure the primary interface followed by one of the following interfaces and slot/port information:
    - For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` 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:
      - **C-Series and S-Series** Range: 1-128
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

- **secondary interface**
  - Enter the keyword `secondary` to configure the secondary interface followed by one of the following interfaces and slot/port information:
    - For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
      - **C-Series and S-Series** Range: 1-128
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

- **control-vlan vlan-id**
  - Enter the keyword `control-vlan` followed by the VLAN ID.
    - Range: 1 to 4094

Defaults

No default values or behavior

Command Modes

- `CONFIGURATION (conf-frrp)`
This command causes the Ring Manager to take ownership of these two ports after the configuration is validated by the IFM. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is, the interface does not belong to any ring.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show frrp</code></td>
<td>Display the Resilient Ring Protocol configuration information</td>
</tr>
</tbody>
</table>

**member-vlan**

Specify the member VLAN identification numbers.

**Syntax**

```
member-vlan {vlan-range}
```

**Parameters**

- `vlan-range` Enter the member VLANs using comma separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example:
  - Comma separated: 3, 4, 6
  - Range: 5-10
  - Combination: 3, 4, 5-10, 8

**Defaults**

No default values or behavior

**Command Modes**

```
CONFIGURATION (conf-frrp)
```

**Command History**

- **Version 8.4.6.0**: Added support for the keyword `fortyGigE`.
- **Version 8.2.1.0**: Introduced for the C-Series
- **Version 7.4.1.0**: Introduced

**mode**

Set the Master or Transit mode of the ring.

**Syntax**

```
mode {master | transit}
```

**Parameters**

- `master` Enter the keyword `master` to set the Ring node to Master mode.
- `transit` Enter the keyword `transit` to set the Ring node to Transit mode.

**Defaults**

Mode None

**Command Modes**

```
CONFIGURATION (conf-frrp)
```
**protocol frrp**

Enter the Resilient Ring Protocol and designate a ring identification.

**Syntax**

```
protocol frrp {ring-id}
```

To exit the ring protocol, use the `no protocol frrp {ring-id}` command.

**Parameters**

- `ring-id` Enter the ring identification number.
  
  Range: 1 to 255

**Defaults**

No default values or behavior

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.2.1.0 Introduced for the C-Series
- Version 7.4.1.0 Introduced

**Usage Information**

This command places you into the Resilient Ring Protocol. After executing this command, the command line prompt changes to conf-frrp.

**show frrp**

Display the Resilient Ring Protocol configuration.

**Syntax**

```
show frrp [ring-id [summary]] | [summary]
```

**Parameters**

- `ring-id` Enter the ring identification number.
  
  Range: 1 to 255

- `summary` (OPTIONAL) Enter the keyword `summary` to view just a summarized version of the Ring configuration.

**Defaults**

No default values or behavior

**Command Modes**

EXEC

**Command History**

- Version 8.2.1.0 Introduced for the C-Series
- Version 7.4.1.0 Introduced
Dell Networking OS Resilient Ring Protocol (FRRP) | 495

Example 1  Figure 18-2.  show frrp summary Command Example

FTOS#show frrp summary

<table>
<thead>
<tr>
<th>Ring-ID</th>
<th>State</th>
<th>Mode</th>
<th>Ctrl_Vlan</th>
<th>Member_Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>UP</td>
<td>Master</td>
<td>2</td>
<td>11-20, 25, 27-30</td>
</tr>
<tr>
<td>31</td>
<td>UP</td>
<td>Transit</td>
<td>31</td>
<td>40-41</td>
</tr>
<tr>
<td>50</td>
<td>Down</td>
<td>Transit</td>
<td>50</td>
<td>32</td>
</tr>
</tbody>
</table>

FTOS#

Example 2  Figure 18-3.  show frrp ring-id Command Example

FTOS#show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary: GigabitEthernet 0/16 State: Forwarding
Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150 msec
Ring Master’s MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009

FTOS#

Example 3  Figure 18-4.  show frrp ring-id summary Command Example

FTOS#show frrp 2 summary

<table>
<thead>
<tr>
<th>Ring-ID</th>
<th>State</th>
<th>Mode</th>
<th>Ctrl_Vlan</th>
<th>Member_Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Up</td>
<td>Master</td>
<td>2</td>
<td>11-20, 25, 27-30</td>
</tr>
</tbody>
</table>

FTOS#

Related Commands

protocol frrp  Enter the Resilient Ring Protocol and designate a ring identification

timer

Set the hello or dead interval for the Ring control packets.

Syntax

timer  {hello-interval milliseconds} | {dead-interval milliseconds}

To remove the timer, use the no timer  {hello-interval milliseconds} | {dead-interval milliseconds} command.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| **hello-interval**
*milliseconds* | Enter the keyword `hello-interval` followed by the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be entered in increments of 50 milliseconds, for example 50, 100, 150 and so on. If an invalid value is entered, an error message is generated. Range: 50 to 2000ms
Default: 500 ms |
| **dead-interval**
*milliseconds* | Enter the keyword `dead-interval` followed by the time, in milliseconds, to set the dead interval of the control packets. Range: 50 to 6000ms
Default: 1500ms
**Note:** The configured dead interval should be at least three times the hello interval |

**Defaults**
Default as shown

**Command Modes**
CONFIGURATION (conf-frrp)

**Command History**
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced for the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**
The hello interval is the interval at which ring frames are generated from the primary interface of the master node. The dead interval is the time that elapses before a timeout occurs.
Dell Networking OS Service Agent

Overview

The Dell Networking OS Service Agent (FTSA), commonly called a call-home service, collects information from the chassis manager, constructs email messages, and sends the messages to the recipients that you configure.

For details on the use of FTSA commands and the structure of FTSA messages, see the Service Agent (FTSA) chapter in the Dell Networking OS Configuration Guide.

All commands in this chapter are supported on C-Series and the E-Series using TeraScale cards. All commands except for three — encrypt, keyadd, and show keys — are supported on E-Series using EtherScale cards. Platform support is indicated by the characters that appear below each command heading — C for C-Series, E for E-Series.

Commands

The FTSA commands are:

- action-list
- admin-email
- call-home
- case-number
- schedule
- seq cli-action
- seq cli-debug
- seq cli-show
- contact-address
- contact-email
- contact-name
- contact-notes
- contact-phone
- dampen
- debug call-home
- default-action
- default-test
- description
- domain-name
- enable
- enable-all
- encrypt
- frequency
- keyadd
- log-messages
- log-only
- match
- message-format
- policy
- policy-action-list
- policy-test-list
- pr-number
- recipient
- run-cpu
- sample-rate
- server
- show configuration
- show debugging
- show keys
- smtp server-address
- test-condition (comparing samples)
- test-condition (comparison to a value)
- test-condition message-text (deprecated)
- test-limit
- test-list
action-list

Specify an action list for the associated policy and enter the conf-call-home-actionlist-name mode.

Syntax

[no] action-list word

Parameters

word Enter the keyword action-list followed by the name of a configured policy action list.

Defaults

none

Command Modes

config-callhome-policy-name

Command History

Version 7.7.1.0 Introduced on C-Series and E-Series

Usage Information

You access this command by first using the policy-action-list command to define a policy-action list name and executing the policy command. Associate this action list to a selected test list through the policy command. When any event occurs that is monitored by the associated test list, the policy invokes the action list that you select here.

Related Commands

default-action Select the information collection action that matches the selected test group.
policy Create a policy with a name and enter config-callhome-policy-name mode.
policy-action-list Name a policy action list and enter the config-callhome-actionlist mode to execute the default-action command.
test-list Enter the name of a configured policy test list.

admin-email

Enter the Administrator email address, the address from which FTSA emails are addressed.

Syntax

admin-email email_address

To remove the Administrator’s email address, use the no admin-email command.

Parameters

email address You have two choices:

- Enter the administrator’s full email address, for example, admin@domain_name.com.
- Enter just the username component, for example, admin.

Defaults

No default behavior or values

Command Modes

CONFIGURATION (conf-callhome)

Command History

Version 7.6.1.0 Introduced for C-Series

Version 6.3.1.0 Introduced for E-Series

Usage Information

The domain name part of the email address can be specified here or by using the command domain-name. In either case, if you specify a domain name by using the domain-name command, that name will be used for the email address instead of a domain name that you might enter here.
**call-home**

This command has two functions:

- Start FTSA.
- Enter the CONFIGURATION (conf-callhome) mode.

**Syntax**

call-home

to stop FTSA, use the no call-home command. Stopping FTSA removes all FTSA configuration from the running configuration.

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION (conf-callhome)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS(conf)#call-home
Apr 28 15:32:21: %RPM1-P:CP %CALL-HOME-3-CALLHOME: Call-home service started
FTOS(conf-callhome)#
```

**Usage Information**

If executing the call-home command starts FTSA (this only happens if FTSA is not already started), Dell Networking OS returns a verification message, and FTSA generates an email message to the default recipient, ftsa@force10networks.com.

If FTSA is already started, executing the call-home command simply puts the user in CONFIGURATION (conf-callhome) mode.

If FTSA is running and the no call-home command is executed, FTSA sends an alert email message to all designated recipients, then stops. The user is returned to CONFIGURATION mode, and Dell Networking OS removes the current FTSA configuration from the running configuration.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>call-home</td>
<td>Start FTSA and Enter the FTSA mode.</td>
</tr>
<tr>
<td>domain-name</td>
<td>Specify the domain name to be used for the Administrator’s email address.</td>
</tr>
<tr>
<td>server</td>
<td>Configure a recipient.</td>
</tr>
<tr>
<td>smtp server-address</td>
<td>Identify the local SMTP (Simple Mail Transfer Protocol) server from which FTSA email messages will be forwarded.</td>
</tr>
<tr>
<td>admin-email</td>
<td>Enter the Administrator’s email address.</td>
</tr>
</tbody>
</table>
case-number

Specify a case number for the associated policy.

**Syntax**

```plaintext
[no] case-number word
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>word</td>
<td>Enter the keyword <code>case-number</code> followed by a case number in the format C-xxxxx or c-xxxxx, where x = 0 to 9. Range: 1 to 20 characters.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

config-callhome-policy-name

**Command History**

- **Version 7.7.1.0**: Introduced on C-Series and E-Series

**Usage Information**

This is an optional command that you access by entering the `policy` command. You would only use this command if there is a TAC case associated with this policy. The specified case number would be returned to the host, if the action list is triggered.

Whatever you enter is saved in the call-home configuration.

**Related Commands**

- `action-list`: Specify a policy action list for the associated policy.
- `policy`: Create a policy with a name and enter config-callhome-policy-name mode.
- `pr-number`: Enter a PR (problem report) number associated with the selected policy.
- `test-list`: Enter the name of a configured policy test list.

---

**schedule**

Executes an action list at the configured time.

**Syntax**

```plaintext
schedule hr:min:sec [once | daily]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hr:min:sec</code></td>
<td>Chassis time specified in hour:minute:second format.</td>
</tr>
<tr>
<td><code>once</code></td>
<td>Executes the action list only once at the configured time.</td>
</tr>
<tr>
<td><code>daily</code></td>
<td>Executes the action list multiple times at the configured time.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

CALL-HOME ACTION-LIST

**Command History**

- **Version 8.2.1.0**: Introduced on C-Series and E-Series.

**Related Commands**

- `action-list`: Specify an action list for the associated policy and enter the conf-call-home-actionlist-name mode.
seq cli-action

Configure an action to execute an Dell Networking OS command for one-time operation, triggered as part of the selected action list.

Syntax

```
seq number cli-action command
```

Parameters

- `seq number`: Use the keyword `seq` followed by a number that Dell Networking OS uses to execute the list of actions in numerical order.
- `command`: Enter a mode command.

Defaults

None

Command Modes

CALL-HOME ACTION-LIST

Command History

- Version 8.2.1.0: Keyword `cli-command` changed to `cli-action`. All options removed. Added keyword `seq`.
- Version 7.8.1.0: Introduced on C-Series and E-Series

Related Commands

- `action-list`: Specify an action list for the associated policy and enter the `conf-call-home-actionlist-name` mode.

seq cli-debug

Configure an action to collect debug information using the designated debug command for the designated time interval.

Syntax

```
seq number cli-debug command time seconds
```

Parameters

- `seq number`: Use the keyword `seq` followed by a number that Dell Networking OS uses to execute the list of actions in numerical order.
- `cli-debug debug-command`: Enter a debug command, but without the initial `debug` keyword. If the debug command has spaces, wrap the command in quotes. Range: 1-100 (max 100 chars including quotes)
- `time seconds`: Enter the keyword `time`, followed by the duration, in seconds, that the debug operation should operate. Range: 1–600 (number of seconds that the operation should operate)

Defaults

None

Command Modes

CALL-HOME ACTION-LIST

Command History

- Version 8.2.1.0: Added keyword `seq`.
- Version 7.8.1.0: Introduced on C-Series and E-Series

Usage

When you enter a debug command, do not repeat the initial `debug` keyword. For example, if the command is `debug cpu-traffic-stats`, enter `cli-debug cpu-traffic-stats`. 
If the debug command has spaces, such as `debug ip bgp events`, put the words following `debug` in double quotes.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action-list</td>
<td>Specify an action list for the associated policy and enter the conf-call-home-actionlist-name mode.</td>
</tr>
</tbody>
</table>

**seq cli-show**

Configure an action to collect the output of the designated `show` command a designated number of times at a designated time interval.

**Syntax**

```
seq number cli-show command repeat number delay seconds
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seq number</code></td>
<td>Use the keyword <code>seq</code> followed by a number that Dell Networking OS uses to execute the list of actions in numerical order.</td>
</tr>
<tr>
<td><code>cli-show</code></td>
<td>Enter the keyword <code>cli-show</code>, followed by a <code>show</code> command. Range: 1-100(max 100 chars including quotes)</td>
</tr>
<tr>
<td><code>command</code></td>
<td>Enter the keyword <code>command</code> after <code>cli-show</code>.</td>
</tr>
<tr>
<td><code>repeat number</code></td>
<td>Enter the keyword <code>repeat</code>, followed by the number of times that the output of the designated <code>show</code> command should be collected. Range: 1–10 (number of times to collect output)</td>
</tr>
<tr>
<td><code>delay seconds</code></td>
<td>Enter the keyword <code>delay</code>, followed by the interval, in number of seconds, to wait in collecting instances of the output of the designated <code>show</code> command. Range: 1–120 (number of seconds to wait between collections)</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

CALL-HOME ACTION-LIST

**Command History**

- **Version 8.2.1.0** Added keyword `seq`.
- **Version 7.8.1.0** Introduced on C-Series and E-Series

**Usage**

If the command has spaces, such as `show processes cpu time`, put the words following `show` in double quotes, as shown in the following example.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action-list</td>
<td>Specify an action list for the associated policy and enter the conf-call-home-actionlist-name mode.</td>
</tr>
</tbody>
</table>
**contact-address**

Enter your customer address (up to 100 characters) to be included in type 5 FTSA messages.

**Syntax**

```
contact-address string
```

**Defaults**

```
one
```

**Command Modes**

```
CALL-HOME
```

**Command History**

```
Version 7.7.1.0    Introduced on C-Series and E-Series
```

**Related Commands**

```
call-home       Start FTSA and enter CONFIGURATION (conf-callhome) mode.
```

**contact-email**

Enter a customer email address (up to 60 characters) to be included in type 5 FTSA messages.

**Syntax**

```
contact-email address
```

**Defaults**

```
one
```

**Command Modes**

```
CALL-HOME
```

**Command History**

```
Version 7.7.1.0    Introduced on C-Series and E-Series
```

**Related Commands**

```
call-home       Start FTSA and enter CONFIGURATION (conf-callhome) mode.
```

**contact-name**

Enter a customer contact name (up to 25 characters) to be included in type 5 FTSA messages.

**Syntax**

```
contact-name name
```

**Defaults**

```
one
```

**Command Modes**

```
CALL-HOME
```

**Command History**

```
Version 7.7.1.0    Introduced on C-Series and E-Series
```

**Related Commands**

```
call-home       Start FTSA and enter CONFIGURATION (conf-callhome) mode.
```
contact-notes

Enter comments (up to 100 characters) to be included in the configuration database and in type 5 FTSA messages.

Syntax  contact-notes string

Defaults none

Command Modes CALL-HOME

Command History

Version 7.7.1.0 Introduced on C-Series and E-Series

Related Commands call-home Start FTSA and enter CONFIGURATION (conf-callhome) mode.

contact-phone

Enter a customer phone number (up to 50 characters) to be included in type-5 FTSA messages.

Syntax  contact-phone number

Defaults none

Command Modes CALL-HOME

Command History

Version 7.7.1.0 Introduced on C-Series and E-Series

Related Commands call-home Start FTSA and enter CONFIGURATION (conf-callhome) mode.

dampen

Set a delay before sampling for a test condition again after it has been matched.

Syntax  dampen number

Parameters

number Enter the number of minutes for FTSA to wait before sampling a test condition again after it has been matched.

Range: 1–1440

Defaults 5 minutes

Command Modes CALL-HOME POLICY

Command History

Version 7.8.1.0 Introduced on C-Series and E-Series

Related Commands policy Create a policy with a name and enter config-callhome-policy-name mode.
**debug call-home**

Monitor FTSA email messages through the CLI.

**Syntax**

ddebug call-home

To turn message monitoring off, use the no debug call-home command.

**Defaults**

no debug call-home

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

show debugging Display the status of FTSA (call-home) debugging.

**default-action**

Select the information collection action that matches the equivalent test group.

**Syntax**

default-action {hardware | software | exception}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hardware</td>
<td>Enter the keyword hardware to collect hardware information. See the Dell Networking OS Configuration Guide for the list of actions executed by this keyword.</td>
</tr>
<tr>
<td>software</td>
<td>Enter the keyword software to collect software information. See the Dell Networking OS Configuration Guide for the list of actions executed by this keyword.</td>
</tr>
<tr>
<td>exception</td>
<td>Enter the keyword exception to collect exception information. See the Dell Networking OS Configuration Guide for the list of actions executed by this keyword.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Mode**

CALL-HOME ACTION-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Starting with Dell Networking OS 7.8.1.0, after you use the policy-test-list and default-list commands to put you in the config-callhome-actionlist mode, you can use the default-action command to select any test group.

The FTSA message (or log entry) contains the information collected by the selected action.

**Related Commands**

policy-action-list This command names the policy action list and enters the config-callhome-actionlist-name mode.
## default-test

Invoke one of three preset system-monitoring test groups.

**Syntax**

```
default-test {hardware | software | exception}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hardware</strong></td>
<td>Enter the keyword <code>hardware</code> to monitor hardware conditions. See the Dell Networking OS Configuration Guide for the list of conditions monitored by this keyword.</td>
</tr>
<tr>
<td><strong>software</strong></td>
<td>Enter the keyword <code>software</code> to monitor software conditions. See the Dell Networking OS Configuration Guide for the list of conditions monitored by this keyword.</td>
</tr>
<tr>
<td><strong>exception</strong></td>
<td>Enter the keyword <code>exception</code> to monitor the exceptions events. See the Dell Networking OS Configuration Guide for the list of conditions monitored by this keyword.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Mode**

CALL-HOME TEST-LIST

**Command History**

Version 7.7.1.0 Introduced on C-Series and E-Series

**Usage Information**

Executing the `policy-test-list` command puts you in the config-callhome-testlist mode, where you use this command to invoke one of three possible test groups. Dell Networking OS monitors the system for any event in the selected test group. If such an event occurs, Dell Networking OS invokes the action you define using the `default-action` command.

**Related Commands**

- `default-action` Select the information collection action that matches the selected test group.
- `policy-test-list` Name a new or existing test list and enter the config-callhome-testlist-name mode.

## description

Enter a description for the Call Home mode.

**Syntax**

```
description {description}
```

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>description</strong></td>
<td>Enter a description to identify the Call Home mode (80 characters maximum).</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

CONFIGURATION-CALLHOME

**Command History**

pre-7.7.1.0 Introduced

**Related Commands**

- `call-home` Enter the Call Home mode on the switch.
domain-name

Specify the domain name for the Administrator’s email address.

Syntax

```
domain-name domain_name
```

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>Enter the keyword domain-name followed by the complete domain name of the Administrator’s email address, for example, domain_name.com.</td>
</tr>
</tbody>
</table>

Defaults

The domain name specified in the admin-email command

Command Modes

CONFIGURATION (conf-callhome)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

Usage Information

If you use this command to specify a domain name, that domain name is used instead of any domain name that you might have specified using the admin-email command.

Related Commands

- admin-email: Enter the Administrator’s email address.
- call-home: Start FTSA and Enter the FTSA mode.

enable

Enable the sending of FTSA email messages to the selected recipient.

Syntax

```
enable
```

To disable (end) the sending of FTSA email messages to the selected recipient, use the no enable command.

Defaults

no enable

Command Modes

conf-callhome

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

Usage Information

If you leave the selected recipient in the default condition of disabled (no FTSA email messages to the selected recipient), you can either come back to this command later, or you can use the enable-all command. If you use the enable-all command, you can then disable email messages to the recipient with the no enable command at the server-specific prompt.

FTSA sends an email notification to the selected recipient whenever the enable status changes.

Note: Execute the enable command only after the SMTP and admin-email commands are executed.
enable-all

Enable (start) the sending of FTSA email messages to all designated recipients.

Syntax

```
enable-all
```

To disable (end) the sending of FTSA email messages to all designated recipients, use the `no enable` command.

Defaults

```
no enable-all
```

Command Modes

```
CONFIGURATION (conf-callhome)
```

Command History

```
Version 7.6.1.0  Introduced on C-Series

Version 6.3.1.0  Introduced for E-Series
```

Usage Information

FTSA sends an email notification to all designated recipients whenever the enable-all status changes.

Note: Execute the `enable-all` command only after the `SMTP` and `admin-email` commands are executed.

Related Commands

```
admin-email  Specify the Administrator’s email address.

call-home    Start FTSA and Enter the FTSA mode.

smtp server-address  Configure the SMTP server detail.
```

encrypt

Specify email encryption for this server.

Syntax

```
encrypt
```

To remove email encryption for this server, use the `no encrypt` command.

Defaults

```\nno encrypt
```

Command Modes

```
CONFIGURATION Server (conf-callhome-server_name)
```

Command History

```
Version 7.6.1.0  Introduced on C-Series

Version 6.3.1.0  Introduced for E-Series
```
Encryption is supported through PGP (Pretty Good Privacy). Encryption cannot be enabled without a public key for the server. On E-Series chassis, this command is only supported for TeraScale cards.

**Note:** Execute the `encrypt` command only *after* the `keyadd` command is executed.

### frequency

Select the interval (frequency) with which email FTSA messages are sent to all designated recipients.

#### Syntax

`frequency minutes`

To return to the default frequency, use the `no frequency` command.

#### Parameters

- `minutes`: Enter the time interval, in minutes, that you want between FTSA status emails.
  - Range: 2 to 10080 minutes
  - Default: 1440 minutes (24 hours)

#### Defaults

1440 minutes (24 hours)

#### Command Modes

CONFIGURATION (conf-callhome)

#### Command History

- **Version 7.6.1.0** Introduced on C-Series
- **Version 6.3.1.0** Introduced for E-Series

#### Usage Information

The frequency is immediately set once the `frequency` command is executed. For example, if you set the frequency to 120 minutes, the 120 minutes begins as soon as the command is executed. In this example, email messages will be sent to all designated recipients exactly two hours after executing the command.

#### Related Commands

- `call-home`: Start FTSA and Enter the FTSA mode.

### keyadd

Add the public encryption key (PGP5-compatible) for a specific recipient if you want to encrypt messages sent to that recipient.

#### Syntax

`keyadd public_key`

To remove the public key, use the `no keyadd public_key` command.

#### Parameters

- `public_key`: Enter the local source and filename of the public key (must be PGP5 compatible) created for the selected recipient, such as `keyadd flash:///mykey`
Defaults
No default behavior or values

Command Modes
CONFIGURATION Server (conf-callhome-server_name)

Command History
Version 7.6.1.0 Introduced on C-Series
Version 6.3.1.0 Introduced for E-Series

Usage Information
The Dell Networking server associated with the default Dell Networking Support recipient has a public key that is shipped as part of Dell Networking OS, so you do not need to enter the key’s filename for that server. However, if the Dell Networking public key is changed, a notification will be made to download the new key from the Dell Networking website and to replace the old key with that new key. Also, if you set up other recipients, use this command to enter their key filenames.

On E-Series chassis, this command is only supported for TeraScale cards.

Note: Execute the encrypt command after the keyadd command to ensure email encryption.

Related Commands
call-home Start FTSA and Enter the FTSA mode.
encrypt Enable email encryption.
server Configure recipients.
show keys Display the email encryption (PGP) keys.

log-messages
This command collects information from the chassis.

Syntax
[no] log-messages [delay 60–1440] [severity 0–7] [filter word]

Parameters
delay 60–1440 (OPTIONAL) Enter the keyword delay followed by the number of minutes to delay from the time of invoking the command after which FTSA will accumulate system log messages into a message.
severity 0–7 (OPTIONAL) Enter the keyword severity followed by the error severity level entered in the system log that should be collected into the FTSA message.
filter word (OPTIONAL) Enter the keyword filter followed by a character string that FTSA should use to search the system log. A search string containing spaces must be in quotes. If the search yields a positive result, FTSA will send a log message with the string included.

Defaults delay = 1440 minutes; severity = 7; filter = no

Command Modes conf-callhome

Command History
Version 7.7.1.0 Introduced on C-Series and E-Series

Usage Information
Each of the three command parameters are optional and can be entered in any order, individually or in combination.
The default severity level of 7 is the recommended severity level. Lower values will result in partial log data sent to the server because messages with higher values are filtered out.

The log-only command is used to collect and save data locally. The command is used in conjunction with the default-action command.

**Syntax**

```
[no] log-only
```

**Defaults**

```
“no log-only”
```

**Command Modes**

```
conf-callhome-actionlist-name
```

**Command History**

```
Version 7.7.1.0 Introduced on C-Series and E-Series
```

**Usage Information**

If you execute this command, data gathered by the action list invoked by the default-action command will be saved in a local file. The file will have the same name as the action list and with a time stamp appended to the file name.

When saved in flash, the file name format is:

```
flash://<actionlistName>-<timestamp>.ftsa
```

For example:
```
flash://hardwareAction-02_16_34 423.ftsa
```

Because the time stamp makes each file unique, files will not be overwritten if the action list executes more than once. If this log-only command is not executed, or if no log-only option is executed, then the collected data will be sent in an FTSA email.

When sent as an email attachment, the file name format is:

```
<actionlistName>-<timestamp>.txt
```

For example:
```
hardwareAction-02_16_34 423.txt
```

If the collected data is split due to a size limit, a sequential version number will be added to it.

For example:
```
hardwareAction-02_16_34 423_0.txt
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>call-home</td>
<td>Start FTSA and Enter the FTSA mode.</td>
</tr>
<tr>
<td>log-only</td>
<td>Select the information collection action that matches the selected test group.</td>
</tr>
<tr>
<td>logging buffered</td>
<td>Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.</td>
</tr>
<tr>
<td>show logging</td>
<td>Display the logging settings and system messages logged to the internal buffer of the switch.</td>
</tr>
<tr>
<td>default-action</td>
<td>Select the information collection action that matches the selected test group.</td>
</tr>
</tbody>
</table>
match
This command enables you to execute the configured action list based on one of three test list criteria.

Syntax
match {any | all | simultaneous}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Entering this keyword will cause a match for any item in the test list to execute the associated action list. This is the default option.</td>
</tr>
<tr>
<td>all</td>
<td>Entering this keyword will require that all conditions in the test list be matched in order to execute the associated action list.</td>
</tr>
<tr>
<td>simultaneous</td>
<td>Entering this keyword indicates that the test conditions must be matched in the same sampling period in order to execute the associated action list.</td>
</tr>
</tbody>
</table>

Default
match any

Command Mode
config-callhome-testlist-name

Command History

| Version 7.8.1.0 | Introduced on C-Series and E-Series |

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td>Create a policy with a name and enter config-callhome-policy-name mode.</td>
</tr>
<tr>
<td>policy-test-list</td>
<td>Name a policy test list and enter the config-callhome-actionlist-name mode.</td>
</tr>
</tbody>
</table>

message-format
Set the format of an action-list (type-5) email message.

Syntax
message-format {xml | text}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xml</td>
<td>Enter the keyword xml to have the type-5 mail generated in XML format.</td>
</tr>
<tr>
<td>text</td>
<td>Enter the keyword text to have the type-5 mail generated in text format.</td>
</tr>
</tbody>
</table>

Default
xml

Command Modes
config-callhome-actionlist-name

Command History

| Version 7.8.1.0 | Introduced on C-Series and E-Series |

Usage Information
A type-5 message emails the output gathered by an action list. The attachment for the Type 5 message contains the output of a single execution of a single action list, as well as the content of the main message.

The example, below, shows generally how a type-5 message would look formatted in XML.
Example

```
<action_list_message>
  <AgentInfo>
    <messagetype>Type - 5</messagetype>
    <time>Oct 18 15:05:34.699 UTC</time>
    <serialnum>E000000001664</serialnum>
  </AgentInfo>

  <contact_info>
    <contact-name>name</contact-name>
    <contact-email>email</contact-email>
    <contact-phone>phone</contact-phone>
    <contact-address>address</contact-address>
    <contact-notes>notes</contact-notes>
  </contact_info>

  <policy_name>xxxxxxxx</policy_name>
  <case_number>xxxxx</case_number>
  <pr_number>xxxxx</pr_number>

  <F10_info>
    <policy_name>xxxxxxx</policy_name>
    <case_number>xxxxx</case_number>
    <pr_number>xxxxx</pr_number>
  </F10_info>

  <action_list_name>name</action_list_name>
  <test_list_match>
    <match>keyword : value</match>
    <match>cpu-5-min: 98%</match>
    etc...
  </test_list_match>

  <content>
    <item>
      <item_name>show pcdfo</item_name>
      <item_time>Oct 18 15:05:34.699 UTC</item_time>
      <item_output>xxx...</item_output>
    </item>
    <item>
      <item_name>debug-cpu-traffic-stats</item_name>
      <item_time>Oct 18 15:05:35.288 UTC</item_time>
      <item_output>xxx...</item_output>
    </item>
    etc...
  </content>
</action_list_message>
```

Related Commands

| action-list | Specify a policy action list for the associated policy and enter the conf-call-home-actionlist-name mode. |

policy

Create a policy with a name and enter config-callhome-policy-name mode. In that mode, you can create a case number identifier to be matched with a test list and action.

Syntax

```
[no] policy word
```

Parameters

- **word** Enter a name (up to 20 characters) for the new policy.

Defaults

No default behavior or values

Command Modes

conf-callhome

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Concurrent policies changed from three to five</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>
You can create up to five concurrent policies with this command. A policy is the association of a test
list with an action list, and optionally a case number. Choose the test list (the type of monitoring to
perform) with the `policy-test-list` command. Choose the associated action to perform with the
`policy-action-list` command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>call-home</code></td>
<td>Start FTSA and Enter the FTSA mode.</td>
</tr>
<tr>
<td><code>case-number</code></td>
<td>Specify a case number for the associated policy</td>
</tr>
<tr>
<td><code>default-test</code></td>
<td>Invoke one of three system-monitoring test groups.</td>
</tr>
<tr>
<td><code>policy-action-list</code></td>
<td>Name a policy action list and enter the config-callhome-actionlist-name mode.</td>
</tr>
<tr>
<td><code>policy-test-list</code></td>
<td>Name a policy test list and enter the config-callhome-testlist-name mode.</td>
</tr>
<tr>
<td><code>pr-number</code></td>
<td>Create an entry for a PR number in policy mode. The PR number is the issue identifier (bug ID) maintained by Dell Networking, and is associated with the test list.</td>
</tr>
<tr>
<td><code>test-list</code></td>
<td>Enter the name of a configured policy test list to be associated with the selected policy.</td>
</tr>
</tbody>
</table>

### policy-action-list

Name a policy action list and enter the `config-callhome-actionlist-name` mode to enter commands that will execute actions based on test results.

**Syntax**

```
policy-action-list word
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>word</code></td>
<td>Enter the name (up to 20 characters) of the new policy test list.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

`conf-callhome`

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on C-Series and E-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Version 7.7.1.0 Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Capturing events with FTSA requires two parallel configurations. You choose the type of testing (monitoring) to perform with the `policy-test-list` command. You choose the action to perform when an event occurs by using this command and then action selection commands, such as `default-action`.

### policy-test-list

Name a policy test list and enter the `config-callhome-testlist-name` mode.

**Syntax**

```
policy-test-list word
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>word</code></td>
<td>Enter the name (up to 20 characters) of the new policy test list.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Mode**

`conf-callhome`

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on C-Series and E-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Version 7.7.1.0 Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Capturing events with FTSA requires two parallel configurations. You choose the type of testing (monitoring) to perform with the `policy-test-list` command. You choose the action to perform when an event occurs by using this command and then action selection commands, such as `default-action`. 
After you name the test list with this command, use the command such as `default-test` to choose the type of monitoring to perform.

### pr-number

**Syntax**

```
pr-number number
```

**Parameters**

- `number` Enter a 5-digit PR number, as supplied by Dell Networking.

**Defaults**

none

**Command Mode**

config-callhome-policy-name

**Command History**

Version 7.8.1.0 Introduced on C-Series and E-Series

**Related Commands**

- `case-number` Specify a case number for the associated policy.
- `policy` Create a policy with a name and enter config-callhome-policy-name mode.
- `policy-test-list` Name a policy test list and enter the config-callhome-actionlist-name mode.

### recipient

Enter the email address of the recipient associated with the selected server name.

**Syntax**

```
recipient email address
```

**Parameters**

- `email address` Enter the recipient’s full email address. For example, `name@domain_name.com`.

**Defaults**

ftsa@force10networks.com (associated with the Dell Networking server only)

**Command Mode**

CONFIGURATION Server (conf-callhome-server_name)

**Command History**

Version 7.6.1.0 Introduced on C-Series

Version 6.3.1.0 Introduced for E-Series

**Usage Information**

After using the `server` command to create a server name, you are placed at that server-specific prompt, where you can use this command to enter the email address of the recipient that you want to associate with that server name.

**Related Commands**

- `call-home` Start FTSA and Enter the FTSA mode.
run-cpu

Set whether the action list associated with the selected test list should be executed, as a function of CPU utilization.

Syntax

```
run-cpu {cpu | rpm-any} {less-than | greater-than} percentage
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>percentage</strong></td>
<td>Enter a CPU utilization percentage.</td>
</tr>
<tr>
<td></td>
<td>Range: 0–100</td>
</tr>
<tr>
<td><strong>cpu</strong></td>
<td>Select a CPU: CP, LP, RP1, or RP2</td>
</tr>
<tr>
<td><strong>rpm-any</strong></td>
<td>Monitor all RPM CPUs for the run-cpu condition (CP, RP1, and RP2)</td>
</tr>
</tbody>
</table>

Default

None

Command Mode

CALL-HOME POLICY

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Added variable cpu, and keyword rpm-any. Keyword more-than changed to greater-than. Keyword unconditional removed.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

Usage

The purpose of this command is to determine whether the action list associated with this test list should be executed, depending on whether the CPU utilization at the time the test list is executed meets the configured parameter:

- If **less-than** is configured, the user might be worried about executing the action list in high CPU usage conditions. In such a case, for example, the user might configure `run-cpu less-than 90`. When a match is made to the test list, the CPU 1-minute average is checked and if it is 85%, for example, then the associated action list will be executed. If the current CPU usage is at 90% or greater, the action list will not be executed. In this case, FTSA logs this in the syslog to note that a match was made, what the match was, and that the action list was not executed because CPU was too high.

- If **greater-than** is configured, it is probably because the user does not care about results that may occur when CPU usage is low. For example, a user might configure `run-cpu greater-than 60`. If a match is found for the test list and the 1-minute CPU average is 40%, then the action list is not executed; if it is 61% or greater, then it is executed.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td>Create a policy with a name and enter config-callhome-policy-name mode.</td>
</tr>
</tbody>
</table>

sample-rate

Set the sampling interval for how often to execute the configured test condition.

Syntax

```
sample-rate number
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
<td>Set the sampling interval for how often to execute the configured test condition.</td>
</tr>
<tr>
<td></td>
<td>Range: 1–1440 (minutes)</td>
</tr>
</tbody>
</table>

Default

1 (one minute)
Use this command to create a server name to be associated with a particular recipient.

**server**

**Syntax**

```
server name
```

To remove a server and the associated recipient, use the `no server name` command.

**Parameters**

- **name**: Enter the name of the server in alphanumeric format, up to 25 characters long.

**Defaults**

Dell Networking OS

**Command Mode**

CONFIGURATION Server (conf-callhome)

**Command History**

- **Version 7.6.1.0**: Introduced on C-Series
- **Version 6.3.1.0**: Introduced for E-Series

**Example**

```
FTOS(conf-callhome)#
FTOS(conf-callhome)#server freedom_bird
FTOS(conf-callhome-freedom_bird)#?
```

**Usage**

The Dell Networking server name is configured for FTSA messages to be sent by default to Dell Networking Support at ftsa@force10networks.com. If you want to change that address, enter the command `server Dell Networking OS`. You will be placed at that server-specific prompt (conf-callhome-FTOS), where you would then use the `recipient` command to enter a new address.

In addition to modifying the Dell Networking server recipient, you can identify up to four more server names and associated recipients.
If you want to use encryption for a particular recipient’s email messages, the server name must match the user ID that is in the encryption file that the recipient will use to decrypt the messages. Use the `keyadd` command to designate the encryption file.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>call-home</td>
<td>Start FTSA and Enter the FTSA mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enable FTSA (call home) email for the selected recipient.</td>
</tr>
<tr>
<td>recipient</td>
<td>Enter the recipient’s email address.</td>
</tr>
<tr>
<td>enable</td>
<td>Enable FTSA (call home) email for the selected recipient.</td>
</tr>
</tbody>
</table>

**show configuration**

Display the FTSA (call-home) configuration.

**Syntax**

`show configuration`  

**Defaults**

No default behavior or values  

**Command Mode**

CONFIGURATION (conf-callhome)  

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

FTOS(conf-callhome)#show configuration

```
! call-home
    admin-email traza
    domain-name force10networks.com
    smtp server-address 10.0.2.6
    no enable-all
    server FTOS
    recipient ftsa@force10networks.com
    keyadd Force10DefaultPublicKey
    no encrypt
    enable
```

FTOS(conf-callhome)#

**show debugging**

Display the status of FTSA (call-home) debugging.

**Syntax**

`show debugging`  

**Defaults**

No default behavior or values  

**Command Mode**

CONFIGURATION (conf-callhome)  

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
**show keys**

Display the email encryption (PGP) keys. On E-Series chassis, this command is only supported for TeraScale cards.

**Syntax**

`show keys`

**Defaults**

No default behavior or values

**Command Mode**

CONFIGURATION (conf-callhome)

**Command History**

- Version 8.4.1.0 Added support to resolve domain names to IPv6 addresses.
- Version 7.6.1.0 Introduced on C-Series
- Version 6.3.1.0 Introduced for E-Series

**Example**

**Figure 19-4. show keys Command Example**

```
FTOS(conf-callhome)#show keys
Type Bits KeyID      Created    Expires    Algorithm       Use
sec+  768 0x64CE09D9 2005-06-27 ---------- RSA             Sign & Encrypt
uid  E000000003209
pub  1024 0xA8E48C2F 2004-12-08 ---------- DSS             Sign & Encrypt
sub  1024 0xD832BB91 2004-12-08 ---------- Diffie-Hellman
uid  FTOS
2 matching keys found
FTOS(conf-callhome)#
```

**Related Commands**

- `debug call-home` Monitor FTSA email messages through the CLI.

- `call-home` Start FTSA and Enter the FTSA mode.

- `encrypt` Enable email encryption.

- `keyadd` Add the server public key for encryption.
smtp server-address

Identify the local SMTP (Simple Mail Transfer Protocol) server from which FTSA email messages will be forwarded.

Syntax

```
smtp server-address server-address [smtp-port port number]
```

To remove the SMTP address, use the no smtp server-address command. This action will disable email messaging until you enter a new SMTP server address.

Parameters

- **server-address** server address: Enter the keyword server-address followed by the SMTP server address, such as smtp.yourco.com. The domain name you specify can be resolved into an IPv4 or IPv6 address.

- **smtp-port** port number: Optionally, enter the keyword smtp-port followed by the SMTP port number. Range: 0 to 65535

Defaults

SMTP port = 25

Command Mode

CONFIGURATION (conf-callhome)

Command History

- Version 7.6.1.0 Introduced on C-Series
- Version 6.3.1.0 Introduced for E-Series

Usage Information

The switch only plays the part of an SMTP client to send email messages to the SMTP server designated here. This SMTP server is required in order to receive the email messages and forward them to local and remote designated recipients. The default port number on an SMTP server is 25. If a host name is given (instead of an IP address), DNS should be enabled to resolve the host name.

Related Commands

- admin-email: Specify the Administrator’s email address.
- enable: Enable FTSA email messages for the selected recipient.
- enable-all: Enable FTSA email messages for all designated recipients.
test-condition (comparing samples)

Configure an action to collect and compare multiple samples of a statistic.

Syntax

```
setup-condition statistic operator sample {cpu | rpm-any} number
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-condition</td>
<td>Enter the keyword test-condition, followed by one of the following statistic request types:</td>
</tr>
<tr>
<td>statistic</td>
<td>Enter the keyword statistic, followed by one of the following statistic request types:</td>
</tr>
<tr>
<td>operator</td>
<td>Enter one of the following Boolean comparison operators: decrease, equal-to, greater-than, increase, less-than, not-equal-to, no-change.</td>
</tr>
<tr>
<td>sample number</td>
<td>Enter the keyword sample, followed by an integer representing the number of the sample collected. For example, 5 is the fifth sample collected, so the first and fifth samples would be compared, using the designated operator.</td>
</tr>
<tr>
<td>number</td>
<td>Range: 2–100 Default: 2</td>
</tr>
<tr>
<td>cpu</td>
<td>rpm-any</td>
</tr>
</tbody>
</table>

Defaults

None

Command Mode

CALL-HOME TEST-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Removed message-text keyword. Added operators.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

Usage Information

FTSA avoids false triggers when a counter rolls over by ignoring the first sample taken after a rollover.

Also, FTSA does not allow you to configure a test that makes no sense because of a comparator that is out of range. For example, by entering `cpu-5-min increase number 150`, you would be looking for a difference between two CPU percentage utilization samples of at least 150. 150 is not possible, because percentage utilization can only go up to 100, so FTSA displays the acceptable range, as shown below, and will issue an error message if you try to enter a value that is out of range.
In this next example, the configuration is to subtract the bit rate that was found in the second sample from the bit rate found in the first sample. If the difference is at least 10Mb, then any associated action list will be invoked.

FTOS(conf-call-home-testlist-test)#test-condition cpu-1-min increase number 80
sample 5

FTOS(conf-callhome-testlist-test)#test-condition cpu-5-min decrease 10

Here are other examples of test-condition configuration statements.

FTOS(conf-call-home-testlist-test)#test-condition interface-bit-rate input 1 decrease 10 sample 2

Related Commands

dampen  Set a delay before sampling for a test condition again after it has been matched.

test-limit  Set the number of times that the test list that should be executed.

test-condition  (comparing samples)  Collect multiple samples of a statistic and compare them using the specified comparator and hurdle value.

test-condition  (comparison to a value)  Collect a sample of a designated statistic and then compare it to the designated number.

test-condition (comparison to a value)

Configure an action to collect a sample of a designated statistic and then use the designated Boolean comparator to compare it to the designated value. When this configuration is associated with an action list, a result outside of the acceptable limit will trigger the action list.

Syntax  test-condition statistic operator number {cpu | rpm-any} value
Parameters

- **test-condition statistic** Enter the keyword `test-condition`, followed by one of the following statistic request types:
  - `cpu-1-min`: Average CPU utilization for 1 minute
  - `cpu-5-min`: Average CPU utilization for 5 minutes
  - `interface-bit-rate input output slot#`: Instantaneous bit rate on a given line card
  - `interface-crc interface`: Number of CRC errors on a given interface
  - `interface-rate interface`: Packet rate on a given interface
  - `interface-throttles interface`: Number of throttles on an interface
  - `memory-free`: Free system memory
  - `memory-free-percent`: Free system memory free in percentage
  - `memory-used`: System memory used
  - `memory-used-percent`: System memory used in percentage
  - `wred-drops interface`: Number of WRED drops on an interface (E-Series only)

- **operator** Enter one of the following Boolean comparison operators: `decrease`, `equal-to`, `greater-than`, `increase`, `less-than`, `not-equal-to`, `no-change`.

- **number value** Enter the keyword `number`, followed by an integer to be the comparison value to the designated statistic, in the range pertinent to the statistic.

- **cpu | rpm-any** Enter the processor that will be tested: `cp`, `lp`, `rp1`, `rp2`, or test all RPM CPUs with the keyword `rpm-any`.

Defaults

None

Command Mode

CALL-HOME TEST-LIST

Command History

- **Version 8.2.1.0** Removed `message-text` keyword. Added operators.
- **Version 7.8.1.0** Introduced on C-Series and E-Series

Usage Information

Dell Networking OS does not allow you to configure a test that makes no sense, such as `cpu-5-min greater-than number 150`. CPU percentage utilization can only go up to 100, so 150 is not possible. Dell Networking OS displays the acceptable range, as shown below.

Examples

```
FTOS(conf-call-home-testlist-test)#test-condition cpu-5-min greater-than ?
number                  The boolean comparison value
FTOS(conf-call-home-testlist-test)#test-condition cpu-5-min greater-than number ? <0-100> Enter the boolean comparison value
FTOS(conf-callhome-testlist-test)#test-condition cpu-5-min greater-than number 10
```

This example shows a couple other `keyword` configuration examples.

```
FTOS(conf-call-home-testlist-test)# test-condition interface-rate input 1 less-than number 98
FTOS(conf-call-home-testlist-test)# test-condition memory-used not-equal-to number 1000
```

Related Commands

- **dampen** Set a delay before sampling for a test condition again after it has been matched.
- **test-limit** Set the number of times that the test list that should be executed.
**test-condition message-text (deprecated)**

Configure a search for a stated value in the output of the designated `show` command or message type — syslog or other error messages, sent to the console, trap, or message logged locally. This applies only to messages logged by Dell Networking OS.

### Syntax

```
test-condition message-text command string equal-to string string
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-condition</td>
<td>Enter the keywords test-condition <code>message-text command</code>, and then for <code>string</code>, enter a <code>show</code> command in quotes.</td>
</tr>
<tr>
<td>message-text</td>
<td>and then for <code>string</code>, enter the text to search for in the show command designated above.</td>
</tr>
<tr>
<td>command string</td>
<td>Range: 1–64 characters</td>
</tr>
<tr>
<td>equal-to string</td>
<td>Enter the keywords <code>equal-to string</code>, and then for <code>string</code>, enter the text to search for in the show command designated above.</td>
</tr>
<tr>
<td>string</td>
<td>Range: 1–64 characters</td>
</tr>
</tbody>
</table>

### Defaults

```
none
```

### Command Modes

```
conf-callhome-testlist-test
```

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

- The search string can be used for both “display xml” and normal “show command” output.
- The search string is `<ifAdminStatus>down</ifAdminStatus>.

Note that the search target, in this example, is enclosed within double quotes. If either string contains spaces, it must be enclosed in quotes or it will be truncated at the first whitespace.

The search string is compared against an entire text message, so a short string, such as the number zero, is likely to produce many unintended matches. Therefore, the search string should be as long as possible to guarantee as close a match as possible to the data that you want to match. However, the maximum length of a string is 64 characters.
Example

Example FTOS(conf-callhome-testlist-test)#test-condition message-text ?
command Enter the show command
FTOS(conf-callhome-testlist-test)#test-condition message-text command ?
WORD Enter the show command
FTOS(conf-callhome-testlist-test)#test-condition message-text command “show
interfaces gi 1/0 | display xml” ?
equal-to Keyword boolean value equal to
FTOS(conf-callhome-testlist-test)#test-condition message-text command “show
interfaces gi 1/0 | display xml” equal-to ?
string Enter the search string pattern
FTOS(conf-callhome-testlist-test)#test-condition message-text command “show
interfaces gi 1/0 | display xml” equal-to string ?
LINE Regular expression
FTOS(conf-callhome-testlist-test)#test-condition message-text command “show
interfaces gi 1/0 | display xml” equal-to string <ifAdminStatus>down</
ifAdminStatus>

Related
Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dampen</td>
<td>Set a delay before sampling for a test condition again after it has been matched.</td>
</tr>
<tr>
<td>test-condition (comparing samples)</td>
<td>Configure an action to collect and compare multiple samples of a statistic.</td>
</tr>
<tr>
<td>test-condition (comparison to a value)</td>
<td>Collect a statistic and compare it to a stated value.</td>
</tr>
<tr>
<td>test-limit</td>
<td>Set the number of times that the test list that should be executed.</td>
</tr>
</tbody>
</table>
test-limit

Set the number of times that the test list should be executed.

Syntax

```
test-limit number
```

Parameters

- `number`: Set the number of times the test list matches that should be attempted.
  Range: 0–256

Default

none. If the `test-limit` number is removed or not configured, there is no limit for how many times to test for the condition.

Command Mode

conf-callhome-policy

Command History

- **Version 7.8.1.0**: Introduced on C-Series and E-Series

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dampen</td>
<td>Set a delay before sampling for a test condition again after it has been matched.</td>
</tr>
<tr>
<td>test-condition</td>
<td>Configure an action to collect and compare multiple samples of a statistic.</td>
</tr>
<tr>
<td>(comparing samples)</td>
<td></td>
</tr>
<tr>
<td>policy</td>
<td>Create a policy with a name and enter config-callhome-policy-name mode.</td>
</tr>
<tr>
<td>policy-test-list</td>
<td>Name a policy test list and enter the config-callhome-actionlist-name mode.</td>
</tr>
<tr>
<td>sample-rate</td>
<td>Set the sampling interval for how often to execute the configured test condition.</td>
</tr>
</tbody>
</table>
test-list

Enter the name of a configured test list to be associated with the selected policy.

Syntax

test-list word

Parameters

word Enter the keyword test-list followed by the name of a configured test list.

Defaults

No default behavior or values

Command Mode

cfg-call-home-policy-name

Command History

Version 7.7.1.0 Introduced on C-Series and E-Series

Usage Information

Executing the policy-test-list command puts you in the config-callhome-testlist mode, where you use this command to invoke one of three possible test groups. Dell Networking OS monitors the system for any event in the selected test group. If such an event occurs, Dell Networking OS invokes the action you defined using the default-action command and then associate in this policy with the action-list command.

Table 19-1. FTSA Test Sets

<table>
<thead>
<tr>
<th>Hardware test set</th>
<th>Software test set</th>
<th>Exception test set</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFM status transition from active to other state</td>
<td>SWP Timeout</td>
<td>CPU usage more than 85%</td>
</tr>
<tr>
<td>Line card transition from active to other state</td>
<td>IPC Timeout</td>
<td>System crash</td>
</tr>
<tr>
<td>Port-pipe error or transition to down</td>
<td>IRC Timeout</td>
<td>Task crash</td>
</tr>
<tr>
<td>RPM status transition from active to other state</td>
<td>CPU usage more than 85%</td>
<td>Dump, reload due to error, RPM failover due to error</td>
</tr>
<tr>
<td>PEM transition from up to other state</td>
<td>Memory usage more than 85%</td>
<td></td>
</tr>
<tr>
<td>AC power supply transition from up to other state</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan tray down or individual fan down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overtemp of any item listed in show environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over/under-voltage of any item listed in show environment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action-list</td>
<td>Specify a policy action list for the associated policy and enter the conf-call-home-actionlist-name mode.</td>
</tr>
<tr>
<td>case-number</td>
<td>Specify a case number for the associated policy.</td>
</tr>
<tr>
<td>dampen</td>
<td>Set a delay before sampling for a test condition again after it has been matched.</td>
</tr>
<tr>
<td>policy</td>
<td>Create a policy name and enter config-callhome-policy-name mode.</td>
</tr>
<tr>
<td>policy-test-list</td>
<td>Name a policy test list and enter the config-callhome-testlist-name mode.</td>
</tr>
</tbody>
</table>
GARP VLAN Registration (GVRP)

Overview

GARP VLAN Registration (GVRP) is supported on platforms C, E, and S.

Commands

The GVRP commands are:

- bpdu-destination-mac-address
- clear gvrp statistics
- debug gvrp
- disable
garp timers
gvrp enable
gvrp registration
protocol gvrp
- show config
- show garp timers
- show gvrp
- show gvrp statistics on page 27

The GARP (Generic Attribute Registration Protocol) 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 local 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 NICs.
- Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecifed) 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.

bpdu-destination-mac-address

Use the Provider Bridge Group address in Spanning Tree or GVRP PDUs.

Syntax

bpdu-destination-mac-address [stp | gvrp] provider-bridge-group

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stp</td>
<td>Force STP, RSTP, and MSTP to use the Provider Bridge Group address as the destination MAC address in its BPDUs.</td>
</tr>
<tr>
<td>gvrp</td>
<td>Forces GVRP to use the Provider Bridge GVRP Address as the destination MAC address in its PDUs.</td>
</tr>
</tbody>
</table>

Defaults

The destination MAC address for BPDUs is the Bridge Group Address.

Command Modes

CONFIGURATION

Command History

Version 8.2.1.0 Introduced on C-Series and S-Series.
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 Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **C-Series** and **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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**

No default values or behavior

**Command Modes**

EXEC

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 7.6.1.0** Introduced on C, E, and S-Series

**Related Commands**

- `show gvrp statistics` Display the GVRP statistics

debug gvrp

Enable debugging on GVRP.

**Syntax**

d debug gvrp {config | events | pdu}

To disable debugging, use the `no debug gvrp {config | events | pdu}` command.

**Parameters**

- **config** Enter the keyword `config` to enable debugging on the GVRP configuration.
**event**

Enter the keyword `event` to enable debugging on the JOIN/LEAVE events.

<table>
<thead>
<tr>
<th><strong>pdu</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the keyword <code>pdu</code> followed one of the following Interface keywords and slot/port or number information:</td>
</tr>
<tr>
<td>• For a Fast Ethernet interface, enter the keyword <code>FastEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td><strong>C-Series</strong> and <strong>S-Series</strong> Range: 1-128</td>
</tr>
<tr>
<td><strong>E-Series</strong> Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Defaults</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command Modes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC Privilege</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.6.0 Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>Version 7.6.1.0 Introduced on C, E, and S-Series</td>
</tr>
</tbody>
</table>

**disable**

Globally disable GVRP.

**Syntax**

```
disable
disable
```

To re-enable GVRP, use the `no disable` command.

<table>
<thead>
<tr>
<th><strong>Defaults</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command Modes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGURATION-GVRP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.6.1.0 Introduced on C, E, and S-Series</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gvrp enable</code> Enable GVRP on physical interfaces and LAGs.</td>
</tr>
<tr>
<td><code>protocol gvrp</code> Access GVRP protocol</td>
</tr>
</tbody>
</table>

**garp timers**

Set the intervals (in milliseconds) for sending GARP messages.

**Syntax**

```
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
garp timers {join | leave | leave-all}
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>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>join</strong></td>
<td>Enter the keyword <strong>join</strong> followed by the number of milliseconds to configure the join time.</td>
</tr>
<tr>
<td><strong>leave</strong></td>
<td>Enter the keyword <strong>leave</strong> followed by the number of milliseconds to configure the leave time.</td>
</tr>
<tr>
<td><strong>leave-all</strong></td>
<td>Enter the keyword <strong>leave-all</strong> followed by the number of milliseconds to configure the leave-all time.</td>
</tr>
</tbody>
</table>

**Defaults**

Default as above

**Command Modes**

CONFIGURATION-GVRP

**Command History**

Version 7.6.1.0 Introduced on C, E, and S-Series

**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**
  Display 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
gvrp registration

Configure the GVRP register type.

**Syntax**

```
gvrp registration {fixed | normal | forbidden}
```

To return to the default, use the `gvrp register normal` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fixed</td>
<td>Enter the keyword <code>fixed</code> followed by the VLAN range in a comma separated VLAN ID set.</td>
</tr>
<tr>
<td>normal</td>
<td>Enter the keyword <code>normal</code> followed by the VLAN range in a comma separated VLAN ID set. This is the default</td>
</tr>
<tr>
<td>forbidden</td>
<td>Enter the keyword <code>forbidden</code> followed by the VLAN range in a comma separated VLAN ID set.</td>
</tr>
</tbody>
</table>

**Defaults**

Default registration is `normal`

**Command Modes**

- CONFIGURATION-INTERFACE

**Command History**

- Version 7.6.1.0 Introduced on C, E, and S-Series

**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.

The **forbidden** is used when you do not want the interface to advertise or learn about VLANs through GVRP.

**Related Commands**

- `show gvrp` Display the GVRP configuration including the registration

---

**protocol gvrp**

Access GVRP protocol — (config-gvrp)#.

**Syntax**

`protocol gvrp`

**Defaults**

Disabled
show config

Display the global GVRP configuration.

Syntax

show config

Command Modes

CONFIGURATION-GVRP

Command History

Version 7.6.1.0  Introduced on C, E, and S-Series

Related Commands

gvrp enable   Enable GVRP on physical interfaces and LAGs.

protocol gvrp  Access GVRP protocol.

show garp timers

Display the GARP timer settings for sending GARP messages.

Syntax

show garp timers

Defaults

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.6.1.0  Introduced on C, E, and S-Series

Example

Figure 20-1.  show garp timers Command Example

FTOS#show garp timers
GARP Timers   Value (milliseconds)
----------------------------------------
Join Timer    200
Leave Timer   600
LeaveAll Timer 10000
FTOS#

garp timers   Set the intervals (in milliseconds) for sending GARP messages.
show gvrp

Display the GVRP configuration.

Syntax

```
show gvrp [brief | interface]
```

Parameters

brief 
(Optional) Enter the keyword `brief` to display a brief summary of the GVRP configuration.

interface 
(Optional) Enter the following keywords and slot/port or number information:

- For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - C-Series and S-Series: Range 1-128
  - E-Series: Range 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- 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

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

- Version 8.4.6.0: Added support for the keyword `fortyGigE`.
- Version 7.6.1.0: Introduced on C, E, and S-Series

Example

```
Figure 20-2. show gvrp brief Command Example

R3#show gvrp brief
GVRP Feature is currently enabled.

<table>
<thead>
<tr>
<th>Port</th>
<th>GVRP Status</th>
<th>Edge-Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gl 3/0</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/1</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/2</td>
<td>Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/3</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/4</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/5</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/6</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/7</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Gl 3/8</td>
<td>Disabled</td>
<td>No</td>
</tr>
</tbody>
</table>

R3#show gvrp brief
```

Usage Information

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

```
GVRP Participants running on <port_list>
```

to

```
GVRP Participants running on no ports
```
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 Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    
    C-Series and S-Series: Range: 1-128
    
    E-Series: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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

No default values or behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 8.4.6.0**
  
  Added support for the keyword `fortyGigE`.

- **Version 7.6.1.0**
  
  Introduced on C, E, and S-Series

Example

**Figure 20-3. show gvrp statistics Command Example**

```
FTOS#show gvrp statistics int gi 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 In 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#
```
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>Display the GVRP configuration</td>
</tr>
</tbody>
</table>
High Availability (HA)

Overview

High Availability (HA) in Dell Networking OS is configuration synchronization to minimize recovery time in the event of a Route Processor Module (RPM) failure. The feature is available on the C-Series and E-Series where noted by these symbols under command headings: [c] [e]

Dell Networking OS on the E-Series supports RPM 1 + 1 redundancy. The Primary RPM performs all routing and control operations, while the Secondary RPM is online and monitoring the Primary RPM.

In general, a protocol is defined as “hitless” in the context of an RPM failure/failover, and not failures of a line card, SFM, or power module. A protocol is defined as hitless if an RPM failover has no impact on the protocol.

Some protocols must be specifically enabled for HA, and some protocols are only hitless if related protocols are also enabled as hitless (see the redundancy protocol command).

High Availability is supported on E-Series ExaScale [ex] with Dell Networking OS 8.1.1.0. and later.

Commands

The HA commands available in Dell Networking OS are:

- `patch flash://RUNTIME_PATCH_DIR`
- `process restartable`
- `redundancy auto-failover-limit`
- `redundancy disable-auto-reboot`
- `redundancy force-failover`
- `redundancy primary`
- `redundancy protocol`
- `redundancy reset-counter`
- `redundancy sfm standby`
- `redundancy synchronize`
- `show patch`
- `show processes restartable`
- `show redundancy`
patch flash:///RUNTIME_PATCH_DIR

Insert an In-Service Modular Hot-Fix patch.

**Syntax**

```
patch flash:///RUNTIME_PATCH_DIR/patch-filename
```

To remove the patch, enter `no patch flash:///RUNTIME_PATCH_DIR/patch-filename`

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

The patch filename includes the Dell Networking OS version, the platform, the cpu, and the process it affects (FTOS-platform-cpu-process-patchversion.rtp). For example, a patch labeled `7.8.1.0-EH-rp2-l2mgr-1.rtp` identifies that this patch applies to Dell Networking OS version 7.8.1.0 - E-Series platform, for RP2, addressing the layer 2 management process, and this is the first version of this patch.

There is no need to reload or reboot the system when the patch is inserted. The In-Service Modular patch replaces the existing process code. Once installation is complete, the system executes the patch code as though it was always there.

**Related Commands**

- `show patch` Display the system patches loaded with the In-Service Modular Hot Fix Command.

process restartable

Enable a process to be restarted. Restartability is subject to a maximum restart limit—the limit is defined as a configured amount of restarts within a configured amount of time. On the software exception that exceeds the limit, the system reloads (for systems with a single RPM) or fails over (for systems with dual RPMs).

**Syntax**

```
process restartable [process] [count number] [period minutes]
```

**Parameters**

- `process` Configure a process to be restartable.
- `count number` Enter the number of times a process can restart within the configured period.
  - Range: 1-3
  - Default: 3
- `period minutes` Enter the amount of time within which the process can restart `count` times.
  - Range: 1-60 minutes
  - Default: 60 minutes

**Defaults**

By default, a process can be restarted a maximum of 3 times within 1 hour. On the exception that exceeds this limit, the system reloads or fails over.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>
Related Commands

- show processes restartable

redundancy auto-failover-limit

Specify an auto-failover limit for RPMs. When a non-recoverable fatal error is detected, an automatic RPM failover occurs. This command does not affect user-initiated (manual) failovers.

Syntax

redundancy auto-failover-limit [count number [period minutes] | period minutes]]

To disable the auto-failover limit control, enter no redundancy auto-failover-limit.

Parameters

- **count number**: Enter the number of times the RPMs can automatically failover within the period defined in the period parameter.
  - Range: 2 to 10
  - Default: 3
- **period minutes**: Enter a duration in which to allow a number of automatic failovers (limited to the number defined in the count parameter).
  - Range: 5 to 9000 minutes
  - Default: 60 minutes

Defaults

- Count: 3
- Period: 60 minutes

Command Modes

- CONFIGURATION

Command History

- Version 8.1.1.0  Introduced on E-Series ExaScale
- Version 7.5.1.0  Introduced on C-Series
- Version 7.6.1.0  Introduced on E-Series

Usage Information

If auto failover is disabled, enter the redundancy auto-failover-limit (without any parameters) to set auto failover to the default parameters (Count 3, Period 60 minutes). Use the show redundancy command to view the redundancy status.

When you change one or both of the optional parameters, FTOS checks that the interval between auto failovers is more than five (5) minutes. If the interval is less, FTOS returns a configuration error message.

redundancy disable-auto-reboot

Prevent the system from auto-rebooting the failed module.

Syntax

redundancy disable-auto-reboot [rpm] card number | all]

To return to the default, enter no redundancy disable-auto-reboot rpm.

Parameters

- **rpm**: Enter the keyword rpm to disable auto-reboot of the failed RPM.

Defaults

- Disabled (that is, the failed module is automatically rebooted).

Command Modes

- CONFIGURATION
Enabling this command will keep the failed RPM in the failed state. If there are two RPMs in the system, enabling this command prevents the failed RPM from becoming a working Standby RPM. If there is only one RPM in the system, the failed RPM will not recover—this will effect the system.

⚠️ **Warning:** When you use this command, if the first VLT peer RPM has crashed, the backup VLT channel is still alive and the second VLT peer will not know that the first VLT is in crash state. As a result, the second VLT peer assumes that the first VLT peer is still up.

### redundancy force-failover

This command can be used to provide a hitless or warm upgrade. A hitless upgrade means that a software upgrade does not require a reboot of the line cards. A warm upgrade means that a software upgrade requires a reset of the line cards and SFMs. A warm upgrade is possible for major releases and lower, while a hitless upgrade can only support patch releases.

You load the software upgrade on one RPM and then issue this command with the `rpm` keyword to move the software to the other RPM. The system senses the condition and provides a series of prompts appropriate to that context, as shown in the following example:

⚠️ **Note:** On C-Series, this command could affect traffic (even during hot-failover) since the switch fabric present on the RPM is taken down during the failover.
redundancy primary

Set an RPM as the primary RPM.

Syntax

redundancy primary [rpm0 | rpm1]

To delete a configuration, enter no redundancy primary.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rpm0</td>
<td>Enter the keyword rpm0 to set the RPM in slot R0 as the primary RPM.</td>
</tr>
<tr>
<td>rpm1</td>
<td>Enter the keyword rpm1 to set the RPM in slot R1 as the primary RPM.</td>
</tr>
</tbody>
</table>

Defaults

The RPM in slot R0 is the Primary RPM.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

redundancy protocol

Enable hitless protocols.

Syntax

redundancy protocol {lacp | xstp}

To disable a hitless protocol, enter no redundancy protocol {lacp | xstp}.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lacp</td>
<td>Enter the keyword lacp to make LACP hitless.</td>
</tr>
<tr>
<td>xstp</td>
<td>Enter the keyword xstp to invoke hitless STP (all STP modes—MSTP, PVST+, RSTP, STP).</td>
</tr>
</tbody>
</table>

Note: On the C-Series, hitless STP is available only for MSTP, PVST+, and RSPT.

Defaults

Disabled
redundancy reset-counter

Reset failover counter and timestamp information displayed in the show redundancy command output.

Syntax redundancy reset-counter

Defaults Not configured

Command Modes EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

redundancy sfm standby

Place the SFM in an offline state.

Syntax redundancy sfm standby

Place the SFM in an online state using the command no redundancy sfm standby command.

Defaults The SFM is online by default.

Command Modes CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

Usage Information

When a secondary RPM with logical SFM is inserted or removed, the system must add or remove the backplane links to the switch fabric trunk. To avoid traffic disruption, use this command when the secondary RPM is inserted. When this command is executed, the logical SFM on the standby RPM is immediately taken offline and the SFM state is set as “standby”.

Note: This command could affect traffic when taking the secondary SFM offline.
Example

**Figure 21-3. redundancy sfm standby Command Example**

```plaintext
FTOS#show sfm all
Switch Fabric State: up
-- Switch Fabric Modules --
Slot  Status
-----------------------------------------------
0   active
1   active

FTOS(config)#redundancy sfm standby
Taking secondary SFM offline...
!
FTOS(config)#do show sfm all
Switch Fabric State: up
-- Switch Fabric Modules --
Slot  Status
-----------------------------------------------
0   active
1   standby

FTOS(config)#no redundancy sfm
Taking secondary SFM online...
!
FTOS(config)#do show sfm all
Switch Fabric State: up
-- Switch Fabric Modules --
Slot  Status
-----------------------------------------------
0   active
1   active
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sfm</td>
<td>Display the SFM status</td>
</tr>
<tr>
<td>show switch links</td>
<td>Display the switch fabric backplane or internal status.</td>
</tr>
</tbody>
</table>

### redundancy synchronize

Manually synchronize data once between the Primary RPM and the Secondary RPM.

**Syntax**

`redundancy synchronize [full | persistent-data | system-data]`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>full</td>
<td>Enter the keyword <code>full</code> to synchronize all data.</td>
</tr>
<tr>
<td>persistent-data</td>
<td>Enter the keywords <code>persistent-data</code> to synchronize the startup configuration between RPMs.</td>
</tr>
<tr>
<td>system-data</td>
<td>Enter the keywords <code>system-data</code> to synchronize persistent-data and the running configuration file, event log, SFM and line card states.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
show patch

Display the system patches loaded with the In-Service Modular Hot Fix Command.

**Syntax**

```plaintext
show patch
```

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>patch flash://</td>
<td>Insert an In-Service Modular Hot-Fix patch.</td>
</tr>
<tr>
<td>RUNTIME_PATCH_DIR</td>
<td></td>
</tr>
</tbody>
</table>

show processes restartable

Display the processes and tasks configured for restartability.

**Syntax**

```plaintext
show processes restartable [history]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>Display the last time the restartable processes crashed.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS#sho processes restartable

+---------------------------------------------+-----------+-----------------+-------------------+
<table>
<thead>
<tr>
<th>Process name</th>
<th>State</th>
<th>How many times restarted</th>
<th>Timestamp last</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius</td>
<td>enabled</td>
<td>0</td>
<td>[-]</td>
</tr>
<tr>
<td>tacplus</td>
<td>enabled</td>
<td>0</td>
<td>[-]</td>
</tr>
</tbody>
</table>

FTOS#show processes restartable history

+---------------------------------------------+-------------------+
<table>
<thead>
<tr>
<th>Process name</th>
<th>Timestamp last crashed</th>
</tr>
</thead>
</table>

```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process restartable</td>
<td></td>
</tr>
</tbody>
</table>

show redundancy

Display the current redundancy configuration.

**Syntax**

```plaintext
show redundancy
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process restartable</td>
<td></td>
</tr>
</tbody>
</table>
### Command Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td></td>
</tr>
<tr>
<td>EXEC Privilege</td>
<td></td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced On</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

### Example

#### Figure 21-4. show redundancy Command Example

```
FTOS#show redundancy
-- RPM Status --
---------------------------------------------
RPM Slot ID:                        1
RPM Redundancy Role:        Primary
RPM State:                       Active
RPM SW Version:                 7.5.1.0
Link to Peer:                   Up
-- PEER RPM Status --
---------------------------------------------
RPM State:                       Standby
RPM SW Version:                 7.5.1.0
-- RPM Redundancy Configuration --
---------------------------------------------
Primary RPM:                      rpm0
Auto Data Sync:                Full
Failover Type:                  Hot Failover
Auto reboot RPM:                Enabled
Auto failover limit:            3 times in 60 minutes
-- RPM Failover Record --
---------------------------------------------
Failover Count:                 1
Last failover timestamp:       Jul 13 2007 21:25:32
Last failover Reason:          User request
-- Last Data Block Sync Record:--
---------------------------------------------
FTOS#
```

### Table 21-1. show redundancy Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPM Status</td>
<td>Displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• Slot number of the RPM</td>
</tr>
<tr>
<td></td>
<td>• Whether the RPM is Primary or Standby</td>
</tr>
<tr>
<td></td>
<td>• The state of the RPM: Active, Standby, Booting, or Offline</td>
</tr>
<tr>
<td></td>
<td>• Whether the link to the second RPM is up or down.</td>
</tr>
<tr>
<td>PEER RPM Status</td>
<td>Displays the state of the second RPM, if present</td>
</tr>
</tbody>
</table>
Table 21-1.  show redundancy Command Example Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| RPM Redundancy Configuration | Displays the following information:  
  • which RPM is the preferred Primary on next boot (redundancy primary command)  
  • the data sync method configured (redundancy synchronize command).  
  • the failover type (you cannot change this; it is software dependent) **Hot Failover** means the running configuration and routing table are applied on secondary RPM. **Fast Failover** means the running configuration is not applied on the secondary RPM till failover occurs, and the routing table on line cards is cleared during failover.  
  • the status of auto booting the RPM (redundancy disable-auto-reboot command)  
  • the parameter for auto failover limit control (redundancy auto-failover-limit command) |
| RPM Failover Record       | Displays the following information:  
  • RPM failover counter (to reset the counter, use the redundancy reset-counter command)  
  • the time and date of the last RPM failover  
  • the reason for the last RPM failover.                                                                                                           |
| Last Data Sync Record     | Displays the data sync information and the timestamp for the data sync:  
  • Start-up Config is the contents of the startup-config file.  
  • Line Card Config is the line card types configured and interfaces on those line cards.  
  • Runtime Event Log is the contents of the Event log.  
  • Running Config is the current running-config. This field only appears when you enter the command from the Primary RPM. |
Internet Group Management Protocol (IGMP)

Overview

The platforms on which a command is supported is indicated by the character — E for the E-Series, C for the C-Series, and S for the S-Series — that appears below each command heading.

This chapter contains the following sections:

• IGMP Commands
• IGMP Snooping Commands

IGMP Commands

FTOS supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

• Dell Networking OS supports PIM-SM and PIM-SSM include and exclude modes.
• IGMPv2 is the default version of IGMP on interfaces. IGMPv3 can be configured on interfaces, and is backward compatible with IGMPv2.
• The maximum number of interfaces supported is 512 on the E-Series. On the C-Series and S-Series 31 interfaces are supported.
• Maximum number of groups supported — no hard limit
• IGMPv3 router interoperability with IGMPv2 and IGMPv1 routers on the same subnet is not supported.
• An administrative command (ip igmp version) is added to manually set the IGMP version.
• All commands, previously used for IGMPv2, are compatible with IGMPv3.

The commands include:

• clear ip igmp groups
• debug ip igmp
• ip igmp access-group
• ip igmp group-join-limit
• ip igmp immediate-leave
• ip igmp last-member-query-interval
• ip igmp querier-timeout
• ip igmp query-interval
• ip igmp query-max-resp-time
• ip igmp ssm-map
• ip igmp static-group
• ip igmp version
• show ip igmp groups
• show ip igmp interface
• show ip igmp ssm-map

**clear ip igmp groups**
Clear entries from the group cache table.

**Syntax**
clear ip igmp groups [group-address | interface]

**Parameters**
- **group-address** (OPTIONAL) Enter the IP multicast group address in dotted decimal format.
- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 10/100 Base-T Ethernet interface, enter the keyword gigabitethernet followed by the slot/port information.
  - For a Gigabit Ethernet interface, enter the keyword gigabitethernet followed by the slot/port information.
  - For a SONET interface, enter the keyword sonet followed by the 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.

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.4.6.0 Added support for the keyword fortyGigE.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series legacy command

**Usage Information**
IGMP commands accept only non-VLAN interfaces—specifying VLAN will not yield a results.

**debug ip igmp**
Enable debugging of IGMP packets.

**Syntax**
debug ip igmp [group address | interface]

To disable IGMP debugging, enter no debug ip igmp [group address | interface]. To disable all debugging, enter undebug all.
Parameters

| group-address (OPTIONAL) Enter the IP multicast group address in dotted decimal format. |
| interface (OPTIONAL) Enter the following keywords and slot/port or number information: |

- Enter one of the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For a Port Channel interface, enter the keyword port-channel followed by number.
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale
  - For SONET interfaces, enter the keyword sonet followed by the slot/port information. This keyword is only available on E-Series and C-Series.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.

Defaults

Disabled

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series legacy command

Usage Information

IGMP commands accept only non-VLAN interfaces—specifying a VLAN will not yield results. This command displays packets for IGMP and IGMP Snooping.

ip igmp access-group

Use this feature to specify access control for packets.

Syntax

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

The access list accepted is an extended ACL. This feature is used to block IGMP reports from hosts, on a per-interface basis; based on the group address and source address specified in the access list.
ip igmp group-join-limit

Use this feature to limit the number of IGMP groups that can be joined in a second.

Syntax ip igmp group-join-limit number

Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the number of IGMP groups permitted to join in a second. Range: 1 to 10000</td>
</tr>
</tbody>
</table>

Defaults

No default values or behavior

Command Modes

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

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

ip igmp immediate-leave

Enable IGMP immediate leave.

Syntax ip igmp immediate-leave [group-list prefix-list-name]

To disable ip igmp immediate leave, use the no ip igmp immediate-leave command.

Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-list prefix-list-name</td>
<td>Enter the keyword group-list followed by a string up to 16 characters long of the prefix-list-name.</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>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>E-Series legacy command</td>
<td></td>
</tr>
</tbody>
</table>

Usage Information

Querier normally sends a certain number of group specific queries when a leave message is received, for a group, prior to deleting a group from the membership database. There may be situations in which immediate deletion of a group from the membership database is required. This command provides a way to achieve the immediate deletion. In addition, this command provides a way to enable immediate-leave processing for specified groups.
ip igmp last-member-query-interval
Change the last member query interval, which is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This interval is also the interval between Group-Specific Query messages.

Syntax
```
ip igmp last-member-query-interval milliseconds
```
To return to the default value, enter `no ip igmp last-member-query-interval`.

Parameters
- `milliseconds` Enter the number of milliseconds as the interval.
  - Default: 1000 milliseconds
  - Range: 100 to 65535

Defaults
1000 milliseconds

Command Modes
INTERFACE

Command History
- Version 7.8.1.0 Introduced on S-Series
- Version 7.7.1.0 Introduced on C-Series
- E-Series legacy command

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
- `seconds` Enter the number of seconds the router must wait to become the new querier.
  - Default: 125 seconds
  - Range: 60 to 300

Defaults
125 seconds

Command Modes
INTERFACE

Command History
- Version 7.8.1.0 Introduced on S-Series
- Version 7.7.1.0 Introduced on C-Series
- Version 7.6.1.0 Introduced on S-Series in Interface VLAN mode only to enable that system to act as an IGMP Proxy Querier.
- Version 7.5.1.0 Introduced on C-Series in Interface VLAN mode only to enable that system to act as an IGMP Proxy Querier.
- E-Series legacy command
**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**

- `seconds`: Enter the number of seconds between queries sent out.
  - Default: 60 seconds
  - Range: 1 to 18000

**Defaults**

60 seconds

**Command Modes**

INTERFACE

**Command History**

- Version 7.8.1.0: Introduced on S-Series
- Version 7.7.1.0: Introduced on C-Series
- Version 7.6.1.0: Introduced on S-Series in Interface VLAN mode only to enable that system to act as an IGMP Proxy Querier.
- Version 7.5.1.0: Introduced on C-Series in Interface VLAN mode only to enable that system to act as an IGMP Proxy Querier.
- E-Series legacy command

**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`.

**Parameters**

- `seconds`: Enter the number of seconds for the maximum response time.
  - Default: 10 seconds
  - Range: 1 to 25

**Defaults**

10 seconds

**Command Modes**

INTERFACE

**Command History**

- Version 7.8.1.0: Introduced on S-Series
- Version 7.7.1.0: Introduced on C-Series
- Version 7.6.1.0: Introduced on S-Series in Interface VLAN mode only to enable that system to act as an IGMP Proxy Querier.
- Version 7.5.1.0: Introduced on C-Series in Interface VLAN mode only to enable that system to act as an IGMP Proxy Querier.
- E-Series legacy command
### ip igmp ssm-map

Use a statically configured list to translate (*,G) memberships to (S,G) memberships.

**Syntax**

```
ip igmp ssm-map std-access-list source-address
```

Undo this configuration, that is, remove SSM map (S,G) states and replace them with (*,G) states using the command `ip igmp ssm-map std-access-list source-address` command.

**Parameters**

- `std-access-list` Specify the standard IP access list that contains the mapping rules for multicast groups.
- `source-address` Specify the multicast source address to which the groups are mapped.

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.8.1.0 Introduced on C-Series and S-Series
- Version 7.7.1.0 Introduced on E-Series

**Usage Information**

Mapping applies to both v1 and v2 IGMP join requests; any updates to the ACL are reflected in the IGMP groups. You may not use extended access lists with this command. When a static SSM map is configured and the router cannot find any matching access lists, the router continues to accept (*,G) groups.

**Related Commands**

- `ip access-list standard` Create a standard access list to filter based on IP address.

### ip igmp static-group

Configure an IGMP static group.

**Syntax**

```
ip igmp static-group {group address [exclude [source address]] | [include {source address}]
```

To delete a static address, use the `no ip igmp static-group {group address [exclude [source address]] | [include {source address}]}` command.

**Parameters**

- `group address` Enter the group address in dotted decimal format (A.B.C.D)
- `exclude source address` (OPTIONAL) Enter the keyword `exclude` followed by the source address, in dotted decimal format (A.B.C.D), for which a static entry needs to be added.
- `include source address` (OPTIONAL) Enter the keyword `include` followed by the source address, in dotted decimal format (A.B.C.D), for which a static entry needs to be added.

**Defaults**

No default values or behavior

**Command Modes**

INTERFACE

**Command History**

- Version 7.8.1.0 Introduced on S-Series
- Version 7.7.1.0 Introduced on C-Series
A group in the **include** mode should have at least one source address defined. In **exclude** mode if no source address is specified, Dell Networking OS implicitly assumes all sources are included. If neither **include** or **exclude** is specified, Dell Networking OS implicitly assumes a IGMPv2 static join.

**Command Limitations**
- Only one mode (**include** or **exclude**) is permitted per multicast group per interface. To configure another mode, all sources belonging to the original mode must be unconfigured.
- If a static configuration is present and a packet for the same group arrives on an interface, the dynamic entry will completely overwrite all the static configuration for the group.

**Related Commands**
- **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 7.8.1.0 Introduced on S-Series
    - Version 7.7.1.0 Introduced on C-Series
    - Version 7.5.1.0 Introduced for E-Series

- **show ip igmp groups**
  - View the IGMP groups.
  - Syntax: `show ip igmp groups [group-address [detail] | detail | interface [group-address [detail]]]`
Parameters

**group-address**  (OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.

**interface**  (OPTIONAL) Enter the interface type and slot/port information:

- For a 100/1000 Ethernet interface, enter the keyword `gigabitethernet` followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - **C-Series** and **S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a SONET interface, enter the keyword `sonet` followed by the 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.
- For a VLAN interface enter the keyword `vlan` followed by a number from 1 to 4094.

**detail**  (OPTIONAL) Enter the keyword `detail` to display the IGMPv3 source information.

Command Modes

**EXEC**

**EXEC Privilege**

Command History

- **Version 8.4.6.0**  Added support for the keyword `fortyGigE`.
- **Version 7.6.1.0**  Introduced on S-Series and on C-Series
- **Version 7.5.1.0**  Expanded to support the `detail` option.

E-Series legacy command

Usage Information

This command displays the IGMP database including configured entries for either all groups on all interfaces, or all groups on specific interfaces, or specific groups on specific interfaces.

Example

**Figure 22-1.  show ip igmp groups Command Example**

```plaintext
FTOS#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
224.0.1.40       GigabitEthernet 13/6     09:45:23  00:02:08  10.87.7.5
FTOS#
```
Example VLT

Note: The asterisk (*) after the port channel number (Po 2) highlighted in the following example indicates the port channel is VLT, that the local VLT port channel is down and the remote VLT port is up.

```
FTOS#show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Mode   Uptime   Expires  Last Reporter
225.0.0.0     Vlan 100  IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.1     Vlan 100  IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.2     Vlan 100  IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.3     Vlan 100  IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
225.0.0.4     Vlan 100  IGMPv2 00:00:05 00:02:04 3.0.0.51
Member Ports: Po 2*
```

Table 22-1. show ip igmp groups Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Lists the multicast address for the IGMP group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Lists the interface type, slot and port number.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Displays the amount of time the group has been operational.</td>
</tr>
<tr>
<td>Expires</td>
<td>Displays the amount of time until the entry expires.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>Displays the IP address of the last host to be a member of the IGMP group.</td>
</tr>
<tr>
<td>Member Ports</td>
<td>Indicates the port channel. If the port channel is VLT, an asterisk (*) after the port channel number indicates the port channel is locally down and that a remote VLT port is up.</td>
</tr>
</tbody>
</table>

**show ip igmp interface**

View information on the interfaces participating in IGMP.

**Syntax**

```
show ip igmp interface [interface]
```

**Parameters**

- **interface** (OPTIONAL) Enter the interface type and slot/port information:
  - For a 100/1000 Ethernet interface, enter the keyword `gigabitethernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` 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:
    - **C-Series** and **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - 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.
IGMP commands accept only non-VLAN interfaces—specifying VLAN will not yield results.

Example

**Figure 22-2. show ip igmp interface Command Example**

```
FTOS#show ip igmp interface
gigabitethernet 0/0 is down, line protocol is down
    Internet protocol processing disabled
    GigabitEthernet 0/5 is down, line protocol is down
    Internet protocol processing disabled
    GigabitEthernet 0/6 is down, line protocol is down
    Internet protocol processing disabled
    GigabitEthernet 0/7 is up, line protocol is down
    Internet protocol processing disabled
    GigabitEthernet 7/9 is up, line protocol is up
    Internet address is 10.87.5.250/24
    IGMP is enabled on interface
    IGMP query interval is 60 seconds
    IGMP querier timeout is 120 seconds
    IGMP max query response time is 10 seconds
    IGMP last member query response interval is 1000 ms
    IGMP activity: 0 joins, 0 leaves
    IGMP querying router is 10.87.5.250 (this system)
    IGMP version is 2
```

**show ip igmp ssm-map**

Display is a list of groups that are currently in the IGMP group table and contain SSM mapped sources.

**Syntax**

```
show ip igmp ssm-map [group]
```

**Parameters**

- `group` (OPTIONAL) Enter the multicast group address in the form A.B.C.D to display the list of sources to which this group is mapped.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.6.0 Added support for the keyword **fortyGigE**
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series legacy command

**Related Commands**

- `ip igmp`
- `ssm-map` Use a statically configured list to translate (*,G) memberships to (S,G) memberships.
IGMP Snooping Commands

Dell Networking OS supports IGMP Snooping version 2 and 3 on all Dell Networking systems:

- `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

- Dell Networking OS supports version 1, version 2, and version 3 hosts.
- Dell Networking OS 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 FIB.
- Dell Networking OS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- Dell Networking OS supports IGMP snooping on JUMBO enabled cards.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 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 STP.
- IGMP snooping reacts to Layer 2 topology changes triggered by 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 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 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series legacy command

**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**

- `no shutdown` Activate an interface

---

**ip igmp snooping fast-leave**

Enable IGMP snooping fast leave for this VLAN.

**Syntax**

```
ip igmp snooping fast-leave
```

To disable IGMP snooping fast leave, use the `no igmp snooping fast-leave` command.

**Defaults**

Not configured

**Command Modes**

- INTERFACE VLAN—`(conf-if-vl-n)`

**Command History**

- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- E-Series legacy command

**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 IGMP fast leave processing is enabled, the switch will remove 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. On the E-Series, when flooding is enabled (the default), unregistered multicast data traffic is flooded to all ports in a VLAN. 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, then unregistered multicast data traffic is dropped. On the C-Series and S-Series, unregistered multicast data traffic is dropped when flooding is disabled; they do not forward the packets to multicast router ports. On the C-Series and S-Series, Layer 3 multicast must be disabled (no ip multicast-routing) in order to disable Layer 2 multicast flooding.

Syntax

ip igmp snooping flood

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version 8.2.1.0</th>
<th>Introduced on the C-Series and S-Series.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.1</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Version 7.6.1.0</th>
<th>Introduced on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

E-Series legacy command
ip igmp snooping mrouter

Syntax: `ip igmp snooping mrouter interface interface`

To delete a specific multicast router interface, use the `no ip igmp snooping mrouter interface interface` command.

Parameters:

<table>
<thead>
<tr>
<th>interface</th>
<th>Enter the following keywords and slot/port or number information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For an 100/1000 Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For 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 Port Channel interface, enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>• C-Series and S-Series: Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• E-Series: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
</tbody>
</table>

Defaults: Not configured

Command Modes: INTERFACE VLAN—(`conf-if-vl-n`)
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**

```plaintext
show ip igmp snooping mrouter [vlan number]
```

**Parameters**

- `vlan number` Enter the keyword `vlan` followed by the vlan number.
  
  `Range: 1-4094`

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

- If the port channel is a VLT port channel, an asterisk (*) after the port channel number (Po 100*) indicates the port channel is locally down and that a remote VLT port is up.

**Example**

```plaintext
FTOS#show ip igmp snooping mrouter
Interface   Router Ports
Vlan 2      Gi 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

The symbols [C E S] under command headings indicate which Dell Networking platforms — C-Series, E-Series, or S-Series, respectively — support the command.

Although all interfaces are supported on E-Series ExaScale, some interface functionality is supported on E-Series ExaScale ex with Dell Networking OS 8.2.1.0. and later. When this is the case that is noted in the command history.

Basic Interface Commands

The following commands are for physical, Loopback, and Null interfaces:

- clear counters
- clear dampening
- cx4-cable-length
- dampening
- description
- disable-on-sfm-failure
- duplex (Management)
- duplex (10/100 Interfaces)
- flowcontrol
- interface
- interface loopback
- interface ManagementEthernet
- interface null
- interface range
- interface range macro (define)
- interface range macro name
- interface vlan
- ipg (Gigabit Ethernet interfaces)
- ipg (10 Gigabit Ethernet interfaces)
- keepalive
- Ifs enable (EtherScale)
- link debounce-timer
- monitor
- mtu
- negotiation auto
- portmode hybrid
- rate-interval
- show config
- show config (from INTERFACE RANGE mode)
- show interfaces
- show interfaces configured
- show interfaces dampening
- show interfaces description
- show interfaces linecard
- show interfaces phy
- show interfaces stack-unit
- show interfaces status
- show interfaces switchport
- show interfaces transceiver
- show range
- shutdown
- speed (for 10/100/1000 interfaces)
- speed (Management interface)
- switchport
- wanport

**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 [ipv6 | 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 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.
- 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:
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For the management interface on the RPM, enter the keyword ManagementEthernet followed by slot/port information. The slot range is 0-1, and the port range is 0.
- For a SONET interface, enter the keyword sonet followed by the slot/port information.
- 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.

vrrp

(Optional) Enter the keyword vrrp to clear the counters of all VRRP groups. To clear the counters of VRRP groups on all IPv6 interfaces, enter ipv6. To clear the counters of a specified group, enter a vrid number from 1 to 255.

vrrp

(Optional) E-Series only: Enter the keyword vrrp to clear counters for all VRRP groups. To clear the counters of VRRP groups in a specified VRF instance, enter the name of the instance (32 characters maximum). IPv6 VRRP groups are not supported.

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.

Note: This option is not supported on the S-Series, as the MAC learning limit is not supported.

Defaults

Without an interface specified, the command clears all interface counters.

Command Modes

EXEC Privilege

Command History

Version 8.4.6.0 Added support for the keyword fortyGigE.
Version 8.4.1.0 On the E-Series, support was added for VRRP groups in a VRF instance.
Version 8.2.1.0 Support for 4093 VLANs on E-Series ExaScale. Prior to release supported 2094.
Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
Version 6.5.1.0 Updated definition of the learning-limit option for clarity.

Example

Figure 23-1.  clear counters Command Example

FTOS#clear counters
Clear counters on all interfaces [confirm]
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 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - `C-Series` and `S-Series` Range: 1-128
    - `E-Series` Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.

**Defaults**
Without a specific interface specified, the command clears all interface dampening counters.

**Command Modes**
EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **Version 7.4.1.0** Introduced on E-Series

**Example**

```
FTOS#clear dampening gigabitethernet 1/2
Clear dampening counters on Gi 1/2 [confirm] y
FTOS#
```

**Related Commands**

- `show interfaces dampening` Display interface dampening information.
- `dampening` Configure dampening on an interface.

---

mac learning-limit

Allow aging of MACs even though a learning-limit is configured or disallow station move on learnt MACs.

show interfaces

Displays information on the interfaces.

---

**cx4-cable-length**

Configure the length of the cable to be connected to the selected CX4 port.
Syntax  

[no] cx4-cable-length {long | medium | short}

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>long</td>
<td>medium</td>
</tr>
<tr>
<td>Enter the keyword that matches the cable length to be used at the selected port:</td>
<td></td>
</tr>
<tr>
<td>short = For 1-meter and 3-meter cable lengths</td>
<td></td>
</tr>
<tr>
<td>medium = For 5-meter cable length</td>
<td></td>
</tr>
<tr>
<td>long = For 10-meter and 15-meter cable lengths</td>
<td></td>
</tr>
</tbody>
</table>

Defaults

medium

Mode

Interface

Command History

Version 7.7.1.0 Introduced on S-Series

Usage Information

This command only works on ports that the system recognizes as CX4 ports. The figure below shows an attempt to configure an XFP port in an S25P with the command after inserting a CX4 converter into the port:

Note: When using a long CX4 cable between the C-Series and the S-Series, configure the cable using the `cx4-cable-length short` command only to avoid any errors.

Note: 15M CX4 active cable is not supported on C-Series and S-series. It is only supported for S2410 with active end on the device.

Example

**Figure 23-2. Example of Unsuccessful CX4 Cable Length Configuration**

```
FTOS#show interfaces tengigabitethernet 0/26 | grep "XFP type"
Pluggable media present, XFP type is 10GBASE-CX4
FTOS(conf-if-te-0/26)#cx4-cable-length short
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length medium
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#cx4-cable-length long
% Error: Unsupported command.
FTOS(conf-if-te-0/26)#
```

The figure below shows a successful CX4 cable length configuration.

**Figure 23-3. Example of CX4 Cable Length Configuration**

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

For details on using XFP ports with CX4 cables, see your S-Series hardware guide.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show config</td>
<td>Display the configuration of the selected interface.</td>
</tr>
</tbody>
</table>
dampening

Configure dampening on an interface.

Syntax

dampening [[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]

To disable dampening, use the no dampening [[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]] command syntax.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>half-life</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.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 30 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 5 seconds</td>
</tr>
<tr>
<td>reuse-threshold</td>
<td>Enter a number as the reuse threshold, the penalty value below which the interface state is changed to “up”.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 20000</td>
</tr>
<tr>
<td></td>
<td>Default: 750</td>
</tr>
<tr>
<td>suppress-threshold</td>
<td>Enter a number as the suppress threshold, the penalty value above which the interface state is changed to “error disabled”.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 20000</td>
</tr>
<tr>
<td></td>
<td>Default: 2500</td>
</tr>
<tr>
<td>max-suppress-time</td>
<td>Enter the maximum number for which a route can be suppressed. The default is four times the half-life value.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 86400</td>
</tr>
<tr>
<td></td>
<td>Default: 20 seconds</td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

INTERFACE (conf-if-)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Example

```
FTOS(conf-if-gi-3/2)#dampening 20 800 4500 120
FTOS(conf-if-gi-3/2)#
```

Usage Information

With each flap, Dell Networking OS penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the configured half-life. Once 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 4 times `half-life`

*Note:* Dampening cannot be applied on an interface that is monitoring traffic for other interfaces.
description

Assign a descriptive text string to the interface.

Syntax
description desc_text

To delete a description, enter no description.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>desc_text</td>
<td>Enter a text string up to 240 characters long.</td>
</tr>
</tbody>
</table>

Defaults

No description is defined.

Command Modes

INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Modified for E-Series: Revised from 78 to 240 characters.</td>
</tr>
</tbody>
</table>

Usage Information

- To use special characters as a part of the description string, you must enclose the whole string in double quotes.
- 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dampening</td>
<td>Clear the dampening counters on all the interfaces or just the specified interface.</td>
</tr>
<tr>
<td>show interfaces dampening</td>
<td>Display interface dampening information.</td>
</tr>
</tbody>
</table>

disable-on-sfm-failure

Disable select ports on E300 systems when a single SFM is available.

Syntax
disable-on-sfm-failure

To delete a description, enter no disable-on-sfm-failure.

Defaults

Port is not disabled

Command Modes

INTERFACE
When an E300 system boots up and a single SFM is active this configuration, any ports configured with this feature will be shut down. If an SFM fails (or is removed) in an E300 system with two SFM, ports configured with this feature will be shut down. All other ports are treated normally.

When a second SFM is installed or replaced, all ports are booted up and treated as normally. This feature does not take affect until a single SFM is active in the E300 system.

duplex (Management)

Set the mode of the Management interface.

Syntax

duplex {half | full}

To return to the default setting, enter no duplex.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>half</td>
<td>Enter the keyword half to set the Management interface to transmit only in one direction.</td>
</tr>
<tr>
<td>full</td>
<td>Enter the keyword full to set the Management interface to transmit in both directions.</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>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.4.1.0</td>
<td>Documentation modified—added Management to distinguish from duplex (10/100 Interfaces)</td>
</tr>
</tbody>
</table>

Usage Information

This command applies only to the Management interface on the RPMs.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface ManagementEthernet</td>
<td>Configure the Management port on the system (either the Primary or Standby RPM).</td>
</tr>
<tr>
<td>duplex (Management)</td>
<td>Set the mode of the Management interface.</td>
</tr>
<tr>
<td>management route</td>
<td>Configure a static route that points to the Management interface or a forwarding router.</td>
</tr>
<tr>
<td>speed (Management interface)</td>
<td>Set the speed on the Management interface.</td>
</tr>
</tbody>
</table>

duplex (10/100 Interfaces)

Configure duplex mode on any physical interfaces where the speed is set to 10/100.

Syntax

duplex {half | full}

To return to the default setting, enter no duplex.
flowcontrol

Control how the system responds to and generates 802.3x pause frames on 1Gig and 10Gig line cards.

Syntax

flowcontrol rx \{off | on\} tx \{off | on\} threshold \{<1-2047> <1-2013> <1-2013>\}

Parameters

rx on
Enter the keywords rx on to process the received flow control frames on this port. This is the default value for the receive side.

rx off
Enter the keywords rx off to ignore the received flow control frames on this port.

tax on
Enter the keywords tx on to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.

threshold (C-Series and S-Series only)
When tx on is configured, you can set the threshold values for:
- Number of flow-control packet pointers: 1-2047 (default = 75)
- Flow-control buffer threshold in KB: 1-2013 (default = 49KB)
- Flow-control discard threshold in KB: 1-2013 (default = 75KB)

Defaults

C-Series: rx off tx off
E-Series: rx on tx on
S-Series: rx off tx off

Command Modes

INTERFACE
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 S-Series. 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 line cards: 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. On 1G interfaces, changing the flow control values causes an automatic interface flap, after which PAUSE values are exchanged as part of the auto-negotiation process. As a workaround, apply the new settings, execute shut followed by no shut on the interface, and then check the running-config of the port.

### Important Points to Remember

- Do not enable tx pause when buffer carving is enabled. Consult Dell Networking TAC for information and assistance.
- Asymmetric flow control (rx on tx off or rx off tx on) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

  Can’t 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:

  Can’t 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:

  Can’t 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.

- Speeds less than 1 Gig cannot be configured when the asymmetric flow control configuration is on. The following error is returned:

  Can’t configure speed <1G when Asymmetric flowcontrol is on, config ignored
- Dell Networking OS only supports \texttt{rx on tx on} and \texttt{rx off tx off} for speeds less than 1 Gig (Symmetric).
- On the C-Series and S-Series systems, the flow-control sender and receiver must be on the same port-pipe. Flow control is not supported across different port-pipes on the C-Series or S-Series system.

**Example**

Figure 23-4. `show running config` (partial)

```
FTOS(conf-if-gi-0/1)#show config
!
interface GigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...
```

The table below displays how Dell Networking OS negotiates the flow control values between two Dell Networking chassis connected back-to-back using 1G copper ports.

**Table 23-1. Negotiated Flow Control Values**

<table>
<thead>
<tr>
<th>Configured</th>
<th>Negotiated</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocRxConf</td>
<td>LocTxConf</td>
</tr>
<tr>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>off</td>
<td>on</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show running-config` Display the flow configuration parameters (non-default values only).
- `show interfaces` Display the negotiated flow control parameters.
**interface**

Configure a physical interface on the switch.

**Syntax**

```
interface interface
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface</strong></td>
<td>Enter one of the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td>-</td>
<td>For 100/1000 Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td>-</td>
<td>For a 1-Gigabit Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td>-</td>
<td>For SONET interfaces, enter the keyword <strong>sonet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td>-</td>
<td>For a 10-Gigabit Ethernet interface, enter the keyword <strong>TenGigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td>-</td>
<td>For a 40-Gigabit Ethernet interface, enter the keyword <strong>fortyGigE</strong> followed by the slot/port information.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS(conf)#interface gig 0/0
FTOS(conf-if-gi-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 **switchport** command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface loopback</td>
<td>Configure a Loopback interface.</td>
</tr>
<tr>
<td>interface null</td>
<td>Configure a Null interface.</td>
</tr>
<tr>
<td>interface port-channel</td>
<td>Configure a port channel.</td>
</tr>
<tr>
<td>interface sonet</td>
<td>Configure a SONET interface.</td>
</tr>
<tr>
<td>interface vlan</td>
<td>Configure a VLAN.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Display 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 8.1.1.0  Introduced on E-Series ExaScale
- Version 7.6.1.0  Introduced on S-Series
- Version 7.5.1.0  Introduced on C-Series
- Version 6.4.1.0  Introduced

**Example**

```
Figure 23-6. interface loopback Command Example

FTOS(conf)#interface loopback 1655
FTOS(conf-if-lo-1655)#
```

**Related Commands**

- `interface` Configure a physical interface.
- `interface null` Configure a Null interface.
- `interface port-channel` Configure a port channel.
- `interface vlan` Configure a VLAN.

interface ManagementEthernet

Configure the Management port on the system (either the Primary or Standby RPM).

**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 8.1.1.0  Introduced on E-Series ExaScale
- Version 7.5.1.0  Introduced for C-Series
- Version 6.4.1.0  Introduced for E-Series
**Example**

Figure 23-7. 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.

If two RPMs are installed in your system, use the `show redundancy` command to display which RPM is the Primary RPM.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>management route</td>
<td>Configure a static route that points to the Management interface or a forwarding router.</td>
</tr>
<tr>
<td>duplex (Management)</td>
<td>Clear FIB entries on a specified line card.</td>
</tr>
<tr>
<td>speed (Management interface)</td>
<td>Clear FIB entries on a specified line card.</td>
</tr>
</tbody>
</table>

**interface null**

Configure a Null interface on the switch.

**Syntax**

```
interface null number
```

**Parameters**

| `number` | Enter zero (0) as the Null interface number. |

**Defaults**

Not configured; `number = 0`

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

Figure 23-8. interface null Command Example

```
FTOS(conf)#interface null 0
FTOS(conf-if-nu-0)#
```

**Usage Information**

You cannot delete the Null interface. The only configuration command possible in a Null interface is `ip unreachables`.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configure a physical interface.</td>
</tr>
<tr>
<td>interface loopback</td>
<td>Configure a Loopback interface.</td>
</tr>
<tr>
<td>interface port-channel</td>
<td>Configure a port channel.</td>
</tr>
<tr>
<td>interface vlan</td>
<td>Configure a VLAN.</td>
</tr>
<tr>
<td>ip unreachables</td>
<td>Enable 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, identical commands can be entered for a range of interface.

Syntax

```
interface range interface , interface , ...
```

Parameters

`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 gigabitethernet 0/1 - 5` is valid; `interface range gigabitethernet 0/1-5` is not valid.

- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a Port Channel interface, enter the keyword port-channel followed by a number:
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword sonet followed by the 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.
- For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

Defaults

This command has no default behavior or values.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

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 23-9. Bulk Configuration Warning Message

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

Example Figure 23-10. Interface Range prompt with Multiple Ports

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

Example Figure 23-11. Interface Range prompt Overlapping Port Ranges

```
FTOS(conf)#interface range gi 2/1 - 11 , gi 2/1 - 23
FTOS(conf-if-range-gi-2/1-23#)
```

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 can not 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, port-channel, and SONET interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN, port-channel or SONET, only those respective interfaces should be configured in a particular range.

The following figure is an example of a single range bulk configuration.

Example Figure 23-12. Single Range Bulk Configuration

```
FTOS(config)# interface range gigabitethernet 5/1 - 23
FTOS(config-if-range)# no shutdown
FTOS(config-if-range)#
```

The following figure shows how to use commas to add different interface types to the range enabling all Gigabit Ethernet interfaces in the range 5/1 to 5/23 and both Ten Gigabit Ethernet interfaces 1/1 and 1/2.

Example Figure 23-13. Multiple Range Bulk Configuration Gigabit Ethernet and Ten Gigabit Ethernet

```
FTOS(config-if)# interface range gigabitethernet 5/1 - 23, tengigabitethernet 1/1 - 2
FTOS(config-if-range)# no shutdown
FTOS(config-if-range)#
```
The following figure shows how to use commas to add SONET, VLAN, and port-channel interfaces to the range.

Example Figure 23-14. Multiple Range Bulk Configuration with SONET, VLAN, and port channel

FTOS(config-if)# interface range gigabitethernet 5/1 - 23, tengigabitethernet 1/1 – 2, Vlan 2 – 100 , Port 1 – 25
FTOS(config-if-range)# no shutdown
FTOS(config-if-range)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel</td>
<td>Configure a port channel group.</td>
</tr>
<tr>
<td>interface vlan</td>
<td>Configure a VLAN interface.</td>
</tr>
<tr>
<td>show config (from INTERFACE RANGE mode)</td>
<td>Show the bulk configuration interfaces.</td>
</tr>
<tr>
<td>show range</td>
<td>Show the bulk configuration ranges.</td>
</tr>
<tr>
<td>interface range macro (define)</td>
<td>Define 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

- `name`: Enter up to 16 characters for the macro name.
- `interface, interface, ...`: Enter the `interface` keyword (see below) and one of the interfaces slot/port, port-channel or VLAN numbers. Select the range of interfaces for bulk configuration. You can enter up to six comma separated ranges—spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, `interface range gigabitethernet 0/1 - 5` is valid; `interface range gigabitethernet 0/1-5` is not valid.
- `GigabitEthernet`: Followed by the slot/port information.
- `port-channel`: Followed by a number:
  - **C-Series and S-Series**: Range: 1-128
  - **E-Series**: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- `sonet`: Followed by the slot/port information.
- `TenGigabitEthernet`: Followed by the slot/port information.
- `fortyGigE`: Followed by the slot/port information.
- `vlan`: Followed by a number from 1 to 4094.

Defaults

This command has no default behavior or value

Command Modes

CONFIGURATION
**Example**

**Figure 23-15. define interface-range macro Command Example**

FTOS(config)#define interface-range test tengigabitethernet 0/0 - 3, gigabitethernet 5/0 - 47 , gigabitethernet 13/0 - 89

FTOS#show running-config | grep define
define interface-range test tengigabitethernet 0/0 - 3, gigabitethernet 5/0 - 47, gigabitethernet 13/0 - 89
FTOS(config)#interface range macro test
FTOS(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#

**Usage Information**
The above figure is an example of how to define an interface range macro named test. Execute the `show running-config` command to display the macro definition.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface range macro</td>
<td>Configure a range of command (bulk configuration)</td>
</tr>
<tr>
<td>interface range macro name</td>
<td>Run an interface range macro.</td>
</tr>
</tbody>
</table>

**interface range macro name**

- **Syntax**
  
  `interface range macro name`

- **Parameters**
  
  - `name` Enter the name of an existing macro.

- **Defaults**
  
  This command has no default behavior or value

- **Command Modes**
  
  `CONFIGURATION`

- **Command History**
  
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code></td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

- **Usage Information**
  
  The following figure runs the macro named `test` that was defined earlier.

- **Example**
  
  **Figure 23-16. interface-range macro Command Example**

  FTOS(config)#interface range macro test
  FTOS(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#
**interface vlan**

Configure a VLAN. You can configure up to 4094 VLANs.

**Syntax**

```plaintext
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 8.2.1.0** Support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.
- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **pre-Version 6.2.1.0** Introduced for E-Series

**Example**

```plaintext
Figure 23-17.  interface vlan Command Example

FTOS(conf)#int vlan 3
FTOS(conf-if-vl-3)#
```

**Usage Information**

For more information on 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. See **Chapter 9, Access Control Lists (ACL)**.

**Related Commands**

- `interface` Configure a physical interface.
- `interface loopback` Configure a loopback interface.
- `interface null` Configure a null interface.
- `interface port-channel` Configure a port channel group.
- `show vlan` Display the current VLAN configuration on the switch.
- `shutdown` Disable/Enable the VLAN.
- `tagged` Add a Layer 2 interface to a VLAN as a tagged interface.
- `untagged` Add a Layer 2 interface to a VLAN as an untagged interface.
**ipg (Gigabit Ethernet interfaces)**

Set the Inter-packet gap (IPG) to 8 bytes for traffic on a Gigabit Ethernet interface.

**Syntax**

```
ipg 8
```

To return to the default setting, enter `no ipg`.

**Parameters**

- `8` Enter the keyword `8` to set the IPG to 8 bytes.

**Defaults**

12 bytes

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

- For 1-Gigabit Ethernet interfaces only.

**Note:** This command is an EtherScale only command.

---

**ipg (10 Gigabit Ethernet interfaces)**

Set the Inter-packet Gap for traffic on 10 Gigabit Ethernet interface.

**Syntax**

```
ipg {ieee-802.3ae | shrink}
```

To return to the default of averaging the IPG, enter `no ipg {shrink | ieee-802.3ae}`

**Parameters**

- `ieee-802.3ae` Enter the keyword `ieee-802.3ae` to set the IPG to 12 (12-15) bytes (packet size dependent)
- `shrink` Enter the keyword `shrink` to set the IPG to 8 (8-11) bytes (packet size dependent).

**Defaults**

averaging the IPG

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series (EtherScale-only)</td>
</tr>
</tbody>
</table>

**Usage Information**

- For 10 Gigabit Ethernet interfaces only.

- IPG equals 96 bits times from end of the previous packet to start of the pre-amble of the next packet.
**keepalive**

On SONET interfaces, send keepalive packets periodically to keep an interface alive when it is not transmitting data.

**Syntax**

```
keepalive [seconds]
```

To stop sending SONET keepalive packets, enter `no keepalive`.

**Parameters**

- `seconds` (OPTIONAL) For SONET interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets.
  - Range: 0 to 23767
  - Default: 10 seconds

**Defaults**

Enabled

**Command Modes**

INTERFACE

**Command History**

- Version 8.1.1.2 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.0 Introduced for E-Series

**Usage Information**

When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

---

**lfs enable (EtherScale)**

Enable Link Fault Signaling (LFS) on EtherScale 10 Gigabit Ethernet interfaces only.

**Syntax**

```
lfs enable
```

To disable LFS, enter `no lfs enable`.

**Defaults**

Enabled.

**Command Modes**

INTERFACE (10 Gigabit Ethernet interfaces only)

**Command History**

- pre-Version 6.1.1.0 Introduced for E-Series

**Usage Information**

If there is a failure on the link, FTOS brings down the interface. The interface will stay down until the link failure signal stops.

On TeraScale line cards, LFS is always enabled by default.
**linecard port portmode quad**

Split a single 40G port into 4-10G ports on the C-series.

**Syntax**

```
linecard slot-number port port-number portmode quad
```

**Parameters**

- **slot-number**
  - Enter a number for the line card slot.
  - C-Series Range: 0-7 for C7008/C300; 0-3 for C7004/C150.

- **port-number**
  - Enter the port number of the 40G port to be split. For the C-series, enter one of the following port numbers: 0, 4, 8, 12, 16 or 20.

**Defaults**

Disabled.

**Command Modes**

Configuration

**Command History**

- Version 8.4.6.0 Introduced for C-Series

**Usage Information**

Splitting a 40G port into 4x10G ports is supported. The 40G port 20 can split into 3x10G ports only. After the port is split, the 40G port is lost in the configuration. As a result, you must ensure that this port is also removed from the other L2/L3 feature configurations.

You must reload the system after issuing this command for the changes to take effect. You cannot use this command if LR4 optics are inserted on the 40G interface.

**link debounce-timer**

Assign the debounce time for link change notification on this interface.

**Syntax**

```
link debounce [milliseconds]
```

**Parameters**

- **milliseconds**
  - Enter the time to delay link status change notification on this interface.
  - Range: 100-5000 ms
  - • Default for copper is 3100 ms
  - • Default for fiber is 100 ms

**Command Modes**

- INTERFACE

**Command History**

- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on E-Series

**Usage Information**

Changes do not affect any ongoing debounces. The timer changes take effect from the next debounce onward.
Monitor counters on a single interface or all interfaces on a line card. The screen is refreshed every 5 seconds and the CLI prompt disappears.

**Syntax**

```plaintext
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 an 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For the management port, enter the keyword `managementethernet` followed by the slot (0-1) and the port (0).
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code></td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The delta column displays changes since the last screen refresh.
### Figure 23-18. monitor Command Example of a Single Interface

**systest-3**  
Monitor time: 00:00:06  
Refresh Intvl.: 2s  
Time: 03:26:26

Interface: Gi 0/3, Enabled, Link is Up, Linespeed is 1000 Mbit

<table>
<thead>
<tr>
<th>Traffic statistics:</th>
<th>Current</th>
<th>Rate</th>
<th>Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input bytes:</td>
<td>9069828</td>
<td>43 Bps</td>
<td>86</td>
</tr>
<tr>
<td>Output bytes:</td>
<td>606915800</td>
<td>43 Bps</td>
<td>87</td>
</tr>
<tr>
<td>Input packets:</td>
<td>54001</td>
<td>0 pps</td>
<td>1</td>
</tr>
<tr>
<td>Output packets:</td>
<td>9401589</td>
<td>0 pps</td>
<td>1</td>
</tr>
<tr>
<td>64B packets:</td>
<td>67</td>
<td>0 pps</td>
<td>0</td>
</tr>
<tr>
<td>Over 64B packets:</td>
<td>49166</td>
<td>0 pps</td>
<td>1</td>
</tr>
<tr>
<td>Over 127B packets:</td>
<td>350</td>
<td>0 pps</td>
<td>0</td>
</tr>
<tr>
<td>Over 255B packets:</td>
<td>1351</td>
<td>0 pps</td>
<td>0</td>
</tr>
<tr>
<td>Over 511B packets:</td>
<td>286</td>
<td>0 pps</td>
<td>0</td>
</tr>
<tr>
<td>Over 1023B packets:</td>
<td>2781</td>
<td>0 pps</td>
<td>0</td>
</tr>
</tbody>
</table>

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  
c - Clear screen  
l - Page up  
a - Page down  
T - Increase refresh interval  
t - Decrease refresh interval  
q - Quit

### Figure 23-19. monitor Command Example of All Interfaces on a Line Card

**systest-3**  
Monitor time: 00:01:31  
Refresh Intvl.: 2s  
Time: 03:54:14

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>In Packets</th>
<th>[delta]</th>
<th>Out Packets</th>
<th>[delta]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 0/0</td>
<td>Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi 0/1</td>
<td>Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi 0/2</td>
<td>Up</td>
<td>61512</td>
<td>52</td>
<td>66160</td>
<td>42</td>
</tr>
<tr>
<td>Gi 0/3</td>
<td>Up</td>
<td>63086</td>
<td>20</td>
<td>9405888</td>
<td>24</td>
</tr>
<tr>
<td>Gi 0/4</td>
<td>Up</td>
<td>14697471418</td>
<td>2661481</td>
<td>13392989657</td>
<td></td>
</tr>
<tr>
<td>Gi 0/5</td>
<td>Up</td>
<td>3759</td>
<td>3</td>
<td>161959604</td>
<td>832816</td>
</tr>
<tr>
<td>Gi 0/6</td>
<td>Up</td>
<td>4070</td>
<td>3</td>
<td>8680346</td>
<td>5</td>
</tr>
<tr>
<td>Gi 0/7</td>
<td>Up</td>
<td>61934</td>
<td>34</td>
<td>138734357</td>
<td>72</td>
</tr>
<tr>
<td>Gi 0/8</td>
<td>Up</td>
<td>61427</td>
<td>1</td>
<td>59960</td>
<td>1</td>
</tr>
<tr>
<td>Gi 0/9</td>
<td>Up</td>
<td>62039</td>
<td>53</td>
<td>104239232</td>
<td>3</td>
</tr>
<tr>
<td>Gi 0/10</td>
<td>Up</td>
<td>17740044091</td>
<td>37</td>
<td>7373849244</td>
<td>79</td>
</tr>
<tr>
<td>Gi 0/11</td>
<td>Up</td>
<td>18182889225</td>
<td>44</td>
<td>7184747584</td>
<td>138</td>
</tr>
<tr>
<td>Gi 0/12</td>
<td>Up</td>
<td>18182682056</td>
<td>0</td>
<td>3682</td>
<td>1</td>
</tr>
<tr>
<td>Gi 0/13</td>
<td>Up</td>
<td>18182681434</td>
<td>43</td>
<td>6592378911</td>
<td>144</td>
</tr>
<tr>
<td>Gi 0/14</td>
<td>Up</td>
<td>61349</td>
<td>55</td>
<td>86281941</td>
<td>15</td>
</tr>
<tr>
<td>Gi 0/15</td>
<td>Up</td>
<td>59808</td>
<td>58</td>
<td>62060</td>
<td>27</td>
</tr>
<tr>
<td>Gi 0/16</td>
<td>Up</td>
<td>59889</td>
<td>1</td>
<td>61616</td>
<td>1</td>
</tr>
<tr>
<td>Gi 0/17</td>
<td>Up</td>
<td>0</td>
<td>0</td>
<td>14950126</td>
<td>81293</td>
</tr>
<tr>
<td>Gi 0/18</td>
<td>Up</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi 0/19</td>
<td>Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi 0/20</td>
<td>Up</td>
<td>62734</td>
<td>54</td>
<td>62766</td>
<td>18</td>
</tr>
<tr>
<td>Gi 0/21</td>
<td>Up</td>
<td>60198</td>
<td>9</td>
<td>200899</td>
<td>9</td>
</tr>
<tr>
<td>Gi 0/22</td>
<td>Up</td>
<td>17304741100</td>
<td>3157554</td>
<td>10102508511</td>
<td></td>
</tr>
<tr>
<td>Gi 0/23</td>
<td>Up</td>
<td>17304769659</td>
<td>3139507</td>
<td>713354895</td>
<td>523329</td>
</tr>
</tbody>
</table>

m - Change mode  
c - Clear screen  
b - Display bytes  
r - Display pkts/bytes per sec  
l - Page up  
a - Page down
mtu

Set the maximum Link MTU (frame size) for an Ethernet interface.

Syntax

```
mtu value
```

To return to the default MTU value, enter `no mtu`.

Parameters

- **value**
  
  Enter a maximum frame size in bytes.

  Range: 594 to 9252

  Default: 1554

Defaults

1554

Command Modes

INTERFACE

Command History

- **Version 8.1.1.0**
  
  Introduced on E-Series ExaScale

- **Version 7.5.1.0**
  
  Introduced on C-Series

- **Pre-Version 6.2.1.0**
  
  Introduced for E-Series

Usage Information

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (`ip mtu` command) must be enough bytes to include the Layer 2 header:

- On C-Series, the IP MTU will get adjusted automatically when the Layer 2 MTU is configured with the `mtu` command.
- On the E-Series, you must compensate for a Layer 2 header when configuring IP MTU and link MTU on an Ethernet interface. Use the `ip mtu` command.
When you enter the **no mtu** command, FTOS reduces the IP MTU value to 1536 bytes. On the E-Series, to return the IP MTU value to the default, enter **no ip mtu**.

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 23-3. 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
This command is supported on C-Series, S-Series, and E-Series (TeraScale and ExaScale) 10/100/1000 Base-T Ethernet interfaces.

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.

⚠️ **Note:** The **mode** option is not available on non-10/100/1000 Base-T Ethernet line cards.

**Figure 23-20. negotiation auto Master/Slave Example**

```
FTOS(conf)# int gi 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.

**Figure 23-21. Display Auto-negotiation Master/Slave Setting (partial)**

```
FTOS#show interfaces configured
GigabitEthernet 13/18 is up, line protocol is up
Hardware is Force10Eth, 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
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:
...
```
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 10/100/1000 Base-T Ethernet interfaces.

### Table 23-4. Auto-negotiation and Link Speed Combinations

<table>
<thead>
<tr>
<th>Port 0</th>
<th>Port 1</th>
<th>Link Status between Port 1 and Port 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-negotiation enabled* speed 1000 or auto</td>
<td>auto-negotiation enabled* speed 1000 or auto</td>
<td>Up at 1000 Mb/s</td>
</tr>
<tr>
<td>auto-negotiation enabled speed 100</td>
<td>auto-negotiation enabled speed 100</td>
<td>Up at 100 Mb/s</td>
</tr>
<tr>
<td>auto-negotiation disabled speed 100</td>
<td>auto-negotiation disabled speed 100</td>
<td>Up at 100 Mb/s</td>
</tr>
<tr>
<td>auto-negotiation disabled speed 100</td>
<td>auto-negotiation enabled 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 10/100/1000 interfaces)**
  
  Set the link speed to 10, 100, 1000 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)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series and S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series only</td>
</tr>
</tbody>
</table>
**Example**  
**Figure 23-22. portmode hybrid configuration example**

FTOS(conf)#interface gi 7/0  
FTOS(conf-if-gi-7/0)#portmode hybrid  
FTOS(conf-if-gi-7/0)#interface vlan 10  
FTOS(conf-if-vl-10)#untagged gi 7/0  
FTOS(conf-if-vl-10)#interface vlan 20  
FTOS(conf-if-vl-20)#tagged gi 7/0  
FTOS(conf-if-vl-20)#

**Usage Information**
The figure above 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 23-23. Display the Tagged Hybrid Interface**

FTOS(conf-if-vl-20)#do show interfaces switchport  
Name: GigabitEthernet 7/0  
802.1QTagged: Hybrid  
Vlan membership:  
Vlan 10, Vlan 20  
Native VlanId: 10  
FTOS(conf-if-vl-20)#

The figure below is an example 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 23-24. Unconfigure the hybrid port**

FTOS(conf-if-vl-20)#interface vlan 10  
FTOS(conf-if-vl-10)#no untagged gi 7/0  
FTOS(conf-if-vl-10)#interface vlan 20  
FTOS(conf-if-vl-20)#no tagged gi 7/0  
FTOS(conf-if-vl-20)#interface gi 7/0  
FTOS(conf-if-vl-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>Display the configuration of switchport (Layer 2) interfaces on the switch.</td>
</tr>
<tr>
<td>switchport</td>
<td>Place the interface in a Layer 2 mode.</td>
</tr>
<tr>
<td>vlan-stack trunk</td>
<td>Specify 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: 30 to 299 seconds

Note: Since polling occurs every 15 seconds, the number of seconds designated here will round to the multiple of 15 seconds lower than the entered value. For example, if 44 seconds is designated it will round to 30; 45 to 59 seconds will round to 45, and so forth.

Defaults

299 seconds

Command Modes

INTERFACE

Command History

Version 8.1.1.0  Introduced on E-Series ExaScale
Version 7.6.1.0  Introduced on S-Series
Version 7.5.1.0  Introduced on C-Series
Version 6.1.1.0  Introduced

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  Display information on physical and virtual interfaces.

show config

Display the interface configuration.

Syntax

show config

Command Modes

INTERFACE

Command History

Version 8.1.1.0  Introduced on E-Series ExaScale
Version 7.6.1.0  Introduced on S-Series
Version 7.5.1.0  Introduced on C-Series
pre-Version 6.2.1.0  Introduced for E-Series

Example

Figure 23-25.  show config Command Example for the INTERFACE Mode

FTOS(conf-if)#show conf
!
interface GigabitEthernet 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)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 23-26. show config (Bulk Configuration) Command Example**

```
FTOS(conf)#interface range gigabitethernet 1/1 - 2
FTOS(conf-if-range-gi-1/1-2)#show config
!
interface GigabitEthernet 1/1
 no ip address
 switchport
 no shutdown
!
interface GigabitEthernet 1/2
 no ip address
 switchport
 no shutdown
FTOS(conf-if-range-gi-1/1-2)#
```

show interfaces

Display information on a specific physical interface or virtual interface.

**Syntax**

```
show interfaces interface
```

**Parameters**

<table>
<thead>
<tr>
<th>interface</th>
<th>Enter one of the following keywords and slot/port or number information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For a Fast Ethernet interface, enter the keyword <code>FastEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Loopback interface, enter the keyword <code>loopback</code> followed by a number from 0 to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For the management interface on an RPM, enter the keyword <code>ManagementEthernet</code> followed by the slot/port information. The slot range is 0-1 and the port range is 0.</td>
</tr>
<tr>
<td></td>
<td>• For a Null interface, enter the keywords <code>null</code> followed by a number.</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><strong>C-Series and S-Series</strong> Range: 1-128</td>
</tr>
<tr>
<td></td>
<td><strong>E-Series</strong> Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For a SONET interface, enter the keyword <code>sonet</code> followed by the slot/port.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN interface, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>
Use this `show interfaces` command for details on a specific interface. Use the `show interfaces linecard` command for details on all interfaces on the designated line card.

Note that, in an E-Series EtherScale chassis, the `show interfaces` command output does not include details about installed SFP or XFP transceivers.

**Example**

**Figure 23-27. show interfaces Command Example for 10G Port (EtherScale in E-Series)**

```
FTOS#show interfaces tengigabitethernet 2/0
TenGigabitEthernet 2/0 is up, line protocol is up
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 23-5. Lines in show interfaces Command Example (EtherScale)**

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet 2/0</td>
<td>Displays the interface’s type, slot/port, and administrative and line protocol status.</td>
</tr>
<tr>
<td>Hardware is...</td>
<td>Displays the interface’s hardware information and its assigned MAC address.</td>
</tr>
<tr>
<td>Interface index...</td>
<td>Displays the interface index number used by SNMP to identify the interface.</td>
</tr>
<tr>
<td>Internet address...</td>
<td>States whether an IP address is assigned to the interface. If one is, that address is displayed.</td>
</tr>
</tbody>
</table>
Table 23-5. Lines in show interfaces Command Example (EtherScale) (continued)

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 <code>show interfaces</code> counters where cleared.</td>
</tr>
<tr>
<td>Queuing strategy...</td>
<td>States the packet queuing strategy. FIFO means first in first out.</td>
</tr>
</tbody>
</table>

Input Statistics: Displays all the input statistics including:
- Number of packets and bytes into the interface
- Number of packets with IP headers, VLAN tagged headers and MPLS headers

**Note:** The sum of the number of packets may not be as expected since a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.
- Packet size and the number of those packets inbound to the interface
- Number of symbol errors, runts, giants, and throttles packets:
  - symbol errors = number packets containing bad data. That is, the port MAC detected a physical coding error in the packet.
  - runts = number of packets that are less than 64B
  - giants = packets that are greater than the MTU size
  - throttles = packets containing PAUSE frames

**Note:** Symbol errors is supported on E-Series EtherScale only.
- Number of CRC, IP Checksum, overrun, and discarded packets:
  - CRC = packets with CRC/FCS errors
  - IP Checksum = packets with IP Checksum errors
  - overrun = number of packets discarded due to FIFO overrun conditions
  - discarded = the sum of input symbol errors, runts, giants, CRC, IP Checksum, and overrun packets discarded without any processing

Output Statistics: Displays output statistics sent out of the interface including:
- Number of packets, bytes and underruns out of the interface
  - packets = total number of packets
  - bytes = total number of bytes
  - underruns = number of packets with FIFO underrun conditions
- Number of Multicast, Broadcast and Unicast packets:
  - Multicasts = number of MAC multicast packets
  - Broadcasts = number of MAC broadcast packets
  - Unicasts = number of MAC unicast packets
- Number of IP, VLAN and MPLS packets:
  - IP Packets = number of IP packets
  - Vlans = number of VLAN tagged packets
  - MPLS = number of MPLS packets (found on a LSR interface)
- Number of throttles and discards packets:
  - throttles = packets containing PAUSE frames
  - discarded = number of packets discarded without any processing
Table 23-5. Lines in show interfaces Command Example (EtherScale) (continued)

<table>
<thead>
<tr>
<th>Line Description</th>
<th>Rate information... Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds). Traffic rate is displayed in bits, packets per second, and percent of line rate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time since...</td>
<td>Elapsed time since the last interface status change (hh:mm:ss format).</td>
</tr>
</tbody>
</table>

Example

**Figure 23-28. show interfaces Command Example for 10G (TeraScale)**

```
FTOS#show interfaces tengigabitethernet 0/0
TenGigabitEthernet 3/0 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:41:77:c5
  Current address is 00:01:e8:41:77:c5
Pluggable media present, XFP type is 10GBASE-SR
  Medium is MultiRate, Wavelength is 850.00nm
  XFP receive power reading is -2.4834
Interface index is 134545468
Port will not be disabled on partial SFM failure
MTU 9252 bytes, IP MTU 9234 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx on
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:15:14
Queueing strategy: fifo
Input Statistics:
  4410013700 packets, 282240876800 bytes
  0 Vlans
  4410013700 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:
  857752 packets, 54894840 bytes, 0 underruns
  857752 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
  24 Multicasts, 0 Broadcasts, 857708 Unicasts
  0 Vlans, 0 throttles, 0 discarded, 0 collisions, 4409143619 wredDrops
Rate info (interval 30 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: 00:12:14
FTOS#
```

Table 23-6. Fields in show interfaces Command Example (TeraScale)

<table>
<thead>
<tr>
<th>Line Description</th>
<th>TenGigabitEthernet 0/0... Interface type, slot/port and administrative and line protocol status.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware is...</td>
<td>Interface hardware information, assigned MAC address, and current address.</td>
</tr>
</tbody>
</table>
| Pluggable media present... | Present pluggable media wavelength, type, and rate. The error scenarios are:  
  - Wavelength, Non-qualified — Dell Networking ID is not present, but wavelength information is available from XFP or SFP serial data  
  - Wavelength, F10 unknown — Dell Networking ID is present, but not able to determine the optics type  
  - Unknown, Non-qualified — if wavelength is reading error, and F10 ID is not present  
  Dell Networking allows unsupported SFP and XFP transceivers to be used, but Dell Networking OS might not be able to retrieve some data about them. In that case, typically when the output of this field is “Pluggable media present, Media type is unknown”, the Medium and the XFP/SFP receive power reading data might not be present in the output. |
<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td>LineSpeed</td>
<td>Displays the interface’s line speed, duplex mode, and Slave</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 where cleared.</td>
</tr>
<tr>
<td>Queuing strategy...</td>
<td>States the packet queuing strategy. FIFO means first in first out.</td>
</tr>
<tr>
<td>Input Statistics:</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 VLAN tagged headers</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 Multicast and Broadcast 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>• Number of runts, giants, and throttles packets:</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, overrun, and discarded packets:</td>
</tr>
<tr>
<td></td>
<td>CRC = packets with CRC/FCS 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 runts, giants, CRC, and overrun packets discarded without any</td>
</tr>
<tr>
<td></td>
<td>processing</td>
</tr>
<tr>
<td>Output Statistics:</td>
<td>Displays output statistics sent out 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>• Packet size and the number of those packets outbound to the interface</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 VLANs, throttles, discards, and collisions:</td>
</tr>
<tr>
<td></td>
<td>Vlans = number of VLAN tagged 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></td>
<td>collisions = number of packet collisions</td>
</tr>
<tr>
<td></td>
<td>wred = count both packets discarded in the MAC and in the hardware-based queues</td>
</tr>
<tr>
<td>Rate information...</td>
<td>Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds)</td>
</tr>
<tr>
<td></td>
<td>Traffic rate is displayed in bits, packets per second, and percent of line rate.</td>
</tr>
<tr>
<td>Time since...</td>
<td>Elapsed time since the last interface status change (hh:mm:ss format).</td>
</tr>
</tbody>
</table>
FTOS#show interfaces gigabitethernet 2/0
GigabitEthernet 2/0 is up, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:41:77:95
Current address is 00:01:e8:41:77:95
Pluggable media present, SFP type is 1000BASE-SX
Wavelength is 850nm
Interface index is 100974648
Port will not be disabled on partial SFM failure
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit
Flowcontrol rx on tx on
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 1w0d5h
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 Multicast, 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 Multicast, 0 Broadcasts, 0 Unicasts
  0 Vlans, 0 throttles, 0 discarded, 0 collisions, 0 wred drops
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: 1w0d5h
FTOS#

FTOS#show interfaces tengigabitethernet 0/44
TenGigabitEthernet 0/44 is down, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:32:44:26
Current address is 00:01:e8:32:44:26
Pluggable media present, SFP+ type is 10GBASE-CU5M
Medium is MultiRate
Interface index is 45417732
FTOS#

FTOS#show interfaces managementethernet 0/0
ManagementEthernet 0/0 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:0b:a9:4c
Current address is 00:01:e8:0b:a9:4c
Pluggable media not present
Interface index is 503595208
Internet address is 10.11.201.5/16
Link local IPv6 address: fe80::201:e8ff:fe0b:a94c/64
Global IPv6 address: 2222::5/64
Virtual-IP is not set
Virtual-IP IPv6 address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10 Mbit, Mode half duplex
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 04:01:08
Queueing strategy: fifo
  Input 943 packets, 78347 bytes, 190 multicast
  Received 0 errors, 0 discarded
  Output 459 packets, 102388 bytes, 15 multicast
  Output 0 errors, 0 invalid protocol
Time since last interface status change: 00:03:09
On the C-Series and S-Series, 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. If two RPMs are installed in your system, use the `show redundancy` command to display which RPM is the Primary RPM.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces configured</code></td>
<td>Display any interface with a non-default configuration.</td>
</tr>
<tr>
<td><code>show interfaces linecard</code></td>
<td>Display information on all interfaces on a specific line card.</td>
</tr>
<tr>
<td><code>show interfaces phy</code></td>
<td></td>
</tr>
<tr>
<td><code>show interfaces rate</code></td>
<td>Display information of either rate limiting or rate policing on the interface.</td>
</tr>
<tr>
<td><code>show interfaces switchport</code></td>
<td>Display Layer 2 information about the interfaces.</td>
</tr>
<tr>
<td><code>show inventory (C-Series and E-Series)</code></td>
<td>Display the chassis type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.</td>
</tr>
<tr>
<td><code>show inventory (S-Series)</code></td>
<td>Display the S-Series switch type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.</td>
</tr>
<tr>
<td><code>show ip interface</code></td>
<td>Display Layer 3 information about the interfaces.</td>
</tr>
<tr>
<td><code>show linecard</code></td>
<td>Display the line card(s) status.</td>
</tr>
<tr>
<td><code>show range</code></td>
<td>Display all interfaces configured using the interface range command.</td>
</tr>
</tbody>
</table>

**Note:** Unicast counters in the `show interface` output will increment when the interface receives multicast or broadcast packets.
show interfaces configured

Display any interface with a non-default configuration.

Syntax

```
show interfaces configured
```

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 6.4.1.0 Changed organization of display output

Example

```
FTOS#show interfaces configured
GigabitEthernet 13/18 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
  Current address is 00:01:e8:05:f7:fc
  Interface index is 474791997
  Internet address is 1.1.1.1/24
  MTU 1554 bytes, IP MTU 1500 bytes
  LineSpeed 1000 Mbit, Mode full duplex, Master
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interfaces" counters 00:12:42
  Queueing strategy: fifo
  Input Statistics:
    10 packets, 10000 bytes
    0 Vlans
    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 10 over 511-byte pkts, 0 over 1023-byte pkts
    0 Multicasts, 0 Broadcasts
    0 runts, 0 giants, 0 throttles
    0 CRC, 0 overrun, 0 discarded
  Output Statistics:
    1 packets, 64 bytes, 0 underruns
    1 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
    0 Multicasts, 1 Broadcasts, 0 Unicasts
    0 Vlans, 0 throttles, 0 discarded, 0 collisions
  Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Time since last interface status change: 00:04:59
FTOS#
```

Related Commands

- **show interfaces**
  Display information on a specific physical interface or virtual interface.
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 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - **C-Series** and **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword **sonet** followed by the 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.

- **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**

No default values or behavior

**Command Modes**

EXEC

**Command History**

- Version 8.4.6.0 Added support for the keyword **fortyGigE**
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 7.4.1.0 Introduced

**Example**

```
Figure 23-33. show interfaces dampening Command Example

<table>
<thead>
<tr>
<th>Interface</th>
<th>Supp</th>
<th>Flaps</th>
<th>Penalty</th>
<th>Half-Life</th>
<th>Reuse</th>
<th>Suppress</th>
<th>Max-Sup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 3/2</td>
<td>Up</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>800</td>
<td>4500</td>
<td>120</td>
</tr>
<tr>
<td>Gi 3/10</td>
<td>Up</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>750</td>
<td>2500</td>
<td>20</td>
</tr>
<tr>
<td>FTOS#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Related Commands**

- **dampening** Configure dampening on an interface
- **show interfaces** Display information on a specific physical interface or virtual interface.
- **show interfaces configured** Display any interface with a non-default configuration.
show interfaces debounce

Display information on interfaces with debounce timer configured.

Syntax

```
show interfaces debounce interface
```

Parameters

`interface` Enter one of the following keywords and slot/port or number information:
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Related Commands

- `show interfaces` Display information on a specific physical interface or virtual interface.

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 a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the 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.
- For Loopback interfaces, enter the keyword `loopback` followed by a number from 0 to 16383.
- For the management interface on the RPM, enter the keyword `ManagementEthernet` followed by the slot/port information. The slot range is 0-1 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: 
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For SONET interfaces, enter the keyword `sonet` followed by the slot/port.
- For VLAN interfaces, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege
Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Example

**Figure 23-34.  show interfaces description Command Example**

```plaintext
FTOS>
Interface                   OK? Status     Protocol  Description
GigabitEthernet 4/17       NO  admin down  down        ***connected-to-host***
GigabitEthernet 4/18       NO  admin down  down        ***connected-to-Tom***
GigabitEthernet 4/19       NO  admin down  down        ***connected-to-Marketing***
GigabitEthernet 4/20       NO  admin down  down        ***connected-to-Bill***
GigabitEthernet 4/21       NO  up        down        ***connected-to-Radius-Server***
GigabitEthernet 4/22       NO  admin down  down        ***connected-to-Web-Server***
GigabitEthernet 4/23       NO  admin down  down        ***connected-to-PC-client***
TenGigabitEthernet 6/0     NO  admin down  down
GigabitEthernet 8/0        YES up        up
GigabitEthernet 8/1        YES up        up
GigabitEthernet 8/2        YES up        up
GigabitEthernet 8/3        YES up        up
GigabitEthernet 8/4        YES up        up
GigabitEthernet 8/5        YES up        up
GigabitEthernet 8/6        YES up        up
GigabitEthernet 8/7        YES up        up
GigabitEthernet 8/8        YES up        up
GigabitEthernet 8/9        YES up        up
GigabitEthernet 8/10       YES up        up
GigabitEthernet 8/11       YES up        up
FTOS>
```

### Table 23-7.  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>
<tr>
<td>Protocol</td>
<td>States whether IP is enabled (up) or disabled (down) on the interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description (if any) manually configured for the interface.</td>
</tr>
</tbody>
</table>

Related Commands

- `show interfaces`  
  Display information on a specific physical interface or virtual interface.
show interfaces linecard

Display information on all interfaces on a specific line card.

Syntax

```
show interfaces linecard slot-number
```

Parameters

- `slot-number` Enter a number for the line card slot.
  - C-Series Range: 0-7 for C7008/C300; 0-3 for C7004/C150
  - E-Series Range: 0 to 13 on the E1200/1200i, 0 to 6 on the E600/600i, 0 to 5 on the E300

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.1.1.2 Introduced support on E-Series ExaScale E600i
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

Usage

The following figure shows a line card that has an XFP interface. The type, medium, wavelength, and receive power details are displayed. When a device that is not certified by Dell Networking is inserted, it might work, but its details might not be readable by Dell Networking OS and not displayed here.

Example

```
Figure 23-35. show interfaces linecard Command Example (in C7004/C150)

FTOS#show interfaces linecard 0
TenGigabitEthernet 0/0 is down, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:51:b2:d4
  Current address is 00:01:e8:51:b2:d4
  Pluggable media present, XFP type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850.00nm
    XFP receive power reading is -2.3538
  Interface index is 35883138
  Internet address is not set
  MTU 1554 bytes, IP MTU 1500 bytes
  LineSpeed 10000 Mbit
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters 20:16:29
  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
    --More--
```

Related Commands

- `show interfaces` Display information on a specific physical interface or virtual interface.
show interfaces phy

Display auto-negotiation and link partner information.

Syntax

show interfaces {gigabitethernet | tengigabitethernet | fortyGigE} slot/port phy

Parameters

- **gigabitethernet**: Enter the keyword `gigabitethernet` followed by the slot/port information.
- **tengigabitethernet**: Enter the keyword `tengigabitethernet` followed by the slot/port information.
- **fortyGigE**: Enter the keyword `fortyGigE` followed by the slot/port number.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.6.0: Added support for the keywords tengigabitethernet and fortyGigE.
- Version 8.1.1.0: Introduced on E-Series ExaScale
- Version 7.6.1.0: Introduced on C-Series and S-Series
- Version 6.5.4.0: Introduced on E-Series

Example

**Figure 23-36. show interfaces gigabitethernet phy Command Example (Partial)**

```
FTOS#show int gigabitethernet 1/0 phy
Mode Control:
  SpeedSelection: 10b
  AutoNeg: ON
  Loopback: False
  PowerDown: False
  Isolate: False
  DuplexMode: Full
Mode Status:
  AutoNegComplete: False
  RemoteFault: False
  LinkStatus: False
  JabberDetect: False
AutoNegotiation Advertise:
  100MegFullDplx: True
  100MegHalfDplx: True
  10MegFullDplx: False
  10MegHalfDplx: True
  Asym Pause: False
  Sym Pause: False
AutoNegotiation Remote Partner's Ability:
  100MegFullDplx: False
  100MegHalfDplx: False
  10MegFullDplx: False
  10MegHalfDplx: False
  Asym Pause: False
  Sym Pause: False
AutoNegotiation Expansion:
  ParallelDetectionFault: False
...
```

Table 23-8. Lines in show interfaces gigabitethernet Command Example

<table>
<thead>
<tr>
<th>Line Description</th>
<th>Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates if auto negotiation is enabled. If so, indicates the selected speed and duplex.</td>
<td>Mode Control</td>
</tr>
<tr>
<td>Displays auto negotiation fault information. When the interface completes auto negotiation successfully, the autoNegComplete field and the linkStatus field read “True.”</td>
<td>Mode Status</td>
</tr>
</tbody>
</table>
Table 23-8. Lines in show interfaces gigabitethernet Command Example

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoNegotiation Advertise</td>
<td>Displays the control words advertised by the local interface during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control supported by the local interface.</td>
</tr>
<tr>
<td>AutoNegotiation Remote Partner's Ability</td>
<td>Displays the control words advertised by the remote interface during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control supported by the remote interface</td>
</tr>
<tr>
<td>AutoNegotiation Expansion</td>
<td>ParallelDetectionFault is the handshaking scheme in which the link partner continuously transmit an “idle” data packet using the Fast Ethernet MLT-3 waveform. Equipment that does not support auto-negotiation must be configured to exactly match the mode of operation as the link partner or else no link can be established.</td>
</tr>
<tr>
<td>1000Base-T Control</td>
<td>1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting a speed to 1000 Mbps with the speed command without auto-negotiation. E-Series line cards support both full-duplex and half-duplex 1000BaseT.</td>
</tr>
</tbody>
</table>
| Phy Specific Control Values   | 0 - Manual MDI  
1 - Manual MDIX  
2 - N/A  
3 - Auto MDI/MDIX |
| Phy Specific Status Displays  | PHY-specific status information. Cable length represents a rough estimate in meters:  
0 - < 50 meters  
1 - 50 - 80 meters  
2 - 80 - 110 meters  
3 - 110 - 140 meters  
4 - 140 meters.  
Link Status:  
Up or Down  
Speed:  
Auto  
1000MB  
100MB  
10MB |

Related Commands

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

show interfaces stack-unit

Display information on all interfaces on a specific S-Series stack member.

**Syntax**

`show interfaces stack-unit unit-number`

**Parameters**

- `unit-number` Enter the stack member number (0 to 7).
show interfaces status

Display a summary of interface information or specify a line card slot and interface to display status information on that specific interface only.

Syntax  
show interfaces [interface | linecard slot-number] status
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 [linecard slot-number] | stack-unit unit-id ]
```
Parameters

**interface**

Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
- For a Port Channel interface, enter the keyword **port-channel** followed by a number:
  - **C-Series** and **S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. This keyword is only available on E-Series and C-Series.
- 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.

<table>
<thead>
<tr>
<th><strong>linecard</strong></th>
<th>(OPTIONAL) Enter the keyword <strong>linecard</strong> followed by the slot number. This option is available only on E-Series and C-Series.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>slot-number</strong></td>
<td><strong>C-Series</strong> Range: 0-7 for C7008/C300; 0-3 for C7004/C150</td>
</tr>
<tr>
<td></td>
<td><strong>E-Series</strong> Range: 0 to 13 on the E1200, 0 to 6 on the E6000, 0 to 5 on the E300</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>stack-unit</strong></th>
<th>(OPTIONAL) Enter the keyword <strong>stack-unit</strong> followed by the stack member number. This option is available only on S-Series.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>unit-id</strong></td>
<td><strong>Range:</strong> 0 to 1</td>
</tr>
</tbody>
</table>

Command Modes

**EXEC**

**EXEC Privilege**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support for 4093 VLANs on E-Series ExaScale</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for hybrid port/native VLAN, introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**E-Series legacy command**
**Example**

```
FTOS#show interfaces switchport
Name: GigabitEthernet 13/0
802.1QTagged: Hybrid
Vlan membership:
Vlan    2, Vlan  20
Native VlanId: 20

Name: GigabitEthernet 13/1
802.1QTagged: True
Vlan membership:
Vlan    2

Name: GigabitEthernet 13/2
802.1QTagged: True
Vlan membership:
Vlan    2

Name: GigabitEthernet 13/3
802.1QTagged: True
Vlan membership:
Vlan    2
--More--
```
**Command Modes**

**EXEC**

**EXEC Privilege**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Output augmented with diagnostic data for pluggable media.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Removed three fields in output: Vendor Name, Vendor OUI, Vendor PN.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series.</td>
</tr>
<tr>
<td>6.5.4.0</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>

**Usage**

See the figure below for an example screenshot, and see the following table or a description of the output fields.

For related commands, see the Related Commands section, below, and see the Debugging and Diagnostics chapter for your platform at the end of this book.
Example

Figure 23-40. show interfaces gigabitethernet transceiver Command Example

FTOS#show interfaces gigabitethernet 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) 100m = 0x00
SFP 0 Length(50um) 10m = 0x1e
SFP 0 Length(62.5um) 10m = 0x0f
SFP 0 Length(Copper) 10m = 0x00
SFP 0 Vendor Rev = A
SFP 0 Laser Wavelength = 850 nm
SFP 0 CheckCodeBase = 0x66
SFP 0 Serial Extended ID fields
SFP 0 Options= 0x00 0x12
SFP 0 BR max= 0
SFP 0 BR min= 0
SFP 0 Vendor SN= P5N1ACE
SFP 0 Datecode = 040528
SFP 0 CheckCodeExt = 0x5b

SFP 1 Diagnostic Information

SFP 1 Rx Power measurement type = Average
SFP 1 Temp High Alarm threshold = 95.000C
SFP 1 Voltage High Alarm threshold = 3.900V
SFP 1 Bias High Alarm threshold = 17.000mA
SFP 1 TX Power High Alarm threshold = 0.631mW
SFP 1 RX Power High Alarm threshold = 1.259mW
SFP 1 Temp Low Alarm threshold = -25.000C
SFP 1 Voltage Low Alarm threshold = 2.700V
SFP 1 Bias Low Alarm threshold = 1.000mA
SFP 1 TX Power Low Alarm threshold = 0.067mW
SFP 1 RX Power Low Alarm threshold = 0.010mW

SFP 1 Temperature = 39.930C
SFP 1 Voltage = 3.293V
SFP 1 Tx Bias Current = 6.894mA
SFP 1 Tx Power = 0.328mW
SFP 1 Rx Power = 0.000mW

SFP 1 Data Ready state Bar = False
SFP 1 Rx LOS state = True
SFP 1 Tx Fault state = False
SFP 1 Rate Select state = False
SFP 1 RS state = False
SFP 1 Tx Disable state = False

SFP 1 Temperature High Alarm Flag = False
SFP 1 Voltage High Alarm Flag = False
SFP 1 Tx Bias High Alarm Flag = False
SFP 1 Tx Power High Alarm Flag = False
SFP 1 RX Power High Alarm Flag = False
SFP 1 Temperature Low Alarm Flag = False
SFP 1 Voltage Low Alarm Flag = False
SFP 1 Tx Bias Low Alarm Flag = False
SFP 1 TX Power Low Alarm Flag = False
SFP 1 RX Power Low Alarm Flag = True

!-------output truncated -------------------------!
Table 23-10. 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” (Receiver optical modulation amplitude).</td>
</tr>
<tr>
<td>Temp High Alarm threshold</td>
<td>Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.</td>
</tr>
<tr>
<td>Voltage High Alarm threshold</td>
<td>Displays the interface index number used by SNMP to identify the interface.</td>
</tr>
<tr>
<td>Bias High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Power Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Current temperature of the sfps. If this temperature crosses Temp High alarm/warning thresholds, then the temperature high alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Voltage</td>
<td>Current voltage of the sfps. If this voltage crosses voltage high alarm/warning thresholds, then the voltage high alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Tx Bias Current</td>
<td>Present Tx bias current of the SFP. If this crosses bias high alarm/warning thresholds, then the tx bias high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, then the tx bias low alarm/warning flag is set to true.</td>
</tr>
</tbody>
</table>
### Table 23-10. 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 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 23-10. 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 displayed above.</td>
</tr>
<tr>
<td>Rx Power High Warning 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 Warning Flag</td>
<td>This can be either true or false, depending on the Current Temperature value displayed above.</td>
</tr>
<tr>
<td>Voltage Low 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 Low Warning 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 Low Warning 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 Warning Flag</td>
<td>This can be either true or false, depending on the Current Rx power value displayed above.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Configure 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>Display information on a specific physical interface or virtual interface.</td>
</tr>
<tr>
<td>show inventory (C-Series and E-Series)</td>
<td>Display the chassis type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.</td>
</tr>
<tr>
<td>show inventory (S-Series)</td>
<td>Display the S-Series switch type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.</td>
</tr>
</tbody>
</table>

show range

Display all interfaces configured using the interface range command.

Syntax

show range

Command Mode

INTERFACE RANGE (config-if-range)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Support for 4093 VLANs on E-Series ExaScale</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example

Figure 23-41. show range Command Example

```
FTOS(conf-if-range-so-2/0-1,fa-0/0)#show range
interface sonet 2/0 - 1
interface fastethernet 0/0
FTOS(conf-if-range-so-2/0-1,fa-0/0)#
```
**shutdown**

Disable an interface.

**Syntax**

```
shutdown
```

To activate an interface, enter **no shutdown**.

**Defaults**

The interface is disabled.

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series legacy command</td>
</tr>
</tbody>
</table>

**Usage Information**

The `shutdown` command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the `show ip interface brief` command. Disabled interfaces are listed as down.

Disabling a VLAN or a port channel causes different behavior. When a VLAN is disabled, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the `shutdown` command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, you must enter `no shutdown` on the port channel interface and at least one interface within that port channel.

The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port channel.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface port-channel</code></td>
<td>Create a port channel interface.</td>
</tr>
<tr>
<td><code>interface vlan</code></td>
<td>Create a VLAN.</td>
</tr>
<tr>
<td><code>show ip interface</code></td>
<td>Displays the interface routing status. Add the keyword <code>brief</code> to display a table of interfaces and their status.</td>
</tr>
</tbody>
</table>
speed (for 10/100/1000 interfaces)

Set the speed for 10/100/1000 Base-T Ethernet interfaces. Both sides of a link must be set to the same speed (10/100/1000) or to auto or the link may not come up.

Syntax

```
speed {10 | 100 | 1000 | auto}
```

To return to the default setting, use the `no speed {10 | 100 | 1000}` command.

Parameters

- **10**: Enter the keyword **10** to set the interface’s speed to 10 Mb/s.

  **Note:** This speed is not supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card. If the command is entered for these interfaces, an error message appears.

- **100**: Enter the keyword **100** to set the interface’s speed to 10/100 Mb/s.

  **Note:** When this setting is enabled, only 100Base-FX optics are supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card.

- **1000**: Enter the keyword **1000** to set the interface’s speed to 1000 Mb/s.

  (Auto-negotiation is enabled. See `negotiation auto` for more information)

  **Note:** When this setting is enabled, only 100Base-FX optics are supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card.

- **auto**: Enter the keyword **auto** to set the interface to auto-negotiate its speed.

  (Auto-negotiation is enabled. See `negotiation auto` for more information)

Defaults

**auto**

Command Modes

**INTERFACE**

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Supported on LC-EH-GE-50P or the LC-EJ-GE-50P cards</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

Usage Information

This command is found on the 10/100/1000 Base-T Ethernet interfaces.

When auto is enabled, the system performs and automatic discovery to determine the optics installed and configure the appropriate speed.

When you configure a speed for the 10/100/1000 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.

**Note:** Starting with Dell Networking OS 7.8.1.0, when a copper SFP2 module with catalog number GP-SFP2-1T is used in the S25P model of the S-Series, 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

- `duplex (10/100 Interfaces)`: Configure duplex mode on physical interfaces with the speed set to 10/100.

- `negotiation auto`: Enable or disable auto-negotiation on an interface.
speed (Management interface)

Set the speed for the Management interface.

Syntax

```
speed {10 | 100 | auto}
```

To return to the default setting, use the `no speed {10 | 100}` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Enter the keyword <code>10</code> to set the interface’s speed to 10 Mb/s.</td>
</tr>
<tr>
<td>100</td>
<td>Enter the keyword <code>100</code> to set the interface’s speed to 100 Mb/s.</td>
</tr>
<tr>
<td>auto</td>
<td>Enter the keyword <code>auto</code> to set the interface to auto-negotiate its speed.</td>
</tr>
</tbody>
</table>

Defaults

`auto`

Command Modes

`INTERFACE`

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

This command is found on the Management interface only.

Related Commands

- `interface ManagementEthernet` Configure the Management port on the system (either the Primary or Standby RPM).
- `duplex (Management)` Set the mode of the Management interface.
- `management route` Configure a static route that points to the Management interface or a forwarding router.

switchport

Place an interface in Layer 2 mode.

Syntax

```
switchport [backup interface {gigabit slotport | tengigabit slotport | port-channel number}]
```

To remove an interface from Layer 2 mode and place it in Layer 3 mode, enter `no switchport`. If a switchport backup interface is configured, you must first remove the backup configuration. To remove a switchport backup interface, enter `no switchport backup interface {gigabit slotport | tengigabit slotport | port-channel number}`.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup interface</td>
<td>Use this option to configure a redundant Layer 2 link without using Spanning Tree. This keyword configures a backup port so that if the primary port fails the backup port changes to the up state. If the primary later comes up, it becomes the backup.</td>
</tr>
<tr>
<td>gigabit</td>
<td>Enter this keyword if the backup port is a 1G port.</td>
</tr>
<tr>
<td>tengigabit</td>
<td>Enter this keyword if the backup port is a 10G port.</td>
</tr>
<tr>
<td>fortyGigE</td>
<td>Enter this keyword if the backup port is 40G port.</td>
</tr>
<tr>
<td>port-channel</td>
<td>Enter this keyword if the backup port is a static or dynamic port channel.</td>
</tr>
<tr>
<td>slot/port</td>
<td>Specify the line card and port number of the backup port.</td>
</tr>
</tbody>
</table>
Disabled (The interface is in Layer 3 mode.)

INTERFACE

<table>
<thead>
<tr>
<th>Command History</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added support for the keyword <strong>fortyGigE.</strong></td>
<td>Added support for port-channel interfaces (<strong>port-channel number</strong> option).</td>
</tr>
<tr>
<td>Introduced on E-Series ExaScale</td>
<td>Added <strong>backup interface</strong> option.</td>
</tr>
<tr>
<td>Introduced on S-Series</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>
| Introduced for E-Series | **wanport**

Enable the WAN mode on a TenGigabitEthernet interface.

**Syntax**

```
wanport
```

To disable the WAN Port, enter **no wanport.**

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

<table>
<thead>
<tr>
<th>Command History</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduced on E-Series ExaScale</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The port must be in a shutdown state to change from LAN mode to WAN mode and vice-versa as shown in the figure below.

For E-Series ExaScale systems, you must configure all the ports in a port-pipe to either WANPHY or non-WANPHY. They cannot be mixed on the same port-pipe.
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 Dell Networking OS, a LAG is referred to as a Port Channel.

**Table 23-11. 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>E-Series ExaScale</td>
<td>255</td>
<td>64</td>
</tr>
<tr>
<td>E-Series TeraScale</td>
<td>255</td>
<td>16</td>
</tr>
<tr>
<td>E-Series EtherScale</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td>C-Series</td>
<td>128</td>
<td>8</td>
</tr>
<tr>
<td>S-Series</td>
<td>128</td>
<td>8</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 S-Series, 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
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 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port 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

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>Version 8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration. Only the `shutdown`, `description`, `mtu`, and `ip mtu` commands can be configured on an interface if it is to be added to a Port Channel. The `mtu` and `ip mtu` commands are only available when the chassis is in Jumbo mode.

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.

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.

On the E-Series TeraScale, you can add up to 16 interfaces to a Port Channel; E-Series ExaScale can have up to 64. You can have eight interfaces per Port Channel on the C-Series and S-Series. The interfaces can be located on different line cards but must be the same physical type and speed (for example, all 1-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.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
</tr>
<tr>
<td>interface port-channel</td>
</tr>
<tr>
<td>shutdown</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.

<table>
<thead>
<tr>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group_number</code></td>
</tr>
<tr>
<td><code>port-channel number</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>No default values or behavior</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT-CHANNEL FAILOVER-GROUP (conf-po-failover-grp)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
</tr>
</tbody>
</table>
interface port-channel

Create a Port Channel interface, which is a link aggregation group containing up to 16 physical interfaces on E-Series, eight physical interfaces on C-Series and S-Series.

Syntax

```
interface port-channel channel-number
```

To delete a Port Channel, use the no interface port-channel channel-number command.

Parameters

```
channel-number
```

For a Port Channel interface, enter the keyword `port-channel` followed by a number:

- **C-Series** and **S-Series**: Range 1-128
- **E-Series**: Range 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.

Defaults

Not configured.

Command Modes

Configuration

Command History

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **pre-Version 6.2.1.0** Introduced for E-Series

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 using the `switchport` command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

The `shutdown`, `description`, and `name` commands are the only commands that you can configure on an interface while it is a member of a Port Channel. To add a physical interface to a Port Channel, the interface can only have the `shutdown`, `description`, and `name` commands configured. The Port Channel’s configuration is applied to the interfaces within the Port Channel.

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 line card 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.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>channel-member</code>  Add a physical interface to the LAG.</td>
</tr>
<tr>
<td><code>interface</code>       Configure a physical interface.</td>
</tr>
<tr>
<td><code>interface loopback</code>  Configure a Loopback interface.</td>
</tr>
<tr>
<td><code>interface null</code>   Configure a null interface.</td>
</tr>
<tr>
<td><code>interface vlan</code>   Configure a VLAN.</td>
</tr>
<tr>
<td><code>shutdown</code>        Disable/Enable the port channel.</td>
</tr>
</tbody>
</table>

### minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in “oper up” status for the LAG to be also in “oper up” status.

**Syntax**

```
minimum-links number
```

**Parameters**

- `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 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.0 Introduced for E-Series

**Usage Information**

If you use this command to configure the minimum number of links in a LAG that must be in “oper up” status, then 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 will be considered down.

### port-channel failover-group

Access the PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

**Syntax**

```
port-channel failover-group
```

**Parameters**

- `no port-channel failover-group` To remove all LAG failover groups, use the no port-channel failover-group command.
This feature groups two LAGs to work in tandem as a supergroup, so that, for example, 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, see the Port Channel chapter in the Dell Networking OS Configuration Guide.

### show config

Display the current configuration of the selected LAG.

**Syntax**

```
show config
```

**Command Modes**

INTERFACE PORTCHANNEL

**Example**

```
FTOS(conf-if-po-1)#show config
!
interface Port-channel 1
  no ip address
  shutdown

FTOS(conf-if-po-1)#
```

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced for C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

### show interfaces port-channel

Display information on configured Port Channel groups.

**Syntax**

```
show interfaces port-channel [channel-number] [brief]
```

**Command Modes**

INTERFACE

**Example**

```
FTOS(conf-if-po-1)#show config
!
interface Port-channel 1
  no ip address
  shutdown

FTOS(conf-if-po-1)#
```

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
show interfaces port-channel

**Brief**

(Optional) Enter the keyword `brief` to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

**Example**

```plaintext
FTOS#show interfaces port-channel 20
Port-channel 20 is up, line protocol is up (Failover-group 1 is down)
Hardware address is 00:01:e8:01:46:fa
Port-channel is part of failover-group 1
Internet address is 1.1.120.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2000 Mbit
Members in this channel: Gi 0/5 Gi 0/18
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of “show interfaces” counters 00:00:00
Queueing strategy: fifo
44507301 packets input, 3563070343 bytes
Input 44506754 IP Packets, 0 Vlans 0 MPLS
41 64-byte pkts, 44502871 over 64-byte pkts, 249 over 127-byte pkts
407 over 255-byte pkts, 3127 over 511-byte pkts, 606 over 1023-byte pkts
Received 0 input symbol errors, 0 runts, 0 giants, 0 throttles
0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
1218120 packets output, 100745130 bytes, 0 underruns
Output 5428 Multicasts, 4 Broadcasts, 1212688 Unicasts
1216142 IP Packets, 0 Vlans, 0 MPLS
0 throttles, 0 discarded
Rate info (interval 299 sec):
Input 01.50Mbits/sec, 2433 packets/sec
Output 00.02Mbits/sec, 4 packets/sec
Time since last interface status change: 00:22:34
FTOS#
```

**Table 23-12. 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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>address.</td>
</tr>
<tr>
<td>Port-channel is part...</td>
<td>Indicates whether the LAG is part of a LAG fate-sharing group</td>
</tr>
<tr>
<td></td>
<td>(“Failover-group”).</td>
</tr>
<tr>
<td>Internet address...</td>
<td>States whether an IP address is assigned to the interface. If one is, that</td>
</tr>
<tr>
<td></td>
<td>address is displayed.</td>
</tr>
</tbody>
</table>
Table 23-12. show interfaces port-channel Command Example Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>MPLS headers. The number of packets may not add correctly because a VLAN</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This information is displayed over three lines.</td>
</tr>
<tr>
<td>Output 0...</td>
<td>Displays the type and number of packets sent out the interface. This</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
</tbody>
</table>

Figure 23-46. show interfaces port-channel brief Command Example

    FTOS#sh int por 1 br

<table>
<thead>
<tr>
<th>LAG Mode</th>
<th>Status</th>
<th>Uptime</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>L2</td>
<td>00:00:08</td>
<td>G1 3/0 (Up)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>G1 3/1 (Down)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>G1 3/2 (Up)</td>
</tr>
</tbody>
</table>

FTOS#

Table 23-13. 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>
</tbody>
</table>
show port-channel-flow

Display an egress port in a given port-channel flow.

Syntax

```
show port-channel-flow outgoing-port-channel number incoming-interface interface
{source-ip address destination-ip address} | {protocol number | icmp | tcp | udp} |
{source-port number destination-port number} | {source-mac address destination-mac address}
```

Parameters

- **outgoing-port-channel number**
  - Enter the keyword `outgoing-port-channel` followed by the number of the port channel to display flow information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.

- **incoming-interface interface**
  - Enter the keyword `incoming-interface` followed by the interface type and slot/port or number information:
    - For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a SONET interface, enter the keyword `sonet` followed by the 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.

- **source-ip address**
  - Enter the keyword `source-ip` followed by the IP source address in IP address format.

- **destination-ip address**
  - Enter the keyword `destination-ip` followed by the IP destination address in IP address format.

- **protocol number | icmp | tcp | udp**
  - On the E-Series only, enter the keyword `protocol` followed by one of the protocol type keywords: `tcp`, `udp`, `icmp` or `protocol number`
  - **Note:** The protocol number keyword applies to E-Series only.
**Command Modes**

**EXEC**

**Usage Information**

Since this command calculates based on a Layer 2 hash algorithm, use this command to display flows for switched Layer 2 packets, not for routed packets (use the **show ip flow** command to display routed packets).

The **show port-channel-flow** command returns the egress port identification in a given port-channel, if a valid flow is entered. A mismatched flow error occurs if MAC-based hashing is configured for a Layer 2 interface and the user is trying to display a Layer 3 flow.

The output will display three entries:

- Egress port for unfragmented packets.
- In the event of fragmented packets, egress port of the first fragment.
- In the event of fragmented packets, egress port of the subsequent fragments.

### Example

**show port-channel-flow outgoing-port-channel number incoming-interface interface source-mac address destination-mac address**

- Load-balance is configured for MAC
- Load balance is configured for IP 4-tuple/2-tuple for the C-Series and S-Series
- A non-IP payload is going out of Layer 2 LAG interface that is a member of VLAN with an IP address.

**Figure 23-47. show port-channel-flow Command for MAC Addresses**

FTOS#show port-channel-flow outgoing-port-channel 1 incoming-interface gi 3/0 source-mac 00:00:50:00:00:00 destination-mac 00:00:a0:00:00:00

Egress Port for port-channel 1, for the given flow, is Te 13/01

### Example

On the E-Series only:

show port-channel-flow outgoing-port-channel number incoming-interface interface source-ip address destination-ip address [protocol number [icmp|tcp|udp]]

- Load balance is configured for IP 5-tuple/3-tuple.
An IP payload is going out of a Layer 2 LAG interface that is a member of a VLAN with an IP address.

```
FTOS#show port-channel-flow outgoing-port-channel 2 incoming-interface gi 3/0 source-ip 2.2.2.0 destination-ip 3.2.3.1 protocol tcp source-port 5 destination-port 6
```

Egress Port for port-channel 2, for the given flow:
Unfragmented packet: Gi 1/6
Fragmented packets (first fragment): Gi 1/12
Fragmented packets (remaining fragments): Gi 1/12

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>load-balance (E-Series)</code></td>
<td>Balance traffic over E-Series port channel members.</td>
</tr>
</tbody>
</table>

### Time Domain Reflectometer (TDR)

TDR is supported on E-Series ExaScale with Dell Networking OS 8.2.1.0 and later.

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.
- Since 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Enter the keyword <code>GigabitEthernet</code> followed by the slot/port information for the 100/1000 Ethernet interface.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or setting

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td></td>
</tr>
</tbody>
</table>
The interface must be enabled to run the test or an error message is generated:

```
FTOS#tdr-cable-test gigabitethernet 5/2
%Error: Interface is disabled GI 5/2
```

The C-Series and S-Series do not generate log messages is generated when the link flaps down/up during TDR tests. The E-series, does produce these log messages.

### Related Commands

- **show tdr**
  
  Display the results of the TDR test.

  **Syntax**

  `show tdr interface`

  **Parameters**

  `interface` Enter the keyword **GigabitEthernet** followed by the slot/port information for the 100/1000 Ethernet interface.

  **Defaults**

  No default behavior or settings

  **Command Modes**

  EXEC

  **Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

```
Figure 23-48.  show tdr gigabitethernet Command Example

FTOS#show tdr gigabitethernet 10/47
Time since last test: 00:00:02
  Pair A, Length: 99 (+/- 1) meters, 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 23-14. TDR Test Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK Status: Terminated</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 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 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 message is generated:

%Error: Please run the TDR test first

Related Commands
- tdr-cable-test Run 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

- This feature is available only on the E-Series platform, as noted by this symbol under each command heading: 

- This feature applies only to E-Series Layer 3 physical or VLAN interfaces.
- 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, then the command ip directed-broadcast 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**

```
display ip udp-helper
```

To disable debug information, use the **no debug ip udp-helper** command.

**Defaults**

Debug disabled

**Command Modes**

EXEC

EXEC Privilege

**Example**

```
FTOS#debug ip udp-helper
UDP helper debugging is on

01:20:22: Pkt rcvd on Gi 5/0 with IP DA (0xffffffff) will be sent on Gi 5/1 Gi 5/2 Vlan 3

01:44:54: Pkt rcvd on Gi 7/0 is handed over for DHCP processing.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip udp-broadcast-address</td>
<td>Configure a UDP IP address for broadcast</td>
</tr>
<tr>
<td>ip udp-helper udp-port</td>
<td>Enable the UDP broadcast feature on an interface.</td>
</tr>
<tr>
<td>show ip udp-helper</td>
<td>Display the configured UDP helper(s) on all interfaces.</td>
</tr>
</tbody>
</table>

**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**

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

**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.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip udp-helper</td>
<td>Enable debug and display the debug information on a console.</td>
</tr>
<tr>
<td>show ip udp-helper</td>
<td>Display 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**

No default behavior or values

**Command Modes**

INTERFACE (config-if)

**Usage Information**

If the `ip helper-address` command and `ip udp-helper udp-port` command are configured, the behavior is that the UDP broadcast traffic with port numbers 67/68 will be unicast relayed to the DHCP server per the `ip helper-address` configuration. This will occur regardless if the `ip udp-helper udp-port` command contains port numbers 67/68 or not.

If only the `ip udp-helper udp-port` command is configured, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the `udp-port-list`.

**Related Commands**

- `ip helper-address` Configure the destination broadcast or host address for DHCP server.
- `debug ip udp-helper` Enable debug and display the debug information on a console.
- `show ip udp-helper` Display the configured UDP helper(s) on all interfaces.

---

show ip udp-helper

Display the configured UDP helper(s) on all interfaces.

**Syntax**

```
show ip udp-helper
```

**Defaults**

No default configuration or values

**Command Modes**

EXEC

**Example**

```
Figure 23-50. show ip udp-helper Command Example

FTOS#show ip udp-helper
-----------------------------
Port      UDP port list
-----------------------------
Gi 10/0   656, 658
Gi 10/1   All
```

**Related Commands**

- `debug ip udp-helper` Enable debug and display the debug information on a console.
- `ip udp-broadcast-address` Configure a UDP IP address for broadcast.
- `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.
IPv4 Routing

Overview

The characters that appear below command headings indicate support for the associated Dell Networking platform, as follows:

- C-Series: C
- E-Series: E
- S-Series: S

Commands

IPv4-related commands are described in this chapter. They are:

- arp
- arp learn-enable
- arp retries
- arp timeout
- clear arp-cache
- clear host
- clear ip fib linecard
- 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 fib download-igp-only
- ip helper-address
- ip helper-address hop-count disable
- ip host
- ip max-frag-count
- ip mtu
Use Address Resolution Protocol (ARP) to associate an IP address with a MAC address in the switch.

**Syntax**

```
arp vrf {vrf name} ip-address mac-address interface
```

To remove an ARP address, use the `no arp ip-address` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf name</td>
<td><strong>E-Series Only</strong>: Enter the VRF process identifier to tie the static route to the VRF process.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Enter an IP address in dotted decimal format.</td>
</tr>
</tbody>
</table>
Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
Version 8.4.6.0 Added support for the keyword fortyGigE.
Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
pre-Version 6.2.1.1 Introduced on E-Series

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 Clear dynamic ARP entries from the ARP table.
show arp Display ARP table.

arp learn-enable
Enable ARP learning via Gratuitous ARP.

Syntax
arp learn-enable

Default
Disabled

Command Modes
CONFIGURATION

Command History
Version 8.3.1.0 Introduced

Usage Information
In Dell Networking OS versions prior to 8.3.1.0, if a gratuitous ARP is received some time after an ARP request is sent, only RP2 installs the ARP information. For example:
At time t=0 Dell Networking OS sends an ARP request for IP A.B.C.D
At time t=1 Dell Networking OS receives an ARP request for IP A.B.C.D
At time t=2 Dell Networking OS installs an ARP entry for A.B.C.D only on RP2.

Beginning with version 8.3.1.0, when a Gratuitous ARP is received, Dell Networking OS installs an ARP entry on all 3 CPUs.

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the number of retries. Range: 5 to 20. Default: 5</td>
</tr>
</tbody>
</table>

**Defaults**

5

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.3.1.0 Introduced

**Usage Information**

Retries are 20 seconds apart.

**Related Commands**

- `show arp retries` - Display 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
```

To return to the default value, enter `no arp timeout`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Enter the number of minutes. Range: 0 to 35790. Default: 240 minutes</td>
</tr>
</tbody>
</table>

**Defaults**

240 minutes (4 hours)

**Command Modes**

INTERFACE

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
**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 [vrf name | interface | ip ip-address] [no-refresh]
```

**Parameters**
- **vrf name** (E-Series Only): Clear only the ARP cache entries tied to the VRF process.
- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port 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:
    - **C-Series and S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
- **ip ip-address** (OPTIONAL) Enter the keyword `ip` followed by the IP address of the ARP entry you wish to clear.
- **no-refresh** (OPTIONAL) Enter the keyword `no-refresh` to delete the ARP entry from CAM. Or use this option with `interface` or `ip ip-address` to specify which dynamic ARP entries you want to delete.

**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**
<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support 4094 VLANs on E-Series ExaScale (prior limit was 2094)</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

**Related Commands**
- `show interfaces` - Displays the ARP timeout value for all available interfaces.
### clear host

Remove one or all dynamically learnt host table entries.

**Syntax**

```plaintext
clear host [vrf vrf-name] name
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.</td>
</tr>
<tr>
<td>name</td>
<td>Enter the name of the host to delete. Enter * to delete all host table entries.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

### clear ip fib linecard

Clear all Forwarding Information Base (fib) entries in the specified line card (use this command with caution, see Usage Information below)

**Syntax**

```plaintext
clear ip fib linecard slot-number | vrf vrf instance
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot-number</td>
<td>Enter the number of the line card slot.</td>
</tr>
<tr>
<td>vrf instance</td>
<td>(Optional) E-Series Only: Clear only the FIB entries on the specified card associated with the VRF instance.</td>
</tr>
</tbody>
</table>

**Command Mode**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.2</td>
<td>Introduced support on E-Series ExaScale E600i</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
Use this command to clear Layer 3 CAM inconsistencies.

**Caution:** Executing this command will cause traffic disruption.

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

**Syntax**
```
clear ip route {* | ip-address mask | vrf vrf instance}
```

**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.
- `vrf vrf instance` (Optional) **E-Series Only:** Clear only the routes tied to the VRF instance.

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.9.1.0 Introduced VRF
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

### clear tcp statistics
Clear TCP counters.

**Syntax**
```
clear tcp statistics [all | cp | rp1 | rp2]
```

**Note:** These options are supported only on the E-Series.

**Parameters**
- `all` Enter the keyword `all` to clear all TCP statistics maintained on all switch processors.
- `cp` (OPTIONAL) Enter the `cp` to clear only statistics from the Control Processor.
- `rp1` (OPTIONAL) Enter the keyword `rp1` to clear only the statistics from Route Processor 1.
- `rp2` (OPTIONAL) Enter the keyword `rp2` to clear only the statistics from Route Processor 2.

**Command Modes**
EXEC Privilege
**debug arp**

View information on ARP transactions.

**Syntax**

```
debug arp [interface] [count value]
```

To stop debugging ARP transactions, enter `no debug arp`.

**Parameters**

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` followed by the slot/port 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:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
  - 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

**Command Modes**

EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`
- **Version 8.2.1.0** Support 4094 VLANs on E-Series ExaScale (prior limit was 2094)
- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **Version 6.3.1.0** Added the count option

**Defaults**

No default behavior or values

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.4.10</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

Figure 24-1. 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 = 0xb05140f, 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 = 0xb05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
```

**Related Commands**

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

**Example**

```
Figure 24-1. debug ip icmp Command Example

FTOSdebug ip icmp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xb05140f, 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 = 0xb05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
```

```
FTOS#debug ip icmp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xb05140f, 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 = 0xb05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
```
Parameters

`interface` (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port 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 0-1.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - **C-Series** and **S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword `sonet` followed by the 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.
- 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code></td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support 4094 VLANs on E-Series ExaScale (prior limit was 2094)</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added the count option</td>
</tr>
</tbody>
</table>

Example

**Figure 24-2. debug ip icmp Command Example (Partial)**

```
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
```

Usage Information

Use the `count` option to stop packets from flooding the user terminal when debugging is turned on.
debug ip packet

View a log of IP packets sent and received.

Syntax

```
debug ip packet [access-group name] [count value] [interface]
```

To disable debugging, use the `no debug ip packet [access-group name] [count value] [interface]` command.

Parameters

- **access-group name**: Enter the keyword `access-group` followed by the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.

- **count value**: (OPTIONAL) Enter the keyword `count` followed by the count value.
  - Range: 1 to 65534
  - Default: Infinity

- **interface**: (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `gigabitethernet` followed by the slot/port information.
  - For the management interface on the RPM, 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:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Mode

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support 4094 VLANs on E-Series ExaScale (prior limit was 2094)</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added the access-group option</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added the count option</td>
</tr>
</tbody>
</table>
Example Figure 24-3. 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=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, Id=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, Id=4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Gi 4/11), len 64, sending broad/multicast
   proto=89
   IP: s=40.40.40.40 (local), d=224.0.0.6 (Gi 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
```

Table 24-1. debug ip packet Command Example Fields

<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 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 24-4). 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 24-4).

**Example**

**Figure 24-4. 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
FTOS#00:10:45: %RPM0-P:CP
%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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>Enter an IP address in dotted decimal format.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>Enter the mask of the IP address in slash prefix format (for example, /24).</td>
</tr>
<tr>
<td><strong>secondary</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>secondary</strong> to designate the IP address as the secondary address.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

You must be in the INTERFACE mode before you add an IP address to an interface. Assign an IP address to an interface prior to entering the 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, enter `no ip directed-broadcast`.

**Defaults**

Disabled (that is, the interface does not receive directed broadcast packets)

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Configure the `ip domain-list` command up to 6 times to configure a list of possible domain names.

If both the `ip domain-name` and `ip domain-list` commands are configured, the software will try to resolve the name using the `ip domain-name` command. If the name is not resolved, the software goes through the list of names configured with the `ip domain-list` command to find a match.

Use the following steps to enable dynamic resolution of hosts:

- specify a domain name server with the `ip name-server` command.
- enable DNS with the `ip domain-lookup` command.

To view current bindings, use the `show hosts` command. To view DNS related configuration, use the `show running-config resolve` command.

**Related Commands**

- `ip domain-name` Specify a DNS server.
ip domain-lookup

Enable dynamic host-name to address resolution (that is, DNS).

Syntax

ip domain-lookup

To disable DNS lookup, use the no ip domain-lookup.

Defaults

Disabled.

Command Mode

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

Usage Information

To fully enable DNS, also specify one or more domain name servers with the ip name-server command.

Dell Networking OS 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>Specify a DNS server.</td>
</tr>
<tr>
<td>show hosts</td>
<td>View 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, enter no ip domain-name.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Enter one domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</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 domain-lookup` 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><code>ip domain-list</code></td>
<td>Configure additional names.</td>
</tr>
</tbody>
</table>

### ip fib download-igp-only

**Syntax**

```
ip fib download-igp-only [small-fib]
```

**Parameters**

- `small-fib` (OPTIONAL) Enter the keyword `small-fib` to download a smaller FIB table. This option is useful on line cards with a limited FIB size.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

### ip helper-address

**Syntax**

```
ip helper-address ip-address | default-vrf
```

**Parameters**

- `ip-address` Enter an IP address in dotted decimal format (A.B.C.D).
- `default-vrf` (Optional) **E-Series Only**: Enter default-vrf for the DHCP server VRF is using.

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.9.1.0 Introduced VRF on the E-Series
- Version 7.6.1.0 Added support for S-Series
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.

Dell Networking OS 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 it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and Dell Networking OS forwards to the client with source port=67, destination port=68.

```
ip helper-address hop-count disable
```

Disable the hop-count increment for the DHCP relay agent.

Syntax
```
ip helper-address hop-count disable
```

To reenable the hop-count increment, use the `no ip helper-address hop-count disable` command.

Defaults
Enabled; the hops field in the DHCP message header is incremented by default

Command Modes
CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version 8.1.1.0</th>
<th>Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>Version 6.3.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through Dell Networking OS. 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 will be discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip helper-address</code></td>
<td>Specify the destination broadcast or host address for DHCP server requests.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Display the current configuration and changes from default values.</td>
</tr>
</tbody>
</table>

```
ip host
```

Assign a name and IP address to be used by the host-to-IP address mapping table.

Syntax
```
ip host [vrf vrf-name] name ip-address
```

To remove an IP host, use the `no ip host name [vrf vrf-name] [ip-address]` command.
### 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, enter `no ip max-frag-count`.

**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 8.1.1.0: Introduced on E-Series ExaScale
- Version 7.6.1.0: Added support for S-Series
- Version 7.5.1.0: Added support for C-Series
- pre-Version 6.1.1.0: Introduced for E-Series

**Usage Information**
To avoid Denial of Service (DOS) attacks, keep the number of fragments allowed for re-assembly low.

### ip mtu

Set the IP MTU (frame size) of the packet transmitted by the RPM for the line card interface. If the packet must be fragmented, FTOS sets the size of the fragmented packets to the size specified in this command.

**Syntax**
```
ip mtu value
```
To return to the default IP MTU value, enter `no ip mtu`.
Parameters

value

Enter the maximum MTU size if the IP packet is fragmented.
Default: 1500 bytes
Range: 576 to 9234

Defaults

1500 bytes

Command Modes

INTERFACE (Gigabit Ethernet and 10 Gigabit Ethernet interfaces)

Command History

Table 24-2. Difference between Link MTU and IP MTU

<table>
<thead>
<tr>
<th>Layer 2 Overhead</th>
<th>Difference between Link MTU and IP MTU</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>

Usage Information

When you enter no mtu command, FTOS reduces the ip mtu value to 1536 bytes. To return the IP MTU value to the default, enter no ip mtu.

You must compensate for Layer 2 header when configuring link MTU on an Ethernet interface or FTOS may not fragment packets. 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 for the Layer 2 header.

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.
ip name-server

Enter up to 6 IPv4 addresses of name servers. The order you enter the addresses determines the order of their use.

Syntax

```
ip name-server ipv4-address [ipv4-address2...ipv4-address6]
```

To remove a name server, use the `no ip name-server ip-address` command.

Parameters

- `ipv4-address` Enter the IPv4 address, in dotted decimal format, of the name server to be used.
- `ipv4-address2...ipv4-address6` (OPTIONAL) Enter up to five more IPv4 addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space.

Defaults

No name servers are configured.

Command Modes

- `CONFIGURATION`

Command History

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Added support for S-Series
- **Version 7.5.1.0** Added support for C-Series
- **pre-Version 6.1.1.0** Introduced for E-Series

Usage Information

Dell Networking OS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

You can separately configure both IPv4 and IPv6 domain name servers.

Related Commands

- `ipv6 name-server` to configure an IPv6 name server.

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 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Added support for S-Series
- **Version 7.5.1.0** Added support for C-Series
- **pre-Version 6.1.1.0** Introduced for E-Series
ip redirects

Enable the interface to send ICMP redirect messages.

Syntax

ip redirects

To return to default, enter no ip redirects.

Defaults
Disabled

Command Modes
INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

This command is available for physical interfaces and port-channel interfaces on the E-Series.

Note: This command is not supported on default VLAN (default vlan-id command).

ip route

Assign a static route to the switch.

Syntax

ip route vrf {vrf instance} 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf name</td>
<td>(OPTIONAL) E-Series Only: Enter the keyword vrf followed by the VRF Instances name to tie the static route to the VRF instance.</td>
</tr>
<tr>
<td>destination</td>
<td>Enter the IP address in dotted decimal format of the destination device.</td>
</tr>
<tr>
<td>mask</td>
<td>Enter the mask in slash prefix formation (/x) of the destination device’s IP address.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Enter the IP address in dotted decimal format of the forwarding router.</td>
</tr>
</tbody>
</table>
### interface

Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a loopback interface, enter the keyword `loopback` followed by a number from zero (0) to 16383.
- For the null interface, enter the keyword `null` followed by zero (0).
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - **C-Series** and **S-Series**: Range: 1-128
  - **E-Series**: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword `sonet` followed by the 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.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

### distance

(Optional) Enter a number as the distance metric assigned to the route.

Range: 1 to 255

### permanent

(Optional) Enter the keyword `permanent` to specify the route is not removed, even if the interface assigned to that route goes down. The route must be up initially to install it in the routing table.

If you disable the interface with an IP address associated with the keyword `permanent`, the route disappears from the routing table.

### tag tag-value

(Optional) Enter the keyword `tag` followed by a number to assign to the route.

Range: 1 to 4294967295

---

### Defaults

Not configured.

### Command Modes

**CONFIGURATION**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Support 4094 VLANs on E-Series ExaScale (prior limit was 2094)</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

Using the following example of a static route:

```
ip route 33.33.33.0 /24 gigabitethernet 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 View the switch routing table. |

### ip source-route

Enable FTOS to forward IP packets with source route information in the header.

**Syntax**

```markdown
ip source-route
```

To drop packets with source route information, enter `no ip route-source`.

**Defaults**

Enabled.

**Command Modes**

CONFIGURATION

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0 Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.6.1.0 Added support for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0 Added support for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0 Introduced for E-Series</td>
</tr>
</tbody>
</table>

### ip unreachable

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

**Syntax**

```markdown
ip unreachable
```

To disable the generation of ICMP messages, enter `no ip unreachable`.

**Defaults**

Disabled

**Command Modes**

INTERFACE

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.1.1.0 Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.6.1.0 Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0 Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0 Introduced on E-Series</td>
</tr>
</tbody>
</table>

### ip vlan-flooding

Enable unicast data traffic flooding on VLAN member ports.

**Syntax**

```markdown
ip vlan-flooding
```

To disable, use the `no ip vlan-flooding` command.

**Defaults**

disabled

**Command Modes**

CONFIGURATION
By default this command is disabled. When enabled, all the Layer 3 unicast routed data traffic going through a VLAN member port is flooded across all the member ports of that VLAN. There might be some ARP table entries which are resolved through ARP packets which had Ethernet MAC SA different from MAC information inside the ARP packet. This unicast data traffic flooding occurs only for those packets which use these ARP entries.

**load-balance (C-Series and S-Series)**

By default for C-Series and S-Series, Dell Networking OS uses an IP 4-tuple (IP SA, IP DA, Source Port, and Destination Port) to distribute IP traffic over members of a Port Channel as well as equal-cost paths. To designate another method to balance traffic over Port Channel members, use the load-balance command.

**Syntax**

```
load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-mac | source-dest-mac | source-mac]} | {tcp-udp [enable]}
```

To return to the default setting (IP 4-tuple), use the `no` version of the command.

**Parameters**

- **ip-selection [dest-ip | source-ip]**
  - Enter the keywords to distribute IP traffic based on the following criteria:
    - `dest-ip`—Uses destination IP address and destination port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to.
    - `source-ip`—Uses source IP address and source port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to.

- **mac [dest-mac | source-dest-mac | source-mac]**
  - Enter the keywords to distribute MAC traffic based on the following criteria:
    - `dest-mac`—Uses the destination MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to.
    - `source-dest-mac`—Uses the destination and source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to.
    - `source-mac`—Uses the source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to.

- **tcp-udp enable**
  - Enter the keywords to distribute traffic based on the following:
    - `enable`—Takes the TCP/UDP source and destination ports into consideration when doing hash computations. (By default, this is enabled)

**Defaults**

IP 4-tuple (IP SA, IP DA, Source Port, Destination Port)

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>
Usage Information

By default, FTOS distributes incoming traffic based on a hash algorithm using the following criteria:

- IP source address
- IP destination address
- TCP/UDP source port
- TCP/UDP destination port

Related Commands

hash-algorithm ecmp

load-balance (E-Series)

By default, for E-Series chassis, Dell Networking OS uses an IP 5-tuple to distribute IP traffic over members of a Port Channel as well as equal cost paths. To designate another method to balance traffic over Port Channel members, use the **load-balance** command.

**Syntax**

```
load-balance [ip-selection 3-tuple | ip-selection packet-based] [mac]
```

To return to the default setting (IP 5-tuple), use one of the following commands:

- no load-balance ip-selection 3-tuple
- no load-balance ip-selection packet-based
- no load-balance mac

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip-selection 3-tuple | Enter the keywords *ip-selection 3-tuple* to distribute IP traffic based on the following criteria:  
- IP source address  
- IP destination address  
- IP Protocol type  
  
  **Note:** For IPv6, only the first 32 bits (LSB) of IP SA and IP DA are used for hash generation. |
| ip-selection packet-based | Enter the keywords *ip-selection packet-based* to distribute IPv4 traffic based on the IP Identification field in the IPv4 header.  
  
  This option does *not* affect IPv6 traffic; that is, IPv6 traffic is not distributed when this command is executed.  
  
  **Note:** Hash-based load-balancing on MPLS does not work when packet-based hashing (**load-balance ip-selection packet-based**) is enabled. |
| mac | Enter the keyword *mac* to distribute traffic based on the following:  
- MAC source address, and  
- MAC destination address |

**Defaults**

IP 5-tuple (IP SA, IP DA, IP Protocol Type, Source Port and Destination Port)

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

By default, FTOS distributes incoming traffic based on a hash algorithm using the following criteria:
• IP source address
• IP destination address
• IP Protocol type
• TCP/UDP source port
• TCP/UDP destination port

Note: For IPV6, only the first 32 bits (LSB) of IP Source Address and IP Destination Address are used for hash generation.

The table below lists the load balance command options and how the command combinations effect the distribution of traffic.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Switched IP Traffic</th>
<th>Routed IP Traffic (IPV4 Only)</th>
<th>Switched Non-IP Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default (IP 5-tuple)</td>
<td>IP 5-tuple</td>
<td>IP 5-tuple</td>
<td>MAC based</td>
</tr>
<tr>
<td>ip-selection 3-tuple</td>
<td>IP 3-tuple</td>
<td>IP 3-tuple</td>
<td>MAC based</td>
</tr>
<tr>
<td>mac</td>
<td>MAC based</td>
<td>IP 5-tuple</td>
<td>MAC based</td>
</tr>
<tr>
<td>ip-selection 3-tuple and mac</td>
<td>MAC based</td>
<td>IP 3-tuple</td>
<td>MAC based</td>
</tr>
<tr>
<td>ip-selection packet-based and mac</td>
<td>MAC based</td>
<td>Packet based: IPV4</td>
<td>MAC based</td>
</tr>
</tbody>
</table>

Related Commands

management route
Configure a static route that points to the Management interface or a forwarding router.

Syntax

```
management route {ipv4-address | ipv6-address}/mask {forwarding-router-address | managementethernet}
```

Parameters

- `ipv4-address | ipv6-address` Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X), followed by the prefix-length for the IP address of the management interface.
- `forwarding-router-address` Enter an IPv4 or IPv6 address of a forwarding router.
- `managementethernet` Enter the keyword `managementethernet` for the Management interface on the Primary RPM.

Defaults
Not configured.

Command Modes

- CONFIGURATION

Command History

- Version 8.4.1.0 Added support for IPv6 management routes.
- Version 8.1.1.0 Introduced on E-Series ExaScale
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 and IPv6 management routes. This command manages both tables.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp</td>
<td>Display the ARP table.</td>
</tr>
</tbody>
</table>

**Syntax**

```
show [vrf vrf-name] [interface interface | ip ip-address [mask] | macaddress mac-address [mac-address mask]] [cpu {cp | rp1 | rp2}] [static | dynamic] [summary]
```

**Parameters**

- **vrf name**
  - E-Series Only: Show only the ARP cache entries tied to the VRF process.
- **cpu**
  - (OPTIONAL) Enter the keyword `cpu` with one of the following keywords to view ARP entries on that CPU:
    - `cp` - view ARP entries on the control processor.
    - `rp1` - view ARP entries on Routing Processor 1.
    - `rp2` - view ARP entries on Routing Processor 2.
- **interface interface**
  - (OPTIONAL) Enter the following keywords and slot/port or number information:
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port 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:
      - C-Series and S-Series Range: 1-128
      - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword `sonet` followed by the 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.
    - 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**
The following figure shows two VLANs that are associated with a private VLAN (PVLAN) (see Chapter 45, Private VLAN (PVLAN)), a feature added for C-Series and S-Series in Dell Networking OS 7.8.1.0.

**Figure 24-5. show arp Command Example (Partial)**

```
FTOS>show arp

Protocol   Address         Age(min)  Hardware Address    Interface  VLAN  CPU
--------------------------------------------------------------------------------
Internet    192.2.1.254           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.253           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.252           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.251           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.250           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.249           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.248           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.247           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.246           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.245           1   00:00:c0:02:01:02   Gi 9/13     -      CP
```

**Figure 24-6. show arp Command Example with Private VLAN data**

```
FTOS#show arp

Protocol   Address         Age(min)  Hardware Address    Interface  VLAN  CPU
--------------------------------------------------------------------------------
Internet    5.5.5.1               -   00:01:e8:43:96:5e      -       Vl 10 pv 200   CP
Internet    5.5.5.10              -   00:01:e8:44:99:55      -       Vl 10      -      CP
Internet    10.1.2.4              1   00:01:e8:d5:9e:e2   Ma 0/0      -             CP
Internet    10.10.10.4            1   00:01:e8:d5:9e:e2   Ma 0/0      -             CP
Internet    10.16.127.53          1   00:01:e8:d5:9e:e2   Ma 0/0      -             CP
Internet    10.16.134.254         20   00:01:e8:d5:9e:e2   Ma 0/0      -             CP
Internet    133.33.33.4           1   00:01:e8:d5:9e:e2   Ma 0/0      -             CP
```

Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN.
Line 2 shows primary VLAN 10.
Figure 24-7. show arp cpu cp Command Example

FTOS# show arp cpu cp

<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>10.1.2.206</td>
<td>0</td>
<td>00:a0:80:00:15:b8</td>
<td>Ma 0/0</td>
<td>-</td>
<td>CP</td>
</tr>
<tr>
<td>Internet</td>
<td>182.16.1.20</td>
<td>0</td>
<td>00:30:19:24:2d:70</td>
<td>Gi 8/0</td>
<td>-</td>
<td>CP</td>
</tr>
<tr>
<td>Internet</td>
<td>100.10.10.10</td>
<td>0</td>
<td>00:30:19:4f:d3:80</td>
<td>Gi 8/12</td>
<td>-</td>
<td>CP</td>
</tr>
<tr>
<td>Internet</td>
<td>10.1.2.209</td>
<td>12</td>
<td>00:a0:80:00:12:6c</td>
<td>Ma 0/0</td>
<td>-</td>
<td>CP</td>
</tr>
</tbody>
</table>

FTOS#

Table 24-4. 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 24-8. 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>83</td>
<td>0</td>
<td>83</td>
<td>CP</td>
</tr>
</tbody>
</table>

FTOS#

Table 24-5. 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: Enable/disable Layer 3 communication in secondary VLANs.
- switchport mode private-vlan: Set 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:
- Introduced in version 8.3.1.0

Related Commands:
- `arp retries`: Set 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:
- Introduced on E-Series ExaScale
- Introduced on S-Series
- Introduced on C-Series
- Introduced for E-Series

Example:

```
FTOS#show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set
Host Flags TTL Type Address
----- ----- ---- ---- -------
ks (perm, OK) - IP 2.2.2.2
4200-1 (perm, OK) - IP 192.68.69.2
1230-3 (perm, OK) - IP 192.68.99.2
Zzr (perm, OK) - IP 192.71.18.2
Z10-3 (perm, OK) - IP 192.71.23.1
FTOS#
```

Table 24-6. 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>
</tbody>
</table>
| Name/address lookup... | States if DNS is enabled on the system.  
|                      | If DNS is enabled, the Name/Address lookup is domain service.              |
|                      | If DNS is not enabled, the Name/Address lookup is static mapping.           |
| Name servers are...  | Lists the name servers, if configured.                                     |
| Host                 | Displays the host name assigned to the IP address.                         |
**show ip cam linecard**

View CAM entries for a port pipe on a line card.

**Syntax**

```
show ip cam linecard number port-set pipe-number [ip-address mask [longer-prefixes] | index index-number | summary | vrf vrf instance]
```

**Parameters**

- **number**: Enter the number of the line card.
  Range: 0 to 13 on an E1200/1200i, 0 to 6 on a E600i, and 0 to 5 on an E300.
- **pipe-number**: Enter the number of the line card’s port-pipe.
  Range: 0 to 1
- **ip-address mask [longer-prefix]**: (OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only.
  Enter the keyword **longer-prefixes** to view routes with a common prefix.
- **index index-number**: (OPTIONAL) Enter the keyword **index** followed by the CAM index number.
  Range: depends on CAM size
- **summary**: (OPTIONAL) Enter the keyword **summary** to view a table listing route prefixes and the total number of routes that can be entered into the CAM.
- **vrf vrf instance**: (OPTIONAL) **E-Series Only**: Enter the keyword **vrf** following by the VRF Instance name to show CAM information as it applies to that VRF instance.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.1.1.2  E-Series ExaScale E600i supported
Version 8.1.1.0  Introduced on E-Series ExaScale
Version 7.9.1.0  Introduced VRF on the E-Series

---

**Table 24-6. show hosts Command Example Fields** (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Classifies the entry as one of the following:</td>
</tr>
<tr>
<td></td>
<td>• perm - the entry was manually configured and will not time out</td>
</tr>
<tr>
<td></td>
<td>• temp - the entry was learned and will time out after 72 hours of inactivity.</td>
</tr>
<tr>
<td></td>
<td>Also included in the flag is an indication of the validity of the route:</td>
</tr>
<tr>
<td></td>
<td>• ok - the entry is valid.</td>
</tr>
<tr>
<td></td>
<td>• ex - the entry expired.</td>
</tr>
<tr>
<td></td>
<td>• ?? - the entry is suspect.</td>
</tr>
<tr>
<td>TTL</td>
<td>Displays the amount of time until the entry ages out of the cache. For dynamically learnt entries only.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays IP as the type of entry.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the IP address(es) assigned to the host.</td>
</tr>
</tbody>
</table>

**Related Commands**

- traceroute View DNS resolution
- ip host Configure a host.
Example

Figure 24-10. show ip cam Command Example on E-Series

```
FTOS#show ip cam linecard 13 port-set 0

<table>
<thead>
<tr>
<th>Index</th>
<th>Destination</th>
<th>EC</th>
<th>CG</th>
<th>V</th>
<th>C</th>
<th>Next-Hop</th>
<th>VId</th>
<th>Mac-Addr</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>3276</td>
<td>6.6.6.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:17c1 CP</td>
<td></td>
</tr>
<tr>
<td>3277</td>
<td>5.5.5.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c1 CP</td>
<td></td>
</tr>
<tr>
<td>3278</td>
<td>4.4.4.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c1 CP</td>
<td></td>
</tr>
<tr>
<td>3279</td>
<td>3.3.3.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c1 CP</td>
<td></td>
</tr>
<tr>
<td>3280</td>
<td>2.2.2.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c1 CP</td>
<td></td>
</tr>
<tr>
<td>11144</td>
<td>6.6.6.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c5 RP2</td>
<td></td>
</tr>
<tr>
<td>11145</td>
<td>5.5.5.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c5 RP2</td>
<td></td>
</tr>
<tr>
<td>11146</td>
<td>4.4.4.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c5 RP2</td>
<td></td>
</tr>
<tr>
<td>11147</td>
<td>3.3.3.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c5 RP2</td>
<td></td>
</tr>
<tr>
<td>11148</td>
<td>2.2.2.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c5 RP2</td>
<td></td>
</tr>
<tr>
<td>65535</td>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td>0</td>
<td>00:00:00:00:00:00:00:00:00:00:00:00:00:00:17c5 RP2</td>
<td></td>
</tr>
</tbody>
</table>
```

FTOS#

Table 24-7. show ip cam Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Displays the CAM index number of the entry.</td>
</tr>
<tr>
<td>Destination</td>
<td>Displays the destination route of the index.</td>
</tr>
<tr>
<td>EC</td>
<td>Displays the number of equal cost multipaths (ECMP) available for the default route for non-Jumbo line cards. Displays 0,1 when ECMP is more than 8, for Jumbo line cards.</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 if the entry is for a line card with Catalog number beginning with LC-EF.</td>
</tr>
<tr>
<td>C</td>
<td>Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP or RP2, depending on Egress port.</td>
</tr>
<tr>
<td>Next-Hop</td>
<td>Displays the next hop IP address of the entry.</td>
</tr>
<tr>
<td>VId</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 17c1 CP, the CP is the pertinent portion. CP = control processor RP2 = route processor 2 Gi = Gigabit Ethernet interface So = SONET interface Te = 10 Gigabit Ethernet interface</td>
</tr>
</tbody>
</table>
Example  Figure 24-11.  show ip cam summary Command Example

FTOS#show ip cam linecard 4 port-set 0 summary
Total Number of Routes in the CAM is 13
Total Number of Routes which can be entered in CAM is 131072

<table>
<thead>
<tr>
<th>Prefix Len</th>
<th>Current Use</th>
<th>Initial Sz</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>7</td>
<td>37994</td>
</tr>
<tr>
<td>31</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>30</td>
<td>0</td>
<td>3932</td>
</tr>
<tr>
<td>29</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>28</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>27</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>26</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>25</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>24</td>
<td>6</td>
<td>40610</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
<td>3932</td>
</tr>
<tr>
<td>22</td>
<td>0</td>
<td>2622</td>
</tr>
<tr>
<td>21</td>
<td>0</td>
<td>2622</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>2622</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>2622</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>3932</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1312</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>8</td>
</tr>
</tbody>
</table>

FTOS#

Table 24-8.  show ip cam summary Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix Length</td>
<td>Displays the prefix-length or mask for the IP address configured on the linecard 0 port pipe 0.</td>
</tr>
<tr>
<td>Current Use</td>
<td>Displays the number of routes currently configured for the corresponding prefix or mask on the linecard 0 port pipe 0.</td>
</tr>
<tr>
<td>Initial Size</td>
<td>Displays the CAM size allocated by Dell Networking OS for the corresponding mask. The CAM size is adjusted by Dell Networking OS if the number of routes for the mask exceeds the initial allocation.</td>
</tr>
</tbody>
</table>

show ip cam stack-unit

Display content-addressable memory (CAM) entries for an S-Series switch.

Syntax

show ip cam stack-unit 0-7 port-set pipe-number [ip-address mask [longer-prefixes] | summary]

Parameters

<table>
<thead>
<tr>
<th>0-7</th>
<th>Enter the stack-unit ID, from 0 to 7.</th>
</tr>
</thead>
<tbody>
<tr>
<td>pipe-number</td>
<td>Enter the number of the Port-Pipe number.</td>
</tr>
<tr>
<td></td>
<td>S50n, S50V range: 0 to 1; S25N, S25P, S25V range: 0 to 0</td>
</tr>
</tbody>
</table>
**Command Modes**

- **EXEC**
- **EXEC Privilege**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Modified: Added support for up to seven stack members.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 24-12. show ip cam stack-unit Command Example**

FTOS#show ip cam stack-unit 0 port-set 0 10.10.10.10/32 longer-prefixes

<table>
<thead>
<tr>
<th>Destination</th>
<th>EC</th>
<th>CG</th>
<th>V</th>
<th>C</th>
<th>VId</th>
<th>Mac-Addr</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.10</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>00:00:00:00:00:00</td>
<td>3f01 CP</td>
</tr>
</tbody>
</table>

FTOS#

**Table 24-9. 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>EC</td>
<td>Displays the number of equal cost multipaths (ECMP) available for the default route for non-Jumbo line cards. Displays 0,1 when ECMP is more than 8, for Jumbo line cards.</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 Gi = Gigabit Ethernet interface Te = 10 Gigabit Ethernet interface</td>
</tr>
</tbody>
</table>

**show ip fib linecard**

View all Forwarding Information Base (FIB) entries.

**Syntax**

`show ip fib linecard slot-number [vrf vrf instance | ip-address/prefix-list | summary]`
IPv4 Routing

Parameters

vrf instance  (OPTIONAL) E-Series Only: Enter the keyword vrf followed by the VRF Instance name to show the FIB cache entries tied to that VRF instance.

slot-number  Enter the number of the line card slot.
C-Series Range: 0-7
E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, 0 to 5 on a E300

ip-address mask  (OPTIONAL) Enter the IP address of the network destination to view only information on that destination.
You must enter the IP address is dotted decimal format (A.B.C.D). You must enter the mask in slash prefix format (/X).

longer-prefixes  (OPTIONAL) Enter the keyword longer-prefixes to view all routes with a common prefix.

summary  (OPTIONAL) Enter the keyword summary to view the total number of prefixes in the FIB.

Command Mode

EXEC
EXEC Privilege

Command History

Version 8.1.1.0  Introduced on E-Series ExaScale
Version 7.9.1.0  Introduced VRF on the E-Series
Version 7.5.1.0  Introduced on C-Series
pre-Version 6.1.1.0  Introduced for E-Series

Example

Figure 24-13.  show ip fib linecard Command Example

```
FTOS>show ip fib linecard 12

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>First-Hop</th>
<th>Mac-Addr</th>
<th>Port</th>
<th>VId</th>
<th>Index</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0.0.0/8</td>
<td>via 100.10.10.10, So 2/8</td>
<td>100.10.10.10</td>
<td>00:01:e8:00:03:ff</td>
<td>So 2/8</td>
<td>0</td>
<td>60260</td>
<td></td>
</tr>
<tr>
<td>3.0.0.8</td>
<td>via 101.10.10.10, So 2/9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.10.0.24</td>
<td>Direct, So 2/8</td>
<td>0.0.0.0</td>
<td>00:01:e8:00:03:ff</td>
<td>So 2/8</td>
<td>0</td>
<td>11144</td>
<td></td>
</tr>
<tr>
<td>100.10.10.1/32</td>
<td>via 127.0.0.1</td>
<td>127.0.0.1</td>
<td>00:00:00:00:00:00 CP</td>
<td>0</td>
<td>3276</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.10.10.1/32</td>
<td>via 101.10.10.10, So 2/8</td>
<td>100.10.10.10</td>
<td>00:01:e8:00:03:ff So 2/8</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>101.10.10.0/24</td>
<td>Direct, So 2/9</td>
<td>0.0.0.0</td>
<td>00:00:00:00:00:00 CP</td>
<td>0</td>
<td>11145</td>
<td></td>
<td></td>
</tr>
<tr>
<td>101.10.10.1/32</td>
<td>via 127.0.0.1</td>
<td>127.0.0.1</td>
<td>00:00:00:00:00:00 CP</td>
<td>0</td>
<td>3277</td>
<td></td>
<td></td>
</tr>
<tr>
<td>101.10.10.10/32</td>
<td>via 101.10.10.10, So 2/9</td>
<td>101.10.10.10</td>
<td>00:01:e8:01:62:32 So 2/9</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Table 24-10.  show ip fib linecard 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>Index</td>
<td>Displays the internal interface number.</td>
</tr>
<tr>
<td>EC</td>
<td>Displays the number of ECMP paths.</td>
</tr>
</tbody>
</table>
show ip fib stack-unit

View all Forwarding Information Base (FIB) entries.

Syntax

```
show ip fib stack-unit 0-7 [ip-address [mask] [longer-prefixes] | summary]
```

Parameters

- **0-7**: Enter the S-Series stack unit ID, from 0 to 7.
- **ip-address mask**: (OPTIONAL) Enter the IP address of the network destination to view only information on that destination. Enter the IP address in dotted decimal format (A.B.C.D). You must enter the mask in slash prefix format (/X).
- **longer-prefixes**: (OPTIONAL) Enter the keyword `longer-prefixes` to view all routes with a common prefix.
- **summary**: (OPTIONAL) Enter the keyword `summary` to view the total number of prefixes in the FIB.

Command Mode

- EXEC
- EXEC Privilege

Command History

- **Version 7.7.1.0** Modified: Added support for up to seven stack members.
- **Version 7.6.1.0** Introduced on S-Series

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 24-11. show ip fib linecard 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 <code>Direct</code> 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>
show ip flow

Show how a Layer 3 packet is forwarded when it arrives at a particular interface.

Syntax

```
show ip flow interface [vrf vrf instance] interface {source-ip address destination-ip address} {protocol number [tcp | udp] | icmp} {src-port number destination-port number}
```

Parameters

- **vrf instance**: E-Series Only: Show only the L3 flow as they apply to that VRF process.
- **interface interface**: Enter the keyword interface followed by of the following interface keywords:
  - For a Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For a SONET interface, enter the keyword sonet followed by the 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.

  (OPTIONAL) Enter an in or out parameter in conjunction with the optional interface:

- **source-ip address**: Enter the keyword source-ip followed by the IP source address in IP address format.
- **destination-ip address**: Enter the keyword destination-ip followed by the IP destination address in IP address format.
- **protocol number [tcp | udp] | icmp**: E-Series only: Enter the keyword protocol followed by one of the protocol type keywords: tcp, udp, icmp or protocol number.
- **src-port number**: Enter the keyword src-port followed by the source port number.
- **destination-port number**: Enter the keyword destination-port followed by the destination port number.

Command Modes

- EXEC

Command History

- Version 8.4.6.0: Added support for the keyword fortyGigE.
- Version 8.1.1.0: Introduced on E-Series ExaScale
- Version 7.9.1.0: Introduced VRF on the E-Series
- Version 7.6.1.0: Introduced on S-Series
- Version 7.6.1.0: Introduced on S-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.0: Introduced for E-Series

Usage Information

This command provides egress port information for a given IP flow. This is useful in identifying which interface the packet will follow in the case of Port-channel and Equal Cost Multi Paths. Use this command for routed packed only. For switched packets use the show port-channel-flow command.
**show ip flow** does not compute the egress port information when **load-balance mac hashing** is also configured due to insufficient information (the egress MAC is not available).

S-Series produces the following error message:

%Error: Unable to read IP route table

C-Series produces the message:

%Error: FIB cannot compute the egress port with the current trunk hash setting.

**Example Figure 24-15. Command Example show ip flow on E-Series**

```
FTOS#show ip flow interface Gi 1/8 189.1.1.1 63.0.0.1 protocol tcp source-port 7898 destination-port 8976
flow: 189.1.1.1 63.0.0.1 protocol 6 7868 8976
Ingress interface: Gi 1/20
Egress interface: Gi 1/14 to 1.7.1.2[CAM hit 103710] unfragmented packet
Gi 1/10 to 1.2.1.2[CAM hit 103710] fragmented packet
```

**show ip interface**

View IP-related information on all interfaces.

**Syntax**

```
show ip interface [interface | brief | linecard slot-number] [configuration]
```

**Parameter**

- **interface**
  - (OPTIONAL) Enter the following keywords and slot/port or number information:
    - For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port 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:
      - **C-Series** and **S-Series** Range: 1-128
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword **sonet** followed by the 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.
    - 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.
**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>8.1.1.2</td>
<td>Supported on E-Series ExaScale E600i</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 24-16. 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 24-12. 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>
<tr>
<td>IP MTU is...</td>
<td>Displays IP MTU value.</td>
</tr>
<tr>
<td>Inbound access...</td>
<td>Displays the name of the any configured incoming access list. If none is configured, the phrase “not set” is displayed.</td>
</tr>
<tr>
<td>Proxy ARP...</td>
<td>States whether proxy ARP is enabled on the interface.</td>
</tr>
<tr>
<td>Split horizon...</td>
<td>States whether split horizon for RIP is enabled on the interface.</td>
</tr>
<tr>
<td>Poison Reverse...</td>
<td>States whether poison for RIP is enabled on the interface</td>
</tr>
<tr>
<td>ICMP redirects...</td>
<td>States if ICMP redirects are sent.</td>
</tr>
<tr>
<td>ICMP unreachables...</td>
<td>States if ICMP unreachable messages are sent.</td>
</tr>
</tbody>
</table>
show ip interface brief

View the IP addresses assigned to the Management interface.

Syntax

show ip interface brief [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.
- **summary** (OPTIONAL) Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
- **static** (OPTIONAL) Enter the keyword `static` to view non-active routes also.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

Table 24-13. show ip interface brief Column Headings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays type of interface and the associated slot and port number.</td>
</tr>
<tr>
<td>IP-Address</td>
<td>Displays the IP address for the interface, if configured.</td>
</tr>
<tr>
<td>Ok?</td>
<td>Indicates if the hardware is functioning properly.</td>
</tr>
<tr>
<td>Method</td>
<td>Displays Manual if the configuration is read from the saved configuration.</td>
</tr>
<tr>
<td>Status</td>
<td>States whether the interface is enabled (up) or disabled (administratively down).</td>
</tr>
<tr>
<td>Protocol</td>
<td>States whether IP is enabled (up) or disabled (down) on the interface.</td>
</tr>
</tbody>
</table>
show ipv6 management-route
Display the IPv6 static routes configured for the management interface.

Syntax
show ipv6 management-route [all | connected | summary | static]

Parameters
- **all**: Enter the keyword `all` to view all IP addresses assigned to all Management interfaces on the switch.
- **connected**: Enter the keyword `connected` to view only routes directly connected to the Management interface.
- **summary**: Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
- **static**: Enter the keyword `static` to view non-active routes also.

Command Modes
- EXEC Privilege

Command History
- Version 8.4.1.0 Introduced
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Regular evaluation optimization enabled/disabled added to display output
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- preVersion 6.1.1.0 Introduced for E-Series

Example
```
FTOS#show ipv6 management-route
IPv6 Destination          Gateway                      State
------------------------------------------------------
2001:34::0/64              ManagementEthernet 0/0    Connected
2001:68::0/64              2001:34::16            Active
FTOS#
```
show ip route

View information, including how they were learned, about the IP routes on the switch.

Syntax

show ip route [vrf [vrf name] hostname | ip-address [mask] [longer-prefixes] | list prefix-list | protocol [process-id | routing-tag] | all | connected | static | summary]

Parameter

- **vrf name**: E-Series Only: Clear only the route entries tied to the VRF process.
- **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.
- **protocol**: (OPTIONAL) Enter the name of a routing protocol (bgp, isis, ospf, rip) or the keywords connected or static.
  - bgp, isis, ospf, rip are E-Series-only options.
  - If you enter bgp, you can include the BGP as-number. (E-Series only)
  - If you enter isis, you can include the ISIS routing-tag. (E-Series only)
  - If you enter ospf, you can include the OSPF process-id.
- **process-id**: (OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
- **routing-tag**: (OPTIONAL) Specify that only ISIS routes with a certain routing tag 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>previous 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 24-20. 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

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0.0.0/8</td>
<td>via 100.10.10.10, So 2/8</td>
<td>120/1</td>
<td>00:07:12</td>
</tr>
<tr>
<td>3.0.0.0/8</td>
<td>via 101.10.10.10, So 2/9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.10.10.0</td>
<td>Direct, So 2/8</td>
<td>0/0</td>
<td>00:08:54</td>
</tr>
<tr>
<td>100.10.10.0</td>
<td>Direct, So 2/8</td>
<td>0/0</td>
<td>00:08:54</td>
</tr>
<tr>
<td>101.10.10.0</td>
<td>Direct, So 2/9</td>
<td>0/0</td>
<td>00:09:15</td>
</tr>
<tr>
<td>101.10.10.0</td>
<td>Direct, So 2/9</td>
<td>120/0</td>
<td>00:09:15</td>
</tr>
</tbody>
</table>

FTOS#show ip route summary

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Active Routes</th>
<th>Non-active Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>static</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Total 3 active route(s) using 612 bytes
```

**Figure 24-21. show ip route summary and show ip route static Command Examples**

```
FTOS#show ip route summary

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Active Routes</th>
<th>Non-active Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>static</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Total 3 active route(s) using 612 bytes
```

```
R1_E600i>show ip route static

```

| *S 0.0.0.0/0 | via 10.10.91.9, Gi 1/2 | 1/0 | 3d2h |
```

**Example**

**Figure 24-21. show ip route summary and show ip route static Command Examples**

```
FTOS#show ip route summary

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Active Routes</th>
<th>Non-active Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>static</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Total 3 active route(s) using 612 bytes
```

```
R1_E600i>show ip route static

```

| *S 0.0.0.0/0 | via 10.10.91.9, Gi 1/2 | 1/0 | 3d2h |
```

FTOS>
show ip route list

**Syntax**

`show ip route list prefix-list`

**Parameters**

- `prefix-list`  
Enter the name of a configured prefix list.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- **Version 8.1.1.0**  
  Introduced on E-Series ExaScale
- **Version 7.6.1.0**  
  Introduced on S-Series
- **Version 7.5.1.0**  
  Introduced on C-Series
- **pre-Version 6.1.1.0**  
  Introduced for E-Series

---

**Table 24-14. show ip route all Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(undefined)</td>
<td>Identifies the type of route:</td>
</tr>
<tr>
<td>C</td>
<td>= connected</td>
</tr>
<tr>
<td>S</td>
<td>= static</td>
</tr>
<tr>
<td>R</td>
<td>= RIP</td>
</tr>
<tr>
<td>B</td>
<td>= BGP</td>
</tr>
<tr>
<td>IN</td>
<td>= internal BGP</td>
</tr>
<tr>
<td>EX</td>
<td>= external BGP</td>
</tr>
<tr>
<td>LO</td>
<td>= Locally Originated</td>
</tr>
<tr>
<td>O</td>
<td>= OSPF</td>
</tr>
<tr>
<td>IA</td>
<td>= OSPF inter area</td>
</tr>
<tr>
<td>N1</td>
<td>= OSPF NSSA external type 1</td>
</tr>
<tr>
<td>N2</td>
<td>= OSPF NSSA external type 2</td>
</tr>
<tr>
<td>E1</td>
<td>= OSPF external type 1</td>
</tr>
<tr>
<td>E2</td>
<td>= OSPF external type 2</td>
</tr>
<tr>
<td>i</td>
<td>= IS-IS</td>
</tr>
<tr>
<td>L1</td>
<td>= IS-IS level-1</td>
</tr>
<tr>
<td>L2</td>
<td>= IS-IS level-2</td>
</tr>
<tr>
<td>IA</td>
<td>= IS-IS inter-area</td>
</tr>
<tr>
<td>*</td>
<td>= candidate default</td>
</tr>
<tr>
<td>&gt;</td>
<td>= non-active route</td>
</tr>
<tr>
<td>+</td>
<td>= summary routes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Identifies the route’s destination IP address.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Identifies whether the route is directly connected and on which interface the route is configured.</td>
</tr>
<tr>
<td>Dist/Metric</td>
<td>Identifies if the route has a specified distance or metric.</td>
</tr>
<tr>
<td>Last Change</td>
<td>Identifies when the route was last changed or configured.</td>
</tr>
</tbody>
</table>

**show ip route list**

Display IP routes in an IP prefix list.

**Syntax**

`show ip route list prefix-list`

**Parameters**

- `prefix-list`  
Enter the name of a configured prefix list.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- **Version 8.1.1.0**  
  Introduced on E-Series ExaScale
- **Version 7.6.1.0**  
  Introduced on S-Series
- **Version 7.5.1.0**  
  Introduced on C-Series
- **pre-Version 6.1.1.0**  
  Introduced for E-Series
**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 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **pre-Version 6.1.1.0** Introduced for E-Series

**Example**

**Figure 24-23. show ip route summary Command Example**

```
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>
```
show ip traffic
View IP, ICMP, UDP, TCP and ARP traffic statistics.

Syntax
```
show ip traffic [all | cp | rp1 | rp2]
```

Parameters
- `all` (OPTIONAL) Enter the keyword `all` to view statistics from all processors.
  If you do not enter a keyword, you also view all statistics from all processors.
- `cp` (OPTIONAL) Enter the `cp` to view only statistics from the Control Processor.
- `rp1` (OPTIONAL) Enter the keyword `rp1` to view only the statistics from Route Processor 1.
- `rp2` (OPTIONAL) Enter the keyword `rp2` to view only the statistics from Route Processor 2.

Command Modes
EXEC Privilege

Command History
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 6.5.1.0 F10 Monitoring MIB available for ip traffic statistics
- pre-Version 6.1.1.0 Introduced for E-Series

### Table 24-15. show ip route summary Column Headings

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Source</td>
<td>Identifies how the route is configured in FTOS.</td>
</tr>
<tr>
<td>Active Routes</td>
<td>Identifies the best route if a route is learned from two protocol sources.</td>
</tr>
<tr>
<td>Non-active Routes</td>
<td>Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route will become the best route.</td>
</tr>
<tr>
<td>ospf 100</td>
<td>If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.</td>
</tr>
<tr>
<td>Total 1388 active...</td>
<td>Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the FTOS, this line does not appear.</td>
</tr>
</tbody>
</table>

**Related Commands**
- `show ip route` Display information about the routes found in switch.
Example

**Figure 24-24. show ip traffic Command Example (partial)**

FTOS#show ip traffic
Control Processor IP Traffic:

**IP statistics:**
- Rcvd: 23857 total, 23829 local destination
- 0 format errors, 0 checksum errors, 0 bad hop count
- 0 unknown protocol, 0 not a gateway
- 0 security failures, 0 bad options
- Frags: 0 reassembled, 0 timeouts, 0 too big
- 0 fragmented, 0 couldn't fragment
- Bcast: 28 received, 0 sent; Mcast: 0 received, 0 sent
- Sent: 16048 generated, 0 forwarded
- 21 encapsulation failed, 0 no route

**ICMP statistics:**
- Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 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: 0 total, 0 checksum errors, 0 no port
- 0 short packets, 0 bad length, 0 no port broadcasts, 0 socket full
- Sent: 0 total, 0 forwarded broadcasts

**TCP statistics:**
- Rcvd: 23829 total, 0 checksum errors, 0 no port
- Sent: 16048 total

**ARP statistics:**
- Rcvd: 156 requests, 11 replies
- Sent: 21 requests, 10 replies (0 proxy)

Routing Processor1 IP Traffic:

Table 24-16. 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 Dell Networking OS.</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. Dell Networking OS sends an arp request prior to forwarding an IP packet. If a reply is not received, Dell Networking OS 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>
</tbody>
</table>
The F10 Monitoring MIB provides access to the statistics described below.

Table 24-16. show ip traffic output definitions

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>...no port</td>
<td>The incoming broadcast/multicast packet did not have any listener.</td>
</tr>
<tr>
<td>broadcasts</td>
<td></td>
</tr>
<tr>
<td>...socket full</td>
<td>The applications buffer was full and the incoming packet had to be dropped.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 24-17. F10 Monitoring MIB

<table>
<thead>
<tr>
<th>Command Display</th>
<th>Object</th>
<th>OIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP statistics:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bcast: 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: 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>ARP statistics:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rcvd: 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: 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 protocol-termination-table

Display the IP Packet Termination Table (IPPTT).

Syntax

show protocol-termination-table linecard number port-set port-pipe-number

Parameters

- **linecard number**: Enter the keyword **linecard** followed by slot number of the line card.
  - **E-Series** Range: 0 to 13 on a E1200/1200i, 0 to 6 on a E600/E600i, and 0 to 5 on a E300

- **port-set port-pipe-number**: Enter the keyword **port-set** followed by the line card’s Port-Pipe number.
  - Range: 0 to 1

Defaults

No default behavior or values

Command Modes

- EXEC
- EXEC Privilege
The IPPTT table is used for looking up forwarding information for IP control traffic destined to the router. For the listed control traffic types, IPPTT contains the information for the following:

- Which CPU to send the traffic (CP, RP1, or RP2)
- What QoS parameters to set

### show protocol-termination-table Command Output

```plaintext
FTOS#show protocol-termination-table linecard 2 port-set 0
Index  Protocol  Src-Port  Dst-Port  Queue  DP  Blk-Hole  VlanCPU  EgPort
-----  --------  --------  --------  -----  --  --------  ----------  -----
 0     ICMP      any      any      Q0      0    No         -            CP
 1     UDP      any      1812     Q7      6    No         -            CP
 2     UDP      any      68       Q7      6    No         -            CP
 3     TCP      any      22       Q7      6    No         -            CP
 4     TCP      22       any      Q7      6    No         -            CP
 5     TCP      any      639      Q7      6    No         -            RP2
 6     TCP      any      646      Q7      6    No         -            RP1
 7     TCP      any      646      Q7      6    No         -            RP1
 8     TCP      any      646      Q7      6    No         -            RP1
 9     TCP      any      646      Q7      6    No         -            RP1
10    UDP      any      646      Q7      6    No         -            RP1
11    UDP      any      646      Q7      6    No         -            RP1
12    TCP      23       any      Q7      6    No         -            CP
13    TCP      any      23       Q7      6    No         -            CP
14    UDP      any      123      Q7      6    No         -            CP
15    TCP      any      21       Q7      6    No         -            CP
16    TCP      any      20       Q7      6    No         -            CP
17    UDP      any      21       Q7      6    No         -            CP
18    UDP      any      20       Q7      6    No         -            CP
19    TCP      21       any      Q7      6    No         -            CP
20    TCP      20       any      Q7      6    No         -            CP
21    UDP      21       any      Q7      6    No         -            CP
22    UDP      20       any      Q7      6    No         -            CP
23    UDP      any      69       Q7      6    No         -            CP
24    UDP      any      69       Q7      6    No         -            CP
25    TCP      any      161      Q7      6    No         -            CP
26    TCP      any      161      Q7      6    No         -            CP
27    TCP      any      162      Q7      6    No         -            CP
28    TCP      any      162      Q7      6    No         -            CP
29    UDP      any      161      Q7      6    No         -            CP
30    UDP      any      161      Q7      6    No         -            CP
31    UDP      any      162      Q7      6    No         -            CP
32    UDP      162      any      Q7      6    No         -            CP
33    PIM-SM    any      any      Q6      0    No         -            RP2
34    ICMP      any      any      Q7      6    No         -            RP2
35    OSPF      any      any      Q7      6    No         -            RP1
```

### show tcp statistics

View information on TCP traffic through the switch.

**Syntax**

```
show tcp statistics {all | cp | rp1 | rp2}
```

**Parameters**

- **all**
  - Enter the keyword `all` to view all TCP information.

- **cp**
  - Enter the keyword `cp` to view only TCP information from the Control Processor.
**Command Modes**

**EXEC Privilege**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>6.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

**Figure 24-26. show tcp statistics cp Command Example**

FTOS#show tcp stat cp

Control Processor TCP:
Rsved: 10585 Total, 0 no port
- 0 checksum error, 0 bad offset, 0 too short
- 329 packets (1263 bytes) in sequence
- 17 dup packets (6 bytes)
- 0 partially dup packets (0 bytes)
- 7 out-of-order packets (0 bytes)
- 0 packets (0 bytes) with data after window
- 0 packets after close
- 0 window probe packets, 41 window update packets
- 41 dup ack packets, 0 ack packets with unsend data
- 10184 ack packets (12439508 bytes)

Sent: 12007 Total, 0 urgent packets
- 25 control packets (including 24 retransmitted)
- 11603 data packets (12439677 bytes)
- 24 data packets (7638 bytes) retransmitted
- 355 ack only packets (41 delayed)
- 0 window probe packets, 0 window update packets
- 7 Connections initiated, 8 connections accepted, 15 connections established
- 14 Connections closed (including 0 dropped, 0 embryonic dropped)
- 20 Total rxmt timeout, 0 connections dropped in rxmt timeout
- 0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive

FTOS#

**Table 24-18. show tcp statistics cp Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rsvd:</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 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 acknowledgement packets with data received.</td>
</tr>
</tbody>
</table>
Table 24-18. show tcp statistics cp Command Example Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 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>
<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 resend 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>
IPv6 Access Control Lists (IPv6 ACLs)

Overview

IPv6 ACLs and IPv6 Route Map commands are supported on platforms:

- IPv6 ACL Commands
- IPv6 Route Map Commands

Note: For IPv4 ACL commands, see Chapter 9, Access Control Lists (ACL).

Important Points to Remember

- E-Series platforms require IPv6-ExtACL CAM profile to support IPv6 ACLs.
- C-Series platforms require manual CAM usage space allotment. Refer to cam-acl later in this document.
- Egress IPv6 ACL and IPv6 ACL on Loopback interface is not supported.
- Reference to an empty ACL will permit any traffic.
- ACLs are not applied to self-originated traffic (e.g. Control Protocol traffic not affected by IPv6 ACL since the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set).
- The same access list name can be used for both IPv4 and IPv6 ACLs.
- Both IPv4 and IPv6 ACLs can be applied on an interface at the same time.
- IPv6 ACLs can be applied on physical interfaces and a logical interfaces (Port-channel/VLAN).
- Non-contiguous masks are not supported in source or destination addresses in IPv6 ACL entries.
- Since prefix mask is specified in /x format in IPv6 ACLs, inverse mask is not supported.
# IPv6 ACL Commands

The following commands configure IPv6 ACLs:

- `cam-acl`
- `clear counters ipv6 access-group`
- `deny`
- `deny icmp`
- `deny tcp`
- `deny udp`
- `ipv6 access-group`
- `ipv6 access-list`
- `permit`
- `permit icmp`
- `permit tcp`
- `permit udp`
- `remark`
- `resequence access-list`
- `resequence prefix-list ipv6`
- `seq`
- `show cam-acl`
- `show config`
- `show ipv6 accounting access-list`
- `show running-config acl`
- `test cam-usage`

## cam-acl

Allocate space for IPv6 ACLs.

### Syntax

cam-acl {default | l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10}

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `default`       | Use the default CAM profile settings, and set the CAM as follows.  
|                 | L3 ACL (ipv4acl): 6  
|                 | L2 ACL(l2acl): 5  
|                 | IPv6 L3 ACL (ipv6acl): 0  
|                 | L3 QoS (ipv4qos): 1  
|                 | L2 QoS (l2qos): 1 |
| `l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10` | Allocate space to support IPv6 ACLs. You must enter all of the profiles and a range.  
|                 | Enter the CAM profile name followed by the amount to be allotted.  
|                 | The total space allocated must equal 13.  
|                 | The `ipv6acl` range must be a factor of 2. |
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 3 blocks and these cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

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 2 (2, 4, 6, 8, 10).

**clear counters ipv6 access-group**

Erase all counters maintained for the IPv6 access lists.

**Syntax**

```
clear counters ipv6 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
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
<tr>
<td></td>
<td>Added <strong>monitor</strong> option</td>
</tr>
</tbody>
</table>
deny

Configure a filter that drops IPv6 packets that match the filter criteria.

Syntax

```
deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp}
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-protocol-number</code></td>
<td>Enter an IPv6 protocol number.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 255</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>Enter the keyword <code>icmp</code> to deny Internet Control Message Protocol version 6.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>Enter the keyword <code>ipv6</code> to deny any Internet Protocol version 6.</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>Enter the keyword <code>tcp</code> to deny the Transmission Control protocol.</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>Enter the keyword <code>udp</code> to deny the User Datagram Protocol.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ACCESS-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced support on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced support on the E-Series TeraScale</td>
</tr>
</tbody>
</table>
deny icmp

Configure a filter to drop all or specific ICMP messages.

**Syntax**

```plaintext
deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [message-type] [count [byte]] [log] [monitor]
```

To remove this filter, you have two choices:
- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>source address</td>
<td>Enter the IPv6 address of the network or host from which the packets were sent in the <code>x:x:x:x::x</code> format followed by the prefix length in the <code>/x</code> format. Range: <code>/0</code> to <code>/128</code>&lt;br&gt;The <code>::</code> notation specifies successive hexadecimal fields of zero.</td>
<td></td>
</tr>
<tr>
<td>mask</td>
<td>Enter a network mask in <code>/prefix format</code> (<code>/x</code>).</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword <code>any</code> to specify that all routes are subject to the filter.</td>
<td></td>
</tr>
<tr>
<td>host ipv6-address</td>
<td>Enter the keyword <code>host</code> followed by the IPv6 address of the host in the <code>x:x:x:x::x</code> format. The <code>::</code> notation specifies successive hexadecimal fields of zero.</td>
<td></td>
</tr>
<tr>
<td>destination address</td>
<td>Enter the IPv6 address of the network or host to which the packets are sent in the <code>x:x:x:x::x</code> format followed by the prefix length in the <code>/x</code> format. Range: <code>/0</code> to <code>/128</code>&lt;br&gt;The <code>::</code> notation specifies successive hexadecimal fields of zero.</td>
<td></td>
</tr>
<tr>
<td>message-type</td>
<td>On the E-Series only, enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. Range: <code>0</code> to <code>255</code> for ICMP type; <code>0</code> to <code>255</code> for ICMP code</td>
<td></td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.</td>
<td></td>
</tr>
<tr>
<td>byte</td>
<td>(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.</td>
<td></td>
</tr>
<tr>
<td>log</td>
<td>(OPTIONAL) Enter the keyword <code>log</code> to have the information kept in an ACL log file.</td>
<td></td>
</tr>
<tr>
<td>monitor</td>
<td>(OPTIONAL) Enter the keyword <code>monitor</code> to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

Not configured

**Command Modes**

ACCESS-LIST

**Command History**

- **Version 8.4.2.1**
  - Introduced on the S-Series
- **Version 8.2.1.0**
  - Introduced support on the E-Series ExaScale
- **Version 7.8.1.0**
  - Introduced support on the C-Series
- **Version 7.4.1.0**
  - Introduced support on the E-Series TeraScale
  - Added `monitor` option
The C-Series cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

The following table lists the keywords displayed in the CLI help and their corresponding ICMP Message Type Name.

### Table 25-1. ICMP Message Type Keywords

<table>
<thead>
<tr>
<th>Keyword</th>
<th>ICMP Message Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>dest-unreachable</td>
<td>Destination unreachable</td>
</tr>
<tr>
<td>echo</td>
<td>Echo request (ping)</td>
</tr>
<tr>
<td>echo-reply</td>
<td>Echo reply</td>
</tr>
<tr>
<td>inverse-nd-na</td>
<td>Inverse neighbor discovery advertisement</td>
</tr>
<tr>
<td>inverse-nd-ns</td>
<td>Inverse neighbor discovery solicitation</td>
</tr>
<tr>
<td>log</td>
<td>Log matches against this entry</td>
</tr>
<tr>
<td>mobile-advertisement</td>
<td>Mobile prefix advertisement</td>
</tr>
<tr>
<td>mobile-solicitation</td>
<td>Mobile prefix solicitation</td>
</tr>
<tr>
<td>mrouter-advertisement</td>
<td>Multicast router advertisement</td>
</tr>
<tr>
<td>mrouter-solicitation</td>
<td>Multicast router solicitation</td>
</tr>
<tr>
<td>mrouter-termination</td>
<td>Multicast router termination</td>
</tr>
<tr>
<td>nd-na</td>
<td>Neighbor advertisement</td>
</tr>
<tr>
<td>nd-ns</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>packet-too-big</td>
<td>Packet is too big</td>
</tr>
<tr>
<td>parameter-problem</td>
<td>Parameter problems</td>
</tr>
<tr>
<td>redirect</td>
<td>Neighbor redirect</td>
</tr>
<tr>
<td>router-advertisement</td>
<td>Neighbor discovery router advertisement</td>
</tr>
<tr>
<td>router-renumbering</td>
<td>All routers renumbering</td>
</tr>
<tr>
<td>router-solicitation</td>
<td>Neighbor discovery router solicitation</td>
</tr>
<tr>
<td>time-exceeded</td>
<td>All time exceeded</td>
</tr>
</tbody>
</table>
**deny tcp**

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

**Syntax**

```
deny tcp {source address mask | any | host ipv6-address} [operator port [port]] {destination address | any | host ipv6-address} {bit} [operator port [port]] [count [byte]] | [log] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no deny tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>source address</strong></td>
<td>Enter the IPv6 address of the network or host from which the packets were sent in the <code>x:x:x::x</code> format followed by the prefix length in the <code>/x</code> format. Range: /0 to /128. The <code>::</code> notation specifies successive hexadecimal fields of zero.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>Enter a network mask in /prefix format (/x).</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Enter the keyword <code>any</code> to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td><strong>host ipv6-address</strong></td>
<td>Enter the keyword <code>host</code> followed by the IPv6 address of the host in the <code>x:x:x::x</code> format. The <code>::</code> notation specifies successive hexadecimal fields of zero.</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 <code>port</code> command parameter.</td>
</tr>
<tr>
<td><strong>port port</strong></td>
<td>Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535.</td>
</tr>
<tr>
<td></td>
<td>The following list includes some common TCP port numbers:</td>
</tr>
<tr>
<td></td>
<td>• 23 = Telnet</td>
</tr>
<tr>
<td></td>
<td>• 20 and 21 = FTP</td>
</tr>
<tr>
<td></td>
<td>• 25 = SMTP</td>
</tr>
<tr>
<td></td>
<td>• 169 = SNMP</td>
</tr>
<tr>
<td><strong>destination address</strong></td>
<td>Enter the IPv6 address of the network or host to which the packets are sent in the <code>x:x:x::x</code> format followed by the prefix length in the <code>/x</code> format. Range: /0 to /128. The <code>::</code> notation specifies successive hexadecimal fields of zero.</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>
</tbody>
</table>
IPv6 Access Control Lists (IPv6 ACLs)

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

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

**log**
(Optional) Enter the keyword `log` to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.

**monitor**
(Optional) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

**Defaults**
Not configured.

**Command Modes**
ACCESS-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
<tr>
<td></td>
<td>Added <code>monitor</code> option</td>
</tr>
</tbody>
</table>

**Usage Information**

The C-Series 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 bitmask 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 8 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 1111111111100000</td>
<td>4000 4031</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0000111111100000 1111111111000000</td>
<td>4032 4095</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000 1111111111000000</td>
<td>4096 6143</td>
<td>2048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000 1111111111000000</td>
<td>6144 7167</td>
<td>1024</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0001111000000000 1111111111100000</td>
<td>7168 7679</td>
<td>512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0001111100000000 1111111111110000</td>
<td>7680 7935</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0001111110000000 1111111111111000</td>
<td>7936 7999</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0001111111000000 1111111111111111</td>
<td>8000 8000</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Ports: 4001

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

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000000000000000 1111111000000000</td>
<td>0 1023</td>
<td>1024</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Ports: 1024

**Related Commands**

- `deny` Assign a filter to deny IP traffic.
- `deny udp` Assign a filter to deny UDP traffic.
deny udp

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

Syntax
deny udp {source address mask | any | host ipv6-address} [operator port [port]] {destination address | any | host ipv6-address} [operator port [port]] [count [byte]] | [log] [monitor]

To remove this filter, you have two choices:
• Use the no seq sequence-number command syntax if you know the filter’s sequence number or
• Use the no deny udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} command.

Parameters

| source address | Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x::x format followed by the prefix length in the /x format. Range: /0 to /128
| mask | Enter a network mask in /prefix format (/x). The :: notation specifies successive hexadecimal fields of zero.
| any | Enter the keyword any to specify that all routes are subject to the filter.
| host ipv6-address | Enter the keyword host followed by the IPv6 address of the host in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
| operator | (OPTIONAL) Enter one of the following logical operand:
| port port | (OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535
| destination address | Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x::x format followed by the prefix length in the /x format. Range: /0 to /128
| count | (OPTIONAL) Enter the keyword count to count packets processed by the filter.
| byte | (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.
| log | (OPTIONAL) Enter the keyword log to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
| monitor | (OPTIONAL) Enter the keyword monitor to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults
Not configured.

Command Modes
ACCESS-LIST
Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
<tr>
<td></td>
<td>Added <code>monitor</code> option</td>
</tr>
</tbody>
</table>

Usage Information

The C-Series 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 bitmask 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 8 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>1111111111110000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111100000</td>
<td>1111111111110000</td>
<td>4032</td>
<td>4095</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000</td>
<td>1111111111111111</td>
<td>4096</td>
<td>6143</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000</td>
<td>1111111111111111</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001111000000000</td>
<td>1111111111111111</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111110000000</td>
<td>1111111111111111</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111111000000</td>
<td>1111111111111111</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111111100000</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>1111111000000000</td>
<td>0</td>
<td>1023</td>
<td>1024</td>
</tr>
</tbody>
</table>

Total Ports: 1024

Related Commands

- `deny` Assign a deny filter for IP traffic.
- `deny tcp` Assign a deny filter for TCP traffic.

**ipv6 access-group**

Assign an IPv6 access-group to an interface.

Syntax

`ipv6 access-group access-list-name {in | out} [implicit-permit] [vlan range]`

To delete an IPv6 access-group configuration, use the `no ipv6 access-group access-list-name {in} [implicit-permit] [vlan range]` command.

Parameters

- `access-list-name`: Enter the name of a configured access list, up to 140 characters.
- `in | out`: Enter either the keyword `in` or `out` to apply the IPv6 ACL to incoming traffic (ingress) or outgoing traffic (egress).
IPv6 Access Control Lists (IPv6 ACLs)

Defaults
Disabled

Command Modes
INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td></td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
</tbody>
</table>

Usage Information
You can assign an IPv6 access group to a physical, LAG, or VLAN interface context.

Example

Figure 25-1. Command Example: ipv6 access-group

```
FTOS(conf-if-gi-9/0)#ipv6 access-group AclList1 in implicit-permit vlan 10-20
FTOS(conf-if-gi-9/0)#show config
!
interface GigabitEthernet 9/0
 no ip address
 ipv6 access-group AclList1 in implicit-permit Vlan 10-20
 no shutdown
FTOSconf-if-gi-9/0)#
```

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

Syntax

```
ipv6 access-list access-list-name
```

To delete an access list, use the `no ipv6 access-list access-list-name` command.

Parameters

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

Defaults
All 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>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td></td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
</tbody>
</table>

implicit-permit

(Optional) Enter the keyword `implicit-permit` to change the default action of the IPv6 ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the IPv6 ACL, the traffic is permitted instead of dropped).

vlan range

(Optional) Enter the keyword `vlan` followed by the VLAN range in a comma separated format.

Range: 1 to 4094
The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Usage Information

- Related Commands

```
show config
```
View the current configuration.

**permit**

Select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP to configure a filter that match the filter criteria.

**Syntax**

```
permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command.

**Parameters**

- `ip-protocol-number`:
  - Enter an IPv6 protocol number.
  - Range: 0 to 255
- `icmp`:
  - Enter the keyword `icmp` to filter Internet Control Message Protocol version 6.
- `ipv6`:
  - Enter the keyword `ipv6` to filter any Internet Protocol version 6.
- `tcp`:
  - Enter the keyword `tcp` to filter the Transmission Control protocol.
- `udp`:
  - Enter the keyword `udp` to filter the User Datagram Protocol.

**Defaults**

Not configured.

**Command Modes**

ACCESS-LIST

**permit icmp**

Configure a filter to allow all or specific ICMP messages.

**Syntax**

```
permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [message-type] [count [byte]] | [log] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

**Parameters**

- `source address`:
  - Enter the IPv6 address of the network or host from which the packets were sent in the `X::X::X::X` format followed by the prefix length in the `/X` format.
  - Range: /0 to /128
  - The `::` notation specifies successive hexadecimal fields of zero.
- `mask`:
  - Enter a network mask in /prefix format (/X).
- `any`:
  - Enter the keyword `any` to specify that all routes are subject to the filter.
**permit tcp**

Configure a filter to pass TCP packets that match the filter criteria.

**Syntax**

```
permit tcp {source address mask | any | host ipv6-address} [operator port [port]]
{destination address | any | host ipv6-address} [bit] [operator port [port]] [count | byte] | [log] [monitor]
```

To remove this filter, you have two choices:

- Use the **no seq sequence-number** command syntax if you know the filter’s sequence number or
- Use the **no permit tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}** command.

**Defaults**

Not configured

**Command Modes**

ACCESS-LIST

**Command History**

- Version 8.4.2.1 Introduced on the S-Series
- Version 8.2.1.0 Introduced on the E-Series ExaScale
- Version 7.8.1.0 Introduced on the C-Series
- Version 7.4.1.0 Introduced on the E-Series TeraScale
  - Added **monitor** option

**Usage Information**

The C-Series cannot count both packets and bytes, so when you enter the **count byte** options, only bytes are incremented.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>source address</strong></td>
<td>Enter the IPv6 address of the network or host from which the packets were sent in the <code>x:x:x::x</code> format followed by the prefix length in the <code>/x</code> format. Range: /0 to /128. The <code>::</code> notation specifies successive hexadecimal fields of zero.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>Enter a network mask in /prefix format (<code>/x</code>).</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Enter the keyword <code>any</code> to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td><strong>host ipv6-address</strong></td>
<td>Enter the keyword <code>host</code> followed by the IPv6 address of the host in the <code>x:x:x::x</code> format. The <code>::</code> notation specifies successive hexadecimal fields of zero.</td>
</tr>
</tbody>
</table>
| **operator** | (OPTIONAL) Enter one of the following logical operand:  
  - `eq` = equal to  
  - `neq` = not equal to  
  - `gt` = greater than  
  - `lt` = less than  
  - `range` = inclusive range of ports (you must specify two port for the `port` parameter.) |
| **port port** | Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers:  
  - 23 = Telnet  
  - 20 and 21 = FTP  
  - 25 = SMTP  
  - 169 = SNMP |
| **destination address** | Enter the IPv6 address of the network or host to which the packets are sent in the `x:x:x::x` format followed by the prefix length in the `/x` format. Range: /0 to /128. The `::` notation specifies successive hexadecimal fields of zero. |
| **bit** | Enter a flag or combination of bits:  
  - `ack`: acknowledgement field  
  - `fin`: finish (no more data from the user)  
  - `psh`: push function  
  - `rst`: reset the connection  
  - `syn`: synchronize sequence numbers  
  - `urg`: urgent field |
| **count** | (OPTIONAL) Enter the keyword `count` to count packets processed by the filter. |
| **byte** | (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter. |
| **log** | (OPTIONAL) Enter the keyword `log` to enter ACL matches in the log. |
| **monitor** | (OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation. |

**Defaults**
Not configured.

**Command Modes**
ACCESS-LIST
The C-Series 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 bitmask 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 8 entries in the CAM:

```
 Rule#       Data             Mask       From  To    #Covered
  1     0000111111010000 1111111111100000 4000  4031  32
  2     0000111111000000 1111111111000000 4032  4095  64
  3     0001000000000000 1111111111000000 4096  6143  2048
  4     0001100000000000 1111111111000000 6144  7167  1024
  5     0001110000000000 1111111111000000 7168  7679  512
  6     0001111000000000 1111111111000000 7680  7935  256
  7     0001111100000000 1111111111000000 7936  7999  64
  8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

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

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

Total Ports: 1024
```

**Related Commands**

- `permit` Assign a permit filter for IPv6 packets.
- `permit udp` Assign a permit filter for UDP packets.

**permit udp**

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

**Syntax**

```
permit udp {source address mask | any | host ipv6-address} [operator port [port]]
{destination address | any | host ipv6-address} [operator port [port]] [count [byte]] | [log]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no permit udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.
IPv6 Access Control Lists (IPv6 ACLs)

- **Parameters**
  - **source address**: Enter the IPv6 address of the network or host from which the packets were sent in the `x:x:x::x` format followed by the prefix length in the `/x` format.
    - Range: /0 to /128
    - The '::' notation specifies successive hexadecimal fields of zero.
  - **mask**: Enter a network mask in /prefix format (/x).
  - **any**: Enter the keyword `any` to specify that all routes are subject to the filter.
  - **host ipv6-address**: Enter the keyword `host` followed by the IPv6 address of the host in the `x:x:x::x` format.
    - The '::' notation specifies successive hexadecimal fields of zero.
  - **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 address**: Enter the IPv6 address of the network or host to which the packets are sent in the `x:x:x::x` format followed by the prefix length in the `/x` format.
    - Range: /0 to /128
    - The '::' notation specifies successive hexadecimal fields of zero.
  - **count** (OPTIONAL): Enter the keyword `count` to count packets processed by the filter.
  - **byte** (OPTIONAL): Enter the keyword `byte` to count bytes processed by the filter.
  - **log** (OPTIONAL): Enter the keyword `log` to enter ACL matches in the log.
  - **monitor** (OPTIONAL): Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

- **Defaults**
  - Not configured.

- **Command Modes**
  - ACCESS-LIST

- **Command History**
  - Version 8.4.2.1 Introduced on the S-Series
  - Version 8.2.1.0 Introduced support on the E-Series ExaScale
  - Version 7.8.1.0 Introduced support on the C-Series
  - Version 7.4.1.0 Introduced support on the E-Series TeraScale
  - Added `monitor` option

- **Usage Information**
  - The C-Series 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 bitmask 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 8 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 1111111111100000</td>
<td>4000 4031 32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0000111111100000 1111111111100000</td>
<td>4032 4095 64</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000 1111100000000000</td>
<td>4096 6143 2048</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000 1111110000000000</td>
<td>6144 7167 1024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000 1111111000000000</td>
<td>7168 7679 512</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0001110000000000 1111111100000000</td>
<td>7680 7935 256</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000 1111111111000000</td>
<td>7936 7999 64</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0001111101000000 1111111111111111</td>
<td>8000 8000 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Ports: 4001

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

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

Total Ports: 1024

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>permit</strong></td>
<td>Assign a permit filter for IP packets.</td>
</tr>
<tr>
<td><strong>permit tcp</strong></td>
<td>Assign a permit filter for TCP packets.</td>
</tr>
</tbody>
</table>
remark

Enter a description for an IPv6 ACL entry.

Syntax

```
remark remark number [description]
```

To delete the description, use the no remark remark number command (it is not necessary to include the remark description that you are deleting).

Parameters

- `remark number` Enter the remark number. Note that the same sequence number can be used 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

ACCESS-LIST

Command History

- Introduced on the S-Series
- Introduced on the E-Series ExaScale
- Introduced on the C-Series
- Introduced on the E-Series TeraScale

Example

```
FTOS(config-ipv6-acl)#remark 10 Remark for Entry # 10
FTOS(config-ipv6-acl)#show config
!
ipv6 access-list Acl1
description IPV6 Access-list
seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count bytes
remark 10 Remark for Entry # 10
seq 10 permit icmp host 3333:: any mobile-advertisement log
seq 15 deny tcp any any rst
seq 20 permit udp any any gt 100 count
!FTOS(config-ipv6-acl)#
```

Usage Information

As shown in the example above, the same sequence number is used for the remark and an ACL rule. The remark will precede the rule in the running-configuration because it is assumed that the remark is for that rule or that group of rules that follow the remark. You can configure up to 4294967290 remarks in a given ACL.

Related Commands

- `show config` Display the current ACL configuration.
resequence access-list

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

Syntax

resequence access-list {ipv4 | ipv6 | mac} {access-list-name StartingSeqNum Step-to-Increment}

Parameters

- **ipv4 | ipv6 | mac**: Enter the keyword ipv4, ipv6 or mac to identify the access list type to resequence.
- **access-list-name**: Enter the name of a configured IP access list, up to 140 characters. Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- **StartingSeqNum**: Enter the starting sequence number to resequence. Range: 0 - 4294967290
- **Step-to-Increment**: Enter the step to increment the sequence number. Range: 1 - 4294967290

Defaults

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

- Version 8.4.2.0: Introduced on the S-Series
- Version 8.2.1.0: Introduced on the E-Series ExaScale
- Version 7.8.1.0: Introduced on the C-Series
- Version 7.4.1.0: Introduced on the E-Series TeraScale

Usage Information

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

Related Commands

- resequence prefix-list ipv6: Resequence a prefix list
Re-assign sequence numbers to entries of an existing prefix list.

Syntax
```
resequence prefix-list ipv6 \{prefix-list-name StartingSeqNum Step-to-increment\}
```

Parameters
- `prefix-list-name` Enter the name of configured prefix list, up to 140 characters. Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- `StartingSeqNum` Enter the starting sequence number to resequence. Range: 0 – 65535
- `Step-to-Increment` Enter the step to increment the sequence number. Range: 1 – 65535

Defaults
No default values or behavior

Command Modes
EXEC

EXEC Privilege

Command History
- Version 8.4.2.1 Introduced on the S-Series
- Version 8.2.1.0 Introduced on the E-Series ExaScale
- Version 7.8.1.0 Introduced on the C-Series
- Version 7.4.1.0 Introduced on the E-Series TeraScale

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

Related Commands
- `resequence access-list` Resequence an access-list
Assign a sequence number to a deny or permit filter in an IPv6 access list while creating the filter.

**Syntax**

```
seq sequence-number {deny | permit} {ipv6-protocol-number | icmp | ip | tcp | udp} 
{source address mask | any | host ipv6-address} 
{destination address | any | host ipv6-address} 
[operator port [port]] [count [byte]] | [log] [monitor]
```

To delete a filter, use the `no seq sequence-number` command.

**Parameters**

- **sequence-number**: Enter a number from 0 to 4294967290.
- **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.
- **ipv6-protocol-number**: Enter an IPv6 protocol number. Range: 0 to 255
- **icmp**: Enter the keyword `icmp` to configure an Internet Control Message Protocol version 6 filter.
- **ipv6**: Enter the keyword `ipv6` to configure any Internet Protocol version 6 filter.
- **tcp**: Enter the keyword `tcp` to configure a Transmission Control protocol filter.
- **udp**: Enter the keyword `udp` to configure a User Datagram Protocol filter.
- **source address**: Enter the IPv6 address of the network or host from which the packets were sent in the `X:X:X:..X` format followed by the prefix length in the `/X` format. Range: /0 to /128
  - The '::' notation specifies successive hexadecimal fields of zero.
- **mask**: Enter a network mask in /prefix format (`/X`).
- **any**: Enter the keyword `any` to specify that all routes are subject to the filter.
- **host ipv6-address**: Enter the keyword `host` followed by the IPv6 address of the host in the `X:X:X:..X` format.
  - The '::' notation specifies successive hexadecimal fields of zero.
- **operator** (OPTIONAL): Enter one of the following logical operands:
  - `eq` = equal to
  - `neq` = not equal to
  - `gt` = greater than
  - `lt` = less than
  - `range` = inclusive range of ports (you must specify two ports for the `port` parameter.)
- **port port** (OPTIONAL): Enter the application layer port number. Enter two port numbers if using the `range` logical operand.
  - Range: 0 to 65535
  - The following list includes some common TCP port numbers:
    - 23 = Telnet
    - 20 and 21 = FTP
    - 25 = SMTP
    - 169 = SNMP
**destination address**
Enter the IPv6 address of the network or host to which the packets are sent in the `X:X:X:X:X` format followed by the prefix length in the `/x` format.

Range: `/0` to `/128`

The `::` notation specifies successive hexadecimal fields of zero.

**message-type**
(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type.

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.

**log**
(OPTIONAL) Enter the keyword `log` to enter ACL matches in the log.

Supported on Jumbo-enabled line cards only.

**monitor**
(OPTIONAL) Enter the keyword `monitor` to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

**Defaults**
Not configured.

**Command Modes**
ACCESS-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the E-Series TeraScale and S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added <code>monitor</code> option</td>
</tr>
</tbody>
</table>

**Related Commands**

- `deny` Configure a filter to drop packets.
- `permit` Configure a filter to forward packets.
show cam-acl

Show space allocated for IPv6 ACLs.

Syntax

show cam-acl

Command Modes

EXEC

EXEC Privileged

Command History

Version 8.4.2.1  Introduced on the S-Series
Version 8.4.2.0  Introduced on the E-Series TeraScale
Version 7.8.1.0  Introduced on the C-Series

Related Commands

cam-acl  Configure CAM profiles to support IPv6 ACLs

Examples

Figure 25-3.  Command Example: show cam-acl (default profile)

FTOS#show cam-acl

-- Chassis Cam ACL --
  Current Settings(in block sizes)
  L2Acl      :         5
  Ipv4Acl    :         6
  Ipv6Acl    :         0
  Ipv4Qos    :         1
  L2Qos      :         1

-- Line card 4 --
  Current Settings(in block sizes)
  L2Acl      :         2
  Ipv4Acl    :         2
  Ipv6Acl    :         4
  Ipv4Qos    :         2
  L2Qos      :         3

FTOS#show cam-acl

Figure 25-4.  Command Example: show cam-acl (manually set profiles)

FTOS#show cam-acl

-- Chassis Cam ACL --
  Current Settings(in block sizes)
  L2Acl      :         2
  Ipv4Acl    :         2
  Ipv6Acl    :         4
  Ipv4Qos    :         2
  L2Qos      :         3

-- Line card 4 --
  Current Settings(in block sizes)
  L2Acl      :         2
  Ipv4Acl    :         2
  Ipv6Acl    :         4
  Ipv4Qos    :         2
  L2Qos      :         3

FTOS#show cam-acl
show config

View the current IPv6 ACL configuration.

Syntax

show config

Command Modes

ACCESS-LIST

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>Version 8.4.2.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
</tbody>
</table>

Example

Figure 25-5. Command Example: show config

```
FTOS(conf-ipv6-acl)#show config
! ipv6 access-list Acl1
  seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count bytes
  seq 10 permit icmp host 3333:: any mobile-advertisement log
  seq 15 deny tcp any any rst
  seq 20 permit udp any any gt 100 count
FTOS(conf-ipv6-acl)#
```

show ipv6 accounting access-list

View the IPv6 access-lists created on the E-Series and the sequence of filters.

Syntax

show ipv6 accounting {access-list access-list-name | cam_count} interface interface

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-name</td>
<td>Enter the name of the ACL to be displayed, up to 140 characters.</td>
</tr>
<tr>
<td>cam_count</td>
<td>List the count of the CAM rules for this ACL.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter the keyword interface followed by the interface type and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port 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>- C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>- E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>- For a SONET interface, enter the keyword sonet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC

EXEC Privilege
**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code></td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td></td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Example**

**Figure 25-6. Command Example: show ipv6 accounting access-lists**

```
FTOS#show ipv6 accounting access-list 
Ingress IPv6 access list AclList1 on GigabitEthernet 9/0
Total cam count 15
  seq 10 permit icmp host 3333:: any mobile-advertisement log 
  seq 15 deny tcp any any rst
  seq 20 permit udp any any gt 101 count (0 packets)

FTOS#
```

**Table 25-2. show ip accounting access-lists Command Example Field**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Ingress IPv6...”</td>
<td>Displays the name of the IPv6 ACL, in this example “AclList1”.</td>
</tr>
<tr>
<td>“seq 10...”</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>
</tbody>
</table>

**show running-config acl**

Display the ACL running configuration.

**Syntax**

`show running-config acl`

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced support on the E-Series TeraScale</td>
</tr>
</tbody>
</table>
**Example**

**Figure 25-7. Command Example: show running-config acl**

```
FTOS#show running-config acl
!
ip access-list extended ext-acl1
!
ip access-list standard std-acl1!
ipv6 access-list Acl1
description IPV6 Access-list
seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count bytes
remark 10 Remark for Entry # 10
seq 10 permit icmp host 3333:: any mobile-advertisement log
seq 15 deny tcp any any rst
seq 20 permit udp any any gt 100 count
!FTOS#
```

**test cam-usage**

Verify that enough ACL CAM space is available for the IPv6 ACLs you have created.

**Syntax**

```
test cam-usage service-policy input policy name linecard {number | all}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-map name</td>
<td>Enter the name of the policy-map to verify.</td>
</tr>
<tr>
<td>number</td>
<td>Enter <strong>all</strong> to get information for all the line cards, or enter the line card <strong>number</strong> to get information for a specific card.</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td></td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td></td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td></td>
<td>Introduced on C-Series and E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Usage Information**

This command applies to both IPv4 and IPv6 CAM Profiles, but is best used when verifying QoS optimization for IPv6 ACLs.

QoS Optimization for IPv6 ACLs does not impact the CAM usage for applying a policy on a single (or the first of several) interfaces. It is most useful when a policy is applied across multiple interfaces; it can reduce the impact to CAM usage across subsequent interfaces.
Example  The following example shows the output shown when using the test cam-usage command.

Figure 25-8. Command Example: test cam-usage (C-Series)

FTOS#test cam-usage service-policy input LauraMapTest linecard all

<table>
<thead>
<tr>
<th>Linecard</th>
<th>Portpipe</th>
<th>CAM Partition</th>
<th>Available CAM</th>
<th>Estimated CAM per Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>IPv4Flow</td>
<td>232</td>
<td>0</td>
<td>Allowed</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>IPv6Flow</td>
<td>0</td>
<td>0</td>
<td>Allowed</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>IPv4Flow</td>
<td>232</td>
<td>0</td>
<td>Allowed</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>IPv6Flow</td>
<td>0</td>
<td>0</td>
<td>Allowed</td>
</tr>
</tbody>
</table>

FTOS#

FTOS#test cam-usage service-policy input LauraMapTest linecard 4 port-set 0

<table>
<thead>
<tr>
<th>Linecard</th>
<th>Portpipe</th>
<th>CAM Partition</th>
<th>Available CAM</th>
<th>Estimated CAM per Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
<td>IPv4Flow</td>
<td>232</td>
<td>0</td>
<td>Allowed</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>IPv6Flow</td>
<td>0</td>
<td>0</td>
<td>Allowed</td>
</tr>
</tbody>
</table>

FTOS#

FTOS#test cam-usage service-policy input LauraMapTest linecard 2 port-set 1

<table>
<thead>
<tr>
<th>Linecard</th>
<th>Portpipe</th>
<th>CAM Partition</th>
<th>Available CAM</th>
<th>Estimated CAM per Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>IPv4Flow</td>
<td>232</td>
<td>0</td>
<td>Allowed</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>IPv6Flow</td>
<td>0</td>
<td>0</td>
<td>Allowed</td>
</tr>
</tbody>
</table>

FTOS#

Table 25-3. Output Explanations: test cam-usage

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linecard</td>
<td>Lists the line card or line cards that are checked. Entering <strong>all</strong> shows</td>
</tr>
<tr>
<td></td>
<td>the status for line cards in the chassis</td>
</tr>
<tr>
<td>Portpipe</td>
<td>Lists the portpipe (port-set) or port pipes (port-sets) that are checked.</td>
</tr>
<tr>
<td></td>
<td>Entering <strong>all</strong> shows the status for line cards and port-pipes in the</td>
</tr>
<tr>
<td></td>
<td>chassis.</td>
</tr>
<tr>
<td>CAM Partition</td>
<td>Shows the CAM profile of the CAM</td>
</tr>
<tr>
<td>Available CAM</td>
<td>Identifies the amount of CAM space remaining for that profile</td>
</tr>
<tr>
<td>Estimated CAM per Port</td>
<td>Estimates the amount of CAM space the listed policy will require.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether or not the policy will be allowed in the CAM</td>
</tr>
</tbody>
</table>
### IPv6 Route Map Commands

The following commands allow you to configure route maps and their redistribution criteria.

- match ipv6 address
- match ipv6 next-hop
- match ipv6 route-source
- route-map
- set ipv6 next-hop
- show config
- show route-map

#### match ipv6 address

Configure a filter to match routes based on IPv6 addresses specified in an access list.

**Syntax**
```
match ipv6 address prefix-list-name
```

To delete a match, use the `no match ipv6 address prefix-list-name` command.

**Parameters**

- **prefix-list-name**: Enter the name of IPv6 prefix list, up to 140 characters.

**Defaults**
Not configured.

**Command Modes**
ROUTE-MAP

**Command History**

- **Version 8.4.2.1**: Introduced on the S-Series
- **Version 8.2.1.0**: Introduced support on the E-Series ExaScale
- **Version 7.8.1.0**: Introduced support on the C-Series
  - Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- **Version 7.4.1.0**: Introduced support on the E-Series TeraScale

**Related Commands**

- match ipv6 next-hop
- match ipv6 route-source

#### match ipv6 next-hop

Configure a filter which matches based on the next-hop IPv6 addresses specified in the IPv6 prefix list.

**Syntax**
```
match ipv6 next-hop prefix-list prefix-list-name
```

To delete a match, use the `no match ipv6 next-hop prefix-list prefix-list-name` command.

**Parameters**

- **prefix-list**: Enter the keywords `prefix-list` followed by the name of configured prefix list, up to 140 characters.

- **prefix-list-name**: Enter the name of IPv6 prefix list, up to 140 characters.

**Defaults**
Not configured.

**Command Modes**
ROUTE-MAP

**Command History**

- **Version 8.4.2.1**: Introduced on the S-Series
- **Version 8.2.1.0**: Introduced support on the E-Series ExaScale
- **Version 7.8.1.0**: Introduced support on the C-Series
  - Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
- **Version 7.4.1.0**: Introduced support on the E-Series TeraScale

**Related Commands**

- match ipv6 address
- match ipv6 route-source
IPv6 Access Control Lists (IPv6 ACLs)

match ipv6 route-source

Configure a filter which matches based on the routes advertised in the IPv6 prefix lists.

Syntax

match ipv6 route-source prefix-list prefix-list-name

To delete a match, use the no match ipv6 route-source prefix-list prefix-list-name command.

Parameters

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 8.4.2.1 Introduced on the S-Series
Version 8.2.1.0 Introduced support on the E-Series ExaScale
Version 7.8.1.0 Introduced support on the C-Series
Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
Version 7.4.1.0 Introduced support on the E-Series TeraScale

Related Commands

match ipv6 address Redistribute routes that match an IP address.
match ipv6 route-source Redistribute routes that match routes advertised by other routers.
route-map

Designate a IPv6 route map name and enter the ROUTE-MAP mode.

Syntax

```
route-map map-name
```

To delete a route map, use the `no route-map map-name` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>map-name</code></td>
<td>Enter a text string to name the route map, up to 140 characters.</td>
</tr>
</tbody>
</table>

Defaults

Not configured

Command Modes

ROUTE-MAP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced support on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on the C-Series</td>
</tr>
<tr>
<td></td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced support on the E-Series TeraScale</td>
</tr>
</tbody>
</table>

Example

```
Figure 25-9. Command Example: route-map

FTOS(conf)#route-map Rmap1
FTOS(config-route-map)#match ?
... ip IP specific information
ipv6 IPv6 specific information
...
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show config</td>
<td>View the current configuration.</td>
</tr>
</tbody>
</table>

set ipv6 next-hop

Configure a filter that specifies IPv6 address as the next hop.

Syntax

```
set ipv6 next-hop ipv6-address
```

To delete the setting, use the `no set ipv6 next-hop ipv6-address` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6-address</code></td>
<td>Enter the IPv6 address in the <code>X:X:X::X</code> format.</td>
</tr>
</tbody>
</table>

Note: The `::` notation specifies successive hexadecimal fields of zeros

Defaults

Not configured.

Command Modes

ROUTE-MAP
The `set ipv6 next-hop` command is the only way to set an IPv6 Next-Hop.

**show config**

View the current route map configuration.

**Syntax**

```
show config
```

**Command Modes**

ROUTE-MAP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced support on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced support on the E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS(config-route-map)#show config
!
route-map Rmap1 permit 10
match ip address v4plist
match ipv6 address plist1
match ipv6 next-hop prefix-list plist2
match ipv6 route-source prefix-list plist3
set next-hop 1.1.1.1
set ipv6 next-hop 3333:2222::
```

**show route-map**

View the current route map configurations.

**Syntax**

```
show route-map
```

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced support on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on the C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced support on the E-Series TeraScale</td>
</tr>
</tbody>
</table>
Example Figure 25-11. Command Example: show route-map

FTOS#show route-map
!
route-map Rmap1, permit, sequence 10
Match clauses:
ip address: v4plist
ipv6 address: plist1
ipv6 next-hop prefix-lists: plist2
ipv6 route-source prefix-lists: plist3
Set clauses:
next-hop 1.1.1.1
ipv6 next-hop 3333:2222::

Related Commands

route-map Configure a route map.
IPv6 Basics

Overview

IPv6 Basic Commands are supported on platforms: C E S

Note: Basic IPv6 basic commands are supported on all platforms. For information on the Dell Networking OS version and platform that supports IPv6 in each software feature, refer to the FTOS Configuration Guide.

Commands

The IPv6 commands in the chapter are:

- clear ipv6 fib
- clear ipv6 route
- ipv6 address
- ipv6 host
- ipv6 nd prefix-advertisement
- ipv6 route
- ipv6 unicast-routing
- show ipv6 cam linecard
- show ipv6 cam stack-unit
- show ipv6 fib linecard
- show ipv6 fib stack-unit
- show ipv6 interface
- show ipv6 route
- trust ipv6-diffserv
clear ipv6 fib

Syntax  clear ipv6 fib linecard slot

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>Enter the slot number to clear the FIB for a linecard.</td>
</tr>
</tbody>
</table>

Command Mode

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

clear ipv6 route

Syntax  clear ipv6 route {* | ipv6-address prefix-length}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Enter the * to clear (refresh) all routes from the IPv6 routing table.</td>
</tr>
<tr>
<td>ipv6-address prefix-length</td>
<td>Enter the IPv6 address in the x:x::X format followed by the prefix length in the /x format. Range: /0 to /128</td>
</tr>
</tbody>
</table>

Note: The :: notation specifies successive hexadecimal fields of zeros

Command Mode

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

ipv6 address

Syntax  ipv6 address {ipv6-address prefix-length}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address prefix-length</td>
<td>Enter the IPv6 address in the x:x::X format followed by the prefix length in the /x format. Range: /0 to /128</td>
</tr>
</tbody>
</table>

Note: The :: notation specifies successive hexadecimal fields of zeros

Defaults

No default values or behavior

Command Modes

INTERFACE
Dell Networking OS allows multiple IPv6 addresses to be configured on an interface. When the `no ipv6 address` command is issued without specifying a particular IPv6 address, all IPv6 addresses on that interface are deleted.

Figure 26-1. Command Example: ipv6 address

FTOS (conf)#interface gigabitethernet 10/0
   FTOS(conf-if-gi-10/0)#ipv6 address ?
   X:X:X::X          IPv6 address
   FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 ?
   <0-128>           Prefix length in bits
   FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96 ?
   <cr>
   FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96
   FTOS(conf-if-gi-10/0)#show config
   !
   interface GigabitEthernet 10/0
   no ip address
   ipv6 address 2002:1:2::3 /96
   no shutdown
   FTOS(conf-if-gi-10/0)#

ipv6 name-server

Enter up to 6 IPv6 addresses of name servers. The order you enter the addresses determines the order of their use.

Syntax

`ipv6 name-server ipv6-address [ipv6-address2...ipv6-address6]`

Parameters

- `ipv6-address`: Enter the IPv6 address (X:X:X::X) of the name server to be used.
- `ipv6-address2...ipv6-address6`: Enter up five more IP 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 8.4.2.1 Introduced on the C-Series and S-Series
- Version 8.4.1.0 Introduced on E-Series TeraScale

Usage Information

You can separately configure both IPv4 and IPv6 domain name servers.
ipv6 host Assign a name and IPv6 address to be used by the host-to-IP address mapping table.

**Syntax**

```
ipv6 host name ip-address
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Enter a text string to associate with one IP address.</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>Enter an IPv6 address (X:X::X) to be mapped to the name.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>
ipv6 nd prefix-advertisement

Specify which IPv6 prefixes are included in Neighbor Advertisements. By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; the `default` keyword can be used to use the default parameters for all prefixes.

**Syntax**

```
ipv6 nd prefix {ipv6-address/prefix-length> | default} [no-advertise] [no-autoconfig] [no-rtr-address] [off-link] [lifetime {valid | infinite} {preferred | infinite}]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-prefix</td>
<td>Enter an IPv6 prefix.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>Enter the prefix followed by the prefix length.</td>
</tr>
<tr>
<td>default</td>
<td>Enter this keyword to set default parameters for all prefixes.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Enter this keyword to prevent the specified prefix from being advertised.</td>
</tr>
<tr>
<td>no-autoconfig</td>
<td>Enter this keyword to disable Stateless Address Autoconfiguration.</td>
</tr>
<tr>
<td>no-rtr-address</td>
<td>Enter this keyword to exclude the full router address from router advertisements (the R bit is not set).</td>
</tr>
<tr>
<td>off-link</td>
<td>Enter this keyword to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.</td>
</tr>
<tr>
<td>valid-lifetime</td>
<td>Enter the amount of time that the prefix is advertised, or enter <code>infinite</code> for an unlimited amount of time.</td>
</tr>
<tr>
<td>infinite</td>
<td>Default: 2592000</td>
</tr>
<tr>
<td>preferred-lifetime</td>
<td>Enter the amount of time that the prefix is preferred, or enter <code>infinite</code> for an unlimited amount of time.</td>
</tr>
<tr>
<td>infinite</td>
<td>Default: 604800; the maximum value means that the preferred lifetime does not expire.</td>
</tr>
</tbody>
</table>

**Command Mode**

`INTERFACE`

**Command History**

`Version 8.3.2.0` Introduced on the E-Series TeraScale, C-Series, and S-Series.
ipv6 route

Establish a static IPv6 route.

**Syntax**

```
ipv6 route ipv6-address prefix-length {interface | ipv6-address} [distance] [tag value] [permanent]
```

To remove the IPv6 route, use the `no ipv6 route ipv6-address prefix-length {interface | ipv6-address} [distance] [tag value] [permanent]` command.

**Parameters**

- `ipv6-address prefix-length` Enter the IPv6 destination address in the `x:x:x::x` format followed by the prefix length in the `/x` format.
  - Range: /0 to /128
  - **Note:** The `::` notation specifies successive hexadecimal fields of zeros
- `interface` Enter one of the following keywords and slot/port or number information of the egress interface on the router:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a loopback interface, enter the keyword `loopback` followed by a number from zero (0) to 16383.
  - For the null interface, enter the keyword `null` followed by zero (0).
  - For a 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.
  - **Note:** If you configure a static IPv6 route using an egress interface and enter the `ping` command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the `ping` command to detect the destination address.
- `ipv6-address` Enter the next-hop address of an IPv6 neighbor router in the `x:x:x:x::x` format.
  - **Note:** The `::` notation specifies successive hexadecimal fields of zeros
- `distance` (OPTIONAL) Enter a number as the distance metric assigned to the route.
  - Range: 1 to 255
- `tag value` (OPTIONAL) Enter the keyword `tag` followed by a tag value number.
  - Range: 1 to 4294967295
- `permanent` (OPTIONAL) Enter the keyword `permanent` to specify that the route is not to be removed, even if the interface assigned to that route goes down.
  - **Note:** If you disable the interface with an IPv6 address associated with the keyword `permanent`, the route disappears from the routing table.

**Defaults**

No default values or behavior

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
<td></td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
<td></td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
<td></td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
<td></td>
</tr>
</tbody>
</table>
### Example Figure 26-2. Command Example: ipv6 route

```
FTOS(conf)#ipv6 route 44::0 /64 33::1 ?
<1-255> Distance metric for this route
permanent Permanent route
tag Set tag for this route

FTOS(conf)#ipv6 route 55::0 /64 ?
X:X:X:X::X Forwarding router's address
gigabitethernet Gigabit Ethernet interface
loopback Loopback interface
null Null interface
port-channel Port channel interface
sonet Sonet interface
tenGigabitethernet TenGigabit Ethernet interface
vlan VLAN interface

FTOS(conf)#ipv6 route 55::0 /64 gigabitethernet 9/0 ?
<1-255> Distance metric for this route
X:X:X:X::X Forwarding router's address
permanent Permanent route
tag Set tag for this route

FTOS(conf)#ipv6 route 55::0 /64 gigabitethernet 9/0 66::1 ?
<1-255> Distance metric for this route
permanent Permanent route
tag Set tag for this route
```

### Usage Information
When the interface goes down, FTOS withdrews the route. The route is re-installed, by Dell Networking OS, when the interface comes back up. When a recursive resolution is “broken,” Dell Networking OS withdraws the route. The route is re-installed, by Dell Networking OS, when the recursive resolution is satisfied.

### Related Commands
- `show ipv6 route` View the IPv6 configured routes.
ipv6 unicast-routing

Enable IPv6 Unicast routing.

Syntax

ipv6 unicast-routing

To disable unicast routing, use the no ipv6 unicast-routing command.

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

Usage Information

Since this command is enabled by default, it does not appear in the running configuration. When unicast routing is disabled, the no ipv6 unicast-routing command is included in the running configuration. Whenever unicast routing is disabled or re-enabled, Dell Networking OS generates a syslog message indicating the action.

Disabling unicast routing on an E-Series chassis causes the following behavior:

- static and protocol learnt routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated.
- connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable
- additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed
- the IPv6 address family configuration (under router bgp) is deleted
- IPv6 Multicast traffic continues to flow unhindered
show ipv6 cam linecard

Displays the IPv6 CAM entries for the specified line card.

**Syntax**

```
show ipv6 cam linecard slot-number port-set {0-1} [summary | index | ipv6 address]
```

**Parameters**

- **slot-number**
  - Enter the line card slot ID number.
  - Range: 0 to 13 on the E1200; 0 on 6 for E600, and 0 to 5 on the E300.

- **port-set**
  - Enter the Port Set to

- **summary**
  - (OPTIONAL) Enter the keyword `summary` to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.

- **index**
  - (OPTIONAL) Enter the index in the IPv6 CAM

- **ipv6-address**
  - Enter the IPv6 address in the `x:x:x:x::x/n` format to display networks that have more specific prefixes.
  - Range: /0 to /128
  - **Note:** The `::` notation specifies successive hexadecimal fields of zeros.

**Defaults**

No default values or behavior

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on S-Series
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.8.1.0 Introduced on C-Series
- Version 7.4.1.0 Introduced on E-Series TeraScale

**Usage Information**

The forwarding table displays host route first, then displays route originated by routing protocol including static route.

The egress port section displays the egress port of the forwarding entry which is designated as:

- C for the Control Processor
- 1 for the Route Processor 1
- 2 for the Route Processor 2

**Note:** If a link-local IPv6 address is statically configured and dynamically learned on a C-Series router, the dynamically -learned IPv6 address is displayed in `show ipv6 cam linecard` output, but the statically-configured IPv6 address may not be displayed. Use the `show ipv6 fib linecard` or `show ipv6 neighbors` commands to display statically-configured addresses of IPv6 neighbors.
### Examples

#### Figure 26-3. Command Example: `show ipv6 cam linecard fib` (C or E-Series)

```
FTOS#show ipv6 cam linecard 13 fib
Neighbor                          Mac-Addr          Port     VId
--------------------------------- ----------------- -------- ----
[   31] 2002:44:1:1::11           00:00:01:1a:1e:d5 Gi 13/2  0
Prefix                          Next-Hop                        Mac-Addr          Port     VId  EC
------------------------------- ------------------------------- ----------------- -------- ---- --
[ 3147] 100::/64                [ 0] 2002:44:1:1::11                -          Gi 0/0       0 1
[   0] 2002:44:1:24::11           -          Gi 0/0       0 1
[   0] 2002:44:1:23::11           -          Gi 0/0       0 1
[   0] 2002:44:1:21::11           -          Gi 0/0       0 1
[   0] 2002:44:1:20::11           -          Gi 0/0       0 1
[   0] 2002:44:1:19::11           -          Gi 0/0       0 1
FTOS#
```

#### Figure 26-4. Command Example: `show ipv6 cam linecard` (C or E-Series)

```
FTOS#show ipv6 cam linecard 1 port-set 0
Neighbor                                         Mac-Addr          Port     VId
------------------------------------------------- ----------------- -------- ----
[    0] fe80::201:e8ff:fe17:5cae                  00:01:e8:17:5c:ae BLK     100
[    1] fe80::201:e8ff:fe17:5bbe                  00:01:e8:17:5b:be BLK     0
[    2] fe80::201:e8ff:fe17:5bbd                  00:01:e8:17:5b:bd BLK     0
[    3] fe80::201:e8ff:fe17:5cb0                   00:01:e8:17:5c:b0 BLK     0
[    4] fe80::201:e8ff:fe17:5cafe                  00:01:e8:17:5c:af BLK    1000
[    5] fe80::201:e8ff:fe17:5caf                    00:01:e8:17:5c:af BLK     0
Prefix                          First-Hop                        Mac-Addr          Port     VId  EC
--------------------------------- ------------------------  ----------------- -------- ---- --
[   80] 2222::2/128                 [    2] ::1               00:00:00:00:00:00 RP2     0 0
[   81] 3333::2/128                 [    2] ::1               00:00:00:00:00:00 RP2     0 0
FTOS#
```
show ipv6 cam stack-unit

Displays the IPv6 CAM entries for the specified stack-unit.

Syntax

```
show ipv6 cam stack-unit unit-number port-set {0-1} [summary | index | ipv6 address]
```

Parameters

- **unit-number**: Enter the stack unit’s ID number.
  - Range: 0 to 7
- **port-set**: Enter the Port Set to
- **summary** (OPTIONAL): Enter the keyword `summary` to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.
- **index** (OPTIONAL): Enter the index in the IPv6 CAM
- **ipv6-address** (OPTIONAL): Enter the IPv6 address in the `X:X:X:X::X/n` format to display networks that have more specific prefixes.
  - Range: /0 to /128
  - **Note**: The `::` notation specifies successive hexadecimal fields of zeros.

Defaults

No default values or behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 8.4.2.1**: Introduced on C-Series and S-Series
- **Version 7.8.1.0**: Introduced on E-Series TeraScale
show ipv6 fib linecard

View all Forwarding Information Base entries.

Syntax

```
show ipv6 fib linecard slot-number \{summary | ipv6-address\}
```

Parameters

- **slot-number**: Enter the number of the line card slot.
  
  E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300

- **summary**: (OPTIONAL) Enter the keyword `summary` to view a summary of entries in IPv6 cam.

- **ipv6-address**: Enter the IPv6 address in the `x:x:x:x::x/n` format to display networks that have more specific prefixes.
  
  Range: /0 to /128

  **Note**: The `::` notation specifies successive hexadecimal fields of zeros.

Command Mode

- EXEC
- EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series TeraScale</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series TeraScale</td>
</tr>
</tbody>
</table>

show ipv6 fib stack-unit

View all Forwarding Information Base entries.

Syntax

```
show ipv6 fib stack-unit unit-number \{summary\} ipv6-address
```

Parameters

- **slot-number**: Enter the number of the stack unit.
  
  Range: 0 to 7

- **summary**: (OPTIONAL) Enter the keyword `summary` to view a summary of entries in IPv6 cam.

- **ipv6-address**: Enter the IPv6 address in the `x:x:x:x::x/n` format to display networks that have more specific prefixes.
  
  Range: /0 to /128

  **Note**: The `::` notation specifies successive hexadecimal fields of zeros.

Command Mode

- EXEC
- EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series TeraScale</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series TeraScale</td>
</tr>
</tbody>
</table>
show ipv6 interface

Display the status of interfaces configured for IPv6.

Syntax

```
show ipv6 interface [brief] [configured] [gigabitethernet slot | slot/port] [linecard slot-number] [loopback interface-number] [managementethernet slot/port] [port-channel number] [tengigabitethernet slot | slot/port] [fortyGigE slot | slot/port] [vlan vlan-id]
```

Parameters

- `interface` (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Loopback interface, enter the keyword `Loopback` followed by a number from 0 to 16383.
  - For the Null interface, enter the keyword `null` followed by zero (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.

- `brief` (OPTIONAL) View a summary of IPv6 interfaces.

- `configured` (OPTIONAL) View information on all IPv6 configured interfaces

- `gigabitethernet` (OPTIONAL) View information for an IPv6 gigabitethernet interface.

- `linecard slot-number` (OPTIONAL) View information for a specific IPv6 linecard or S-Series stack-unit
  - Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
  - Range: 0-7 for C-Series
  - Range 0-7 for S-Series

- `managementethernet slot/port` (OPTIONAL) View information on an IPv6 Management port. Enter the slot number (0-1) and port number zero (0).

- `loopback` (OPTIONAL) View information for IPv6 loopback interfaces.

- `port-channel` (OPTIONAL) View information for IPv6 port channels.

- `tengigabitethernet` (OPTIONAL) View information for an IPv6 tengigabit ethernet interface.

- `fortyGigE` (OPTIONAL) View information for an IPv6 40-Gigabit ethernet interface.

- `vlan` (OPTIONAL) View information for IPv6 VLANs.

Defaults

No default values or behavior

Command Modes

```
EXEC
EXEC Privilege
```

Command History

```
Version 8.4.6.0 Added support for the keyword `fortyGigE`.
Version 8.4.2.1 Introduced on S-Series
Version 8.2.1.0 Introduced on E-Series ExaScale.
Support for the `managementethernet slot/port` parameter was added.
Version 7.8.1.0 Introduced on C-Series
Version 7.4.1.0 Introduced on E-Series TeraScale
```

IPv6 Basics | 735
The Management port is enabled by default (no shutdown). If necessary, use the `ipv6 address` command to assign an IPv6 address to the Management port.

**Example**

**Figure 26-5. Command Example: show ipv6 interface**

```bash
FTOS#show ipv6 interface gigabitethernet 1/1
GigabitEthernet 1/1 is up, line protocol is up
   IPv6 is enabled
   Link Local address: fe80::201:e8ff:fe04:62c4
   Global Unicast address(es):
       2001::1, subnet is 2001::/64
       2002::1, subnet is 2002::/120
       2003::1, subnet is 2003::/120
       2004::1, subnet is 2004::/32
   Global Anycast address(es):
   Joined Group address(es):
      ff02::1
      ff02::2
      ff02::1:ff00:1
      ff02::1:ff04:62c4
   MTU is 1500
   ICMP redirects are not sent
   DAD is enabled: number of DAD attempts: 1
   ND reachable time is 30 seconds
   ND advertised reachable time is 30 seconds
   ND advertised retransmit interval is 30 seconds
```

**Figure 26-6. Command Example: show ipv6 interface managementethernet**

```bash
FTOS#show ipv6 interface managementethernet 0/0
ManagementEthernet 0/0 is up, line protocol is up
   IPv6 is enabled
   Link Local address: fe80::201:e8ff:fe0b:a94c
   Global Unicast address(es):
       Actual address is 2222::5, subnet is 2222::/64
   Virtual-IP IPv6 address is not set
   Global Anycast address(es):
   Joined Group address(es):
      ff02::1
      ff02::2
      ff02::1:ff00:5
      ff02::1:ff0b:a94c
   MTU is 1500
   ICMP redirects are not sent
   DAD is enabled, number of DAD attempts: 3
   ND reachable time is 3600000 milliseconds
   ND advertised reachable time is 3600000 milliseconds
   ND advertised retransmit interval is 0 milliseconds
   ND router advertisements are sent every 200 to 600 seconds
   ND router advertisements live for 9000 seconds
```
**Figure 26-7. Command Example: show ipv6 interface brief**

```plaintext
FTOS#show ipv6 interface brief

GigabitEthernet 0/0               [up/up]
    fe80::201:e8ff:fe3a:143e
    10::1/64
...
ManagementEthernet 0/0           [up/up]
    fe80::201:e8ff:fe5d:b74c
    fdaa:bbbb:cccc:1004::50/64
...
Vlan 3                            [up/up]
    fe80::201:e8ff:fe3a:19b7
```
**show ipv6 route**

Displays the IPv6 routes.

**Syntax**

```
show ipv6 route [ipv6-address prefix-length] [hostname] [all] [bgp as number] [connected] [isis tag] [list prefix-list name] [ospf process-id] [rip] [static] [summary]
```

**Parameter**

- `ipv6-address prefix-length` (OPTIONAL) Enter the IPv6 address in the `x:x:x:x` format followed by the prefix length in the `/x` format. Range: `/0` to `/128`. The `::` notation specifies successive hexadecimal fields of zeros.
- `hostname` (OPTIONAL) View information for this IPv6 route with Host Name.
- `all` (OPTIONAL) View information for all IPv6 routes.
- `bgp` (OPTIONAL) View information for all IPv6 BGP routes.
- `connected` (OPTIONAL) View only the directly connected IPv6 routes.
- `isis` (OPTIONAL) View information for all IPv6 IS-IS routes.
- `list` (OPTIONAL) View the IPv6 prefix list.
- `ospf` (OPTIONAL) View information for all IPv6 OSPF routes.
- `rip` (OPTIONAL) View information for all IPv6 RIP routes.
- `static` (OPTIONAL) View only routes configured by the `ipv6 route` command.
- `summary` (OPTIONAL) View a brief list of the configured IPv6 routes.

**Defaults**

No default values or behavior.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Example**

**Figure 26-8. Command Example: show ipv6 route**

```
FTOS#show ipv6 route

Codes:  C - connected, L - local, 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, Gateway of last resort is not set

Destination    Dist/Metric, Gateway,   Last Change
-----------------------------------------------------
C 2001::/64    [0/0] Direct, Gi 1/1, 00:28:49
C 2002::/120   [0/0] Direct, Gi 1/1, 00:28:49
C 2003::/120   [0/0] Direct, Gi 1/1, 00:28:49
C 2004::/32    [0/0] Direct, Gi 1/1, 00:28:49
L fe80::/10    [0/0] Direct, Nu 0, 00:29:09
```
Example

Figure 26-9. Command Example: show ipv6 route summary

```
FTOS#show ipv6 route summary

Route Source             Active Routes Non-active Routes
connected                5               0
static                   0               0
Total                     5               0
Total 5 active route(s) using 952 bytes
```

Table 26-1. show ipv6 route Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(undefined)</td>
<td>Identifies the type of route:</td>
</tr>
<tr>
<td></td>
<td>• L = Local</td>
</tr>
<tr>
<td></td>
<td>• C = connected</td>
</tr>
<tr>
<td></td>
<td>• S = static</td>
</tr>
<tr>
<td></td>
<td>• R = RIP</td>
</tr>
<tr>
<td></td>
<td>• B = BGP</td>
</tr>
<tr>
<td></td>
<td>• IN = internal BGP</td>
</tr>
<tr>
<td></td>
<td>• EX = external BGP</td>
</tr>
<tr>
<td></td>
<td>• LO = Locally Originated</td>
</tr>
<tr>
<td></td>
<td>• O = OSPF</td>
</tr>
<tr>
<td></td>
<td>• IA = OSPF inter area</td>
</tr>
<tr>
<td></td>
<td>• N1 = OSPF NSSA external type 1</td>
</tr>
<tr>
<td></td>
<td>• N2 = OSPF NSSA external type 2</td>
</tr>
<tr>
<td></td>
<td>• E1 = OSPF external type 1</td>
</tr>
<tr>
<td></td>
<td>• E2 = OSPF external type 2</td>
</tr>
<tr>
<td></td>
<td>• i = IS-IS</td>
</tr>
<tr>
<td></td>
<td>• L1 = IS-IS level-1</td>
</tr>
<tr>
<td></td>
<td>• L2 = IS-IS level-2</td>
</tr>
<tr>
<td></td>
<td>• IA = IS-IS inter-area</td>
</tr>
<tr>
<td></td>
<td>• * = candidate default</td>
</tr>
<tr>
<td></td>
<td>• &gt; = non-active route</td>
</tr>
<tr>
<td></td>
<td>• + = summary routes</td>
</tr>
<tr>
<td>Destination</td>
<td>Identifies the route’s destination IPv6 address.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Identifies whether the route is directly connected and on which interface the route is configured.</td>
</tr>
<tr>
<td>Dist/Metric</td>
<td>Identifies if the route has a specified distance or metric.</td>
</tr>
<tr>
<td>Last Change</td>
<td>Identifies when the route was last changed or configured.</td>
</tr>
</tbody>
</table>
trust ipv6-diffserv

C E S

Allows the dynamic classification of IPv6 DSCP.

Syntax

trust ipv6-diffserv

To remove the definition, use the no trust ipv6-diffserv command.

Defaults

This command has no default behavior or values.

Command Modes

CONFIGURATION-POLICY-MAP-IN

Command History

- Version 8.4.2.1 Introduced on C-Series and S-Series
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

When trust IPv6 diffserv is configured, matched bytes/packets counters are not incremented in the show qos statistics command.

Trust diffserv (IPv4) can co-exist with trust ipv6-diffserv in an Input Policy Map. Dynamic classification happens based on the mapping detailed in the following table.

Table 26-2. IPv6 -Diffserv Mapping

<table>
<thead>
<tr>
<th>IPv6 Service Class Field</th>
<th>Queue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>111XXXXX</td>
<td>7</td>
</tr>
<tr>
<td>110XXXXX</td>
<td>6</td>
</tr>
<tr>
<td>101XXXXX</td>
<td>5</td>
</tr>
<tr>
<td>100XXXXX</td>
<td>4</td>
</tr>
<tr>
<td>011XXXXX</td>
<td>3</td>
</tr>
<tr>
<td>010XXXXX</td>
<td>2</td>
</tr>
<tr>
<td>001XXXXX</td>
<td>1</td>
</tr>
<tr>
<td>000XXXXX</td>
<td>0</td>
</tr>
</tbody>
</table>
IPv6 Border Gateway Protocol (IPv6 BGP)

Overview

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on platforms: 

This chapter includes the following commands:

- IPv6 BGP Commands
- IPv6 MBGP Commands

IPv6 BGP Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

The following commands allow you to configure and enable BGP:

- aggregate-address
- bgp always-compare-med
- bgp bestpath as-path ignore
- bgp bestpath med confed
- bgp bestpath med missing-as-best
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp dampening
- bgp default local-preference
- bgp enforce-first-as
- bgp fast-external-fallover
- bgp four-octet-as-support
- bgp graceful-restart
- bgp log-neighbor-changes
- bgp non-deterministic-med
- bgp recursive-bgp-next-hop
- bgp regex-eval-optz-disable
- bgp router-id
- bgp soft-reconfig-backup
- capture bgp-pdu neighbor (ipv6)
- capture bgp-pdu max-buffer-size
- clear ip bgp as-number
- clear ip bgp ipv6-address
- clear ip bgp peer-group
- clear ip bgp ipv6 dampening
- clear ip bgp ipv6 flap-statistics
- clear ip bgp ipv6 unicast soft
- debug ip bgp
- debug ip bgp events
- debug ip bgp ipv6 dampening
- debug ip bgp ipv6 unicast soft-reconfiguration
- debug ip bgp keepalives
- debug ip bgp notifications
- debug ip bgp updates
- default-metric
- description
- distance bgp
- maximum-paths
- neighbor activate
- neighbor advertisement-interval
- neighbor allowas-in
- neighbor default-originate
- neighbor description
- neighbor distribute-list
- neighbor ebgp-multihop
- neighbor fall-over
- neighbor filter-list
- neighbor maximum-prefix
- neighbor X:X:X::X password
- neighbor next-hop-self
- neighbor peer-group (assigning peers)
- neighbor peer-group (creating group)
- neighbor peer-group passive
- neighbor remote-as
- neighbor remove-private-as
- neighbor route-map
- neighbor route-reflector-client
- neighbor send-community
- neighbor shutdown
- neighbor soft-reconfiguration inbound
- neighbor subnet
- neighbor timers
address-family

Enable the IPv4 multicast or the IPv6 address family.

Syntax

```
address-family [ipv4 multicast| ipv6 unicast]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 multicast</td>
<td>Enter BGPv4 multicast mode.</td>
</tr>
<tr>
<td>ipv6 unicast</td>
<td>Enter BGPv6 mode.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

ROUTER BGP
aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

**Syntax**

```
aggregate-address ipv6-address prefix-length [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]
```

**Parameters**

- `ipv6-address prefix-length`: Enter the IPv6 address in the `X:X:X:X::X` format followed by the prefix length in the `/x` format.
  - Range: `/0` to `/128`
  - The `::` notation specifies successive hexadecimal fields of zeros

- `advertise-map map-name`: (OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.

- `as-set`: (OPTIONAL) Enter the keyword `as-set` to generate path attribute information and include it in the aggregate. `AS_SET` includes `AS_PATH` and community information from the routes included in the aggregated route.

- `attribute-map map-name`: (OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding `AS_PATH` and `NEXT_HOP` attributes.

- `summary-only`: (OPTIONAL) Enter the keyword `summary-only` to advertise only the aggregate address. Specific routes will not be advertised.

- `suppress-map map-name`: (OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION-ROUTER-BGPV6-ADDRESS FAMILY

**Usage Information**

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate, if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the `AS_PATH`. 
In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected via the `network` command, that route will still appear in the routing table if the summary-only parameter is configured in the `aggregate-address` command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

In the `show ip bgp ipv6 unicast` command, aggregates contain an ‘a’ in the first column and routes suppressed by the aggregate contain an ‘s’ in the first column.

### `bgp always-compare-med`

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

**Syntax**

```
bgp always-compare-med
```

To disable comparison of MED, enter `no bgp always-compare-med`.

**Defaults**

Disabled (that is, the software only compares MEDs from neighbors within the same AS).

**Command Modes**

`ROUTER BGP`

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Usage Information**

Any update without a MED attribute is the least preferred route.

If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

### `bgp bestpath as-path ignore`

Ignore the AS PATH in BGP best path calculations.

**Syntax**

```
bgp bestpath as-path ignore
```

To return to the default, enter `no bgp bestpath as-path ignore`.

**Defaults**

Disabled (that is, the software considers the AS_PATH when choosing a route as best).

**Command Modes**

`ROUTER BGP`

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
</tbody>
</table>
bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

Syntax

```
bgp bestpath med confed
```

To disable MED comparison on BGP confederation paths, enter `no bgp bestpath med confed`.

Defaults

Disabled.

Command Modes

ROUTER BGP

Usage Information

The software compares the MEDs only if the path contains no external autonomous system numbers.

If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

Syntax

```
bgp bestpath med missing-as-best
```

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Usage Information

The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.
bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

Syntax

```
bgp client-to-client reflection
```

To disable client-to-client reflection, enter `no bgp client-to-client reflection`.

Defaults

Enabled when a route reflector is configured.

Command Modes

- `ROUTER BGP`

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

Usage Information

Route reflection to clients is not necessary if all client routers are fully meshed.

Related Commands

- `bgp cluster-id` Assign ID to a BGP cluster with two or more route reflectors.
- `neighbor route-reflector-client` Configure a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

Syntax

```
bgp cluster-id {ip-address | number}
```

To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

- `ip-address` Enter an IP address as the route reflector cluster ID.
- `number` Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults

Not configured.

Command Modes

- `ROUTER BGP`

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

Usage Information

When a BGP cluster contains only one route reflector, the cluster ID is the route reflector’s router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it will be displayed as an integer.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp client-to-client reflection</td>
<td>Enable route reflection between route reflector and clients.</td>
</tr>
<tr>
<td>neighbor route-reflector-client</td>
<td>Configure a route reflector and clients.</td>
</tr>
<tr>
<td>show ip bgp ipv6 unicast cluster-list</td>
<td>View paths with a cluster ID.</td>
</tr>
</tbody>
</table>

bgp confederation identifier

Configure an identifier for a BGP confederation.

Syntax

```
bgp confederation identifier as-number
```

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

- `as-number`: Enter the AS number.
  - Range: 1 to 65535

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

- Version 8.4.2.1: Introduced on C-Series and S4810.
- Version 8.2.1.0: Introduced on E-Series ExaScale
- Version 7.4.1.0: Introduced on E-Series TeraScale

Usage Information

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

FTOS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

bgp confederation peers

Specify the Autonomous Systems (ASs) that belong to the BGP confederation.

Syntax

```
bgp confederation peers as-number [...as-number]
```

To enter no bgp confederation peer.

Parameters

- `as-number`: Enter the AS number.
  - Range: 1 to 65535
- `...as-number` (OPTIONAL): Enter up to 16 confederation numbers.
  - Range: 1 to 65535

Defaults

Not configured.
bpg dampening

Enable BGP route dampening and configure the dampening parameters.

Syntax

```plaintext
bpg dampening [half-life reuse suppress max-suppress-time] [route-map map-name]
```

To disable route dampening, use the `no bpg dampening [half-life reuse suppress max-suppress-time] [route-map map-name]` command.

Parameters

- **half-life**: (OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires.
  - Range: 1 to 45.
  - Default: 15 minutes

- **reuse**: (OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route’s Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed).
  - Range: 1 to 20000.
  - Default: 750

- **suppress**: (OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed).
  - Range: 1 to 20000.
  - Default: 2000

- **max-suppress-time**: (OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value.
  - Range: 1 to 255.
  - Default: 60 minutes

- **route-map map-name**: (OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map.
  - Only match commands in the configured route map are supported.

Defaults

- Disabled.
b GP default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

Syntax

```
bgp default local-preference value
```

Parameters

```
value
```

Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred.

Range: 0 to 4294967295

Default: 100

Defaults: 100

Command Modes: ROUTER BGP

Usage Information

The `bgp default local-preference` command setting is applied by all routers within the AS.

b GP enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

Syntax

```
bgp enforce-first-as
```

To turn off the default, use the `no bgp enforce-first-as` command.

Defaults: Enabled
IPv6 Border Gateway Protocol (IPv6 BGP) | 751

**Command Modes**

**ROUTER BGP**

**Usage Information**

This is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. Use the `show ip bgp ipv6 unicast neighbors` command to view the “failed enforce-first-as check counter.

If enforce-first-as is disabled, it can be viewed via the `show ip protocols` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip bgp ipv6 unicast neighbors</code></td>
<td>Display IPv6 routing information exchanged by BGP neighbors.</td>
</tr>
<tr>
<td><code>show ip protocols</code></td>
<td>View Information on routing protocols.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale.</td>
</tr>
</tbody>
</table>

**bgp fast-external-fallover**

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

**Syntax**

`bgp fast-external-fallover`

To disable fast external fallover, enter `no bgp fast-external-fallover`.

**Defaults**

Enabled

**Command Modes**

**ROUTER BGP**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale.</td>
</tr>
</tbody>
</table>

**Usage Information**

The `bgp fast-external-fallover` command appears in the `show config` command output.

**bgp four-octet-as-support**

Enable 4-byte support for the BGP process

**Syntax**

`bgp four-octet-as-support`

To disable fast external fallover, enter `no bgp four-octet-as-support`.

**Defaults**

Disabled (supports 2-Byte format)

**Command Modes**

**ROUTER BGP**
Routers supporting 4-Byte ASNs advertise that function in the OPEN message. The behavior of a 4-Byte router will be slightly different depending on whether it is speaking to a 2-Byte router or a 4-Byte router.

When creating Confederations, all the routers in the Confederation must be 4 or 2 byte identified routers. You cannot mix them.

Where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295. Both formats are accepted, and the advertisements will reflect the entered format.

For more information about using the 2 or 4-Byte format, refer to the Dell Networking OS Configuration Guide.

```
bgp graceful-restart
```

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

**Syntax**
```
bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]
```

To return to the default, enter the `no bgp graceful-restart` command.

**Parameters**
- `neighbor ip-address | peer-group-name` Enter the keyword `neighbor` followed by one of the options listed below:
  - `ip-address` of the neighbor in IP address format of the neighbor
  - `peer-group-name` of the neighbor peer group.
- `restart-time seconds` Enter the keyword `restart-time` followed by the maximum number of seconds needed to restart and bring up all peers.
  Range: 1 to 3600 seconds
  Default: 120 seconds
- `stale-path-time seconds` Enter the keyword `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer’s stale paths.
  Default: 360 seconds.
- `role receiver-only` Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

**Defaults**
As above

**Command Modes**
ROUTER BGP
Usage Information
This feature is advertised to BGP neighbors through a capability advertisement. In receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

bgp log-neighbor-changes
Enable logging of BGP neighbor resets.

Syntax
bgp log-neighbor-changes

To disable logging, enter no bgp log-neighbor-changes.

Defaults
Enabled

Command Modes
ROUTER BGP

Usage Information
The bgp log-neighbor-changes command appears in the show config command output.

Related Commands
show config  View the current configuration

bgp non-deterministic-med
Compare MEDs of paths from different Autonomous Systems.

Syntax
bgp non-deterministic-med

To return to the default, enter no bgp non-deterministic-med.

Defaults
Disabled (that is, paths/routes for the same destination but from different ASs will not have their MEDs compared).

Command Modes
ROUTER BGP

Usage Information
In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to FTOS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors since MED may or may not get compared between adjacent paths. In deterministic mode (no bgp non-deterministic-med), FTOS compares MED between adjacent paths within an AS group since all paths in the AS group are from the same AS.
When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter `capture bgp-pdu max-buffer-size` command to clear existing paths.

### bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

**Syntax**

```
bgp recursive-bgp-next-hop
```

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

**Defaults**

Enabled

**Command Modes**

ROUTER BGP

**Usage Information**

This command is a knob to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route’s protocol source and is checked if the route is learned from BGP or not.

The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture bgp-pdu max-buffer-size</code></td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

- **Version 8.4.2.1**: Introduced on C-Series and S4810.
- **Version 8.2.1.0**: Introduced on E-Series ExaScale
- **Version 7.4.1.0**: Introduced on E-Series TeraScale

### bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

**Syntax**

```
bgp regex-eval-optz-disable
```

To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

**Defaults**

Enabled by default

**Command Modes**

ROUTER BGP (conf-router_bgp)

**Usage Information**

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.
BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the show bgp commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.

**Related Commands**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip protocols</strong></td>
<td>View information on all routing protocols enabled and active on the E-Series.</td>
</tr>
<tr>
<td>Version 8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

### bgp router-id

Assign a user-given ID to a BGP router.

**Syntax**

```
bgp router-id ip-address
```

To delete a user-assigned IP address, enter `no bgp router-id`.

**Parameters**

- `ip-address`: Enter an IP address in dotted decimal format to reset only that BGP neighbor.

**Defaults**

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

**Command Modes**

- ROUTER BGP

**Command History**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Usage Information**

Peering sessions are reset when you change the router ID of a BGP router.

### bgp soft-reconfig-backup

Use this command only when route-refresh is not negotiated between peers to avoid having a peer resend BGP updates.

**Syntax**

```
bgp soft-reconfig-backup
```

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

**Defaults**

Off
When soft-reconfiguration is enabled for a neighbor and the `clear ip bgp soft in` is executed, the update database stored in the router is replayed and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (upon execution of `clear ip bgp soft in`), then BGP sends a route-refresh request to the neighbor and receives all of the peer’s updates.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ip bgp ipv6 unicast soft in</code></td>
<td>Activate inbound policies for IPv6 routes without resetting the BGP TCP session.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv4 multicast and IPv6 unicast address families</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S4810</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

---

**capture bgp-pdu neighbor (ipv6)**

Enable capture of an IPv6 BGP neighbor packet.

**Syntax**

```plaintext
capture bgp-pdu neighbor ipv6-address direction {both | rx | tx}
```

To disable capture of the IPv6 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv6-address` command.

**Parameters**

- **ipv6-address**
  
Enter the IPv6 address of the target BGP neighbor.

- **direction**
  
  Enter the keyword `direction` and a direction— either `rx` for inbound, `tx` for outbound, or `both`.

**Defaults**

Not configured.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Related Commands**

- `capture bgp-pdu max-buffer-size` Enable route reflection between route reflector and clients.
- `show capture bgp-pdu neighbor` Configure a route reflector and clients.
- `capture bgp-pdu neighbor` Enable capture of an IPv4 BGP neighbor packet.
capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Syntax

capture bgp-pdu max-buffer-size 100-102400000

Parameters

100-102400000 Enter a size for the capture buffer.

Defaults

40960000 bytes

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale

Related Commands

capture bgp-pdu neighbor (ipv6) Enable capture of an IPv6 BGP neighbor packet.
show capture bgp-pdu neighbor Configure a route reflector and clients.

clear ip bgp * (asterisk)

Reset all BGP sessions in the specified category on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax

clear ip bgp * [ipv4 multicast soft [in | out] | ipv6 unicast soft [in | out] | soft [in | out]]

Parameters

* Enter an asterisk (*) to reset all BGP sessions.
ipv4 multicast soft [in | out] (OPTIONAL) This keyword sequence sets options within the a specified IPv4 address family.
ipv6 unicast soft [in | out] (OPTIONAL) This keyword sequence sets options within the a specified IPv6 address family.
soft (OPTIONAL) Enter the keyword soft to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
Note: If you enter clear ip bgp ip6-address soft, both inbound and outbound policies are reset.
in (OPTIONAL) Enter the keyword in to activate only inbound policies.
out (OPTIONAL) Enter the keyword out to activate only outbound policies.

Command Modes

EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale
clear ip bgp as-number

Reset BGP sessions on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

**Syntax**

```
clear ip bgp as-number [flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}}] soft [in | out]
```

**Parameters**

- **as-number**: Enter an autonomous system (AS) number to reset neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS.
  - Range: 1 to 65535
- **flap-statistics**: (OPTIONAL) Enter the keyword `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that AS.
- **ipv4**: (OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
- **ipv6**: (OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
- **unicast**: (OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.
- **multicast**: (OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family.
  - Multicast is supported on IPv4 only
- **soft**: (OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
  - **Note**: If you enter `clear ip bgp ipv6-address soft`, both inbound and outbound policies are reset.
- **in**: (OPTIONAL) Enter the keyword `in` to activate only inbound policies.
- **out**: (OPTIONAL) Enter the keyword `out` to activate only outbound policies.

**Command Modes**

EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

---

clear ip bgp ipv6-address

Reset BGP sessions specific to an IPv6 address on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

**Syntax**

```
clear ip bgp ipv6-address [flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}}] soft [in | out]
```

**Parameters**

- **ipv6-address**: Enter a specific IPv6 address.
- **flap-statistics**: (OPTIONAL) Enter the keyword `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that AS.
- **ipv4**: (OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
- **ipv6**: (OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
- **unicast**: (OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.
- **multicast**: (OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family.
  - Multicast is supported on IPv4 only
- **soft**: (OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
  - **Note**: If you enter `clear ip bgp ipv6-address soft`, both inbound and outbound policies are reset.
- **in**: (OPTIONAL) Enter the keyword `in` to activate only inbound policies.
- **out**: (OPTIONAL) Enter the keyword `out` to activate only outbound policies.
clear ip bgp peer-group

Reset a peer-group’s BGP sessions.

Syntax clear ip bgp peer-group peer-group-name

Parameters peer-group-name Enter the peer group name to reset the BGP sessions within that peer group.

Command Modes EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version 8.4.2.1</th>
<th>Introduced on C-Series and S4810.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

clear ip bgp ipv6 dampening

Clear information on route dampening and return suppressed route to active state.

Syntax clear ip bgp ipv6 unicast dampening [ipv6-address]

Parameters ipv6-address Enter an IPv6 address to reset neighbors belonging to that IP. Used without a qualifier, the keyword resets all neighbors belonging to that IP.

flap-statistics (OPTIONAL) Enter the keyword flap-statistics to clear all flap statistics belonging to that AS or a specified address family within that IP.

ipv4 (OPTIONAL) Enter the keyword ipv4 to select options for that address family.

ipv6 (OPTIONAL) Enter the keyword ipv6 to select options for that address family.

unicast (OPTIONAL) Enter the keyword unicast to select the unicast option within the selected address family.

multicast (OPTIONAL) Enter the keyword multicast to select the multicast option within the selected address family. Multicast is supported on IPv4 only.

soft (OPTIONAL) Enter the keyword soft to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. Note: If you enter clear ip bgp ipv6-address soft, both inbound and outbound policies are reset.

in (OPTIONAL) Enter the keyword in to activate only inbound policies.

out (OPTIONAL) Enter the keyword out to activate only outbound policies.

Parameters

ipv6-address

Command Modes EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version 8.4.2.1</th>
<th>Introduced on C-Series and S4810.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>
**clear ip bgp ipv6 flap-statistics**

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

**Syntax**
```
clear ip bgp ipv6 unicast flap-statistics [ipv6-address | filter-list as-path-name | regexp regular-expression]
```

**Parameters**
- **ipv6-address** (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format.
  - Range: /0 to /128
  - The :: notation specifies successive hexadecimal fields of zeros
- **filter-list as-path-name** (OPTIONAL) Enter the keyword filter-list followed by the name of a configured AS-PATH list.
- **regexp regular-expression** (OPTIONAL) Enter the keyword regexp followed by regular expressions. Use one or a combination of the following:
  - . (period) matches on any single character, including white space
  - * (asterisk) matches on sequences in a pattern (zero or more sequences)
  - + (plus sign) matches on sequences in a pattern (one or more sequences)
  - ? (question mark) matches sequences in a pattern (0 or 1 sequences)
  - [ ] (brackets) matches a range of single-character patterns.
  - ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
  - $ (dollar sign) matches the end of the output string.

**Command Modes**
- EXEC Privilege

**Command History**
- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

**Usage Information**
After you enter this command, the software deletes history routes and returns suppressed routes to active state.
Usage Information

If you enter `clear ip bgp ipv6 flap-statistics` without any parameters, all statistics are cleared.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip bgp ipv6 unicast flap-statistics</code></td>
<td>View BGP flap statistics.</td>
</tr>
</tbody>
</table>

**clear ip bgp ipv6 unicast soft**

Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

**Syntax**

```
clear ip bgp { * | as-number | ipv4-neighbor-addr | ipv6-neighbor-addr | peer-group name | ipv6 unicast soft [ in | out ] }
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>*</code></td>
<td>Clear and reapply policies for all BGP sessions.</td>
</tr>
<tr>
<td><code>as-number</code></td>
<td>Clear and reapply policies for all neighbors belonging to the AS.</td>
</tr>
<tr>
<td>`ipv4-neighbor-addr</td>
<td>ipv6-neighbor-addr`</td>
</tr>
<tr>
<td><code>peer-group name</code></td>
<td>Clear and reapply policies for all BGP routers in the specified peer group.</td>
</tr>
<tr>
<td><code>ipv6 unicast</code></td>
<td>Clear and reapply policies for all IPv6 unicast routes.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Reapply only inbound policies. Note: If you enter <code>soft</code>, without an <code>in</code> or <code>out</code> option, both inbound and outbound policies are reset.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Reapply only outbound policies. Note: If you enter <code>soft</code>, without an <code>in</code> or <code>out</code> option, both inbound and outbound policies are reset.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv4 multicast and IPv6 unicast routes</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support on S4810</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced support on C-Series</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
</tbody>
</table>

**debug ip bgp**

Allows you to view all information on BGP, including BGP events, keepalives, notifications, and updates.

**Syntax**

```
debug ip bgp [ ipv6-address | peer-group peer-group-name ] [ in | out ]
```

To disable all BGP debugging, enter `no debug ip bgp`. 
Parameters

<table>
<thead>
<tr>
<th>ipv6-address</th>
<th>(OPTIONAL) Enter the IPv6 address in the \text{x:x:x:x} format followed by the prefix length in the /x format. Range: /0 to /128 The :: notation specifies successive hexadecimal fields of zeros.</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group peer-group-name</td>
<td>Enter the keyword peer-group followed by the name of the peer group.</td>
</tr>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword in to view only information on inbound BGP routes.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword out to view only information on outbound BGP routes.</td>
</tr>
</tbody>
</table>

Command Modes

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

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

Usage Information

To view information on both incoming and outgoing routes, do not include the in and out parameters in the debugging command. The in and out parameters cancel each other; for example, if you enter `debug ip bgp in` and then enter `debug ip bgp out`, you will not see information on the incoming routes.

Entering a no debug ip bgp command removes all configured debug commands for BGP.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip bgp events</td>
<td>View information about BGP events.</td>
</tr>
<tr>
<td>debug ip bgp keepalives</td>
<td>View information about BGP keepalives.</td>
</tr>
<tr>
<td>debug ip bgp notifications</td>
<td>View information about BGP notifications.</td>
</tr>
<tr>
<td>debug ip bgp updates</td>
<td>View information about BGP updates.</td>
</tr>
</tbody>
</table>

**debug ip bgp events**

Allows you to view information on local BGP state changes and other BGP events.

**Syntax**

```
debug ip bgp [ipv6-address | peer-group peer-group-name] events [in | out]
```

To disable debugging, use the `no debug ip bgp ipv6-address | peer-group peer-group-name] events [in | out]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>(OPTIONAL) Enter the IPv6 address in the \text{x:x:x:x} format followed by the prefix length in the /x format. Range: /0 to /128 The :: notation specifies successive hexadecimal fields of zeros.</td>
</tr>
<tr>
<td>peer-group peer-group-name</td>
<td>(OPTIONAL) Enter the keyword peer-group followed by the name of the peer group.</td>
</tr>
</tbody>
</table>
debug ip bgp ipv6 dampening

View information on IPv6 routes being dampened.

Syntax

```
debug ip bgp ipv6 unicast dampening [in | out]
```

To disable debugging, enter `no debug ip bgp ipv6 unicast dampening`.

Parameters

```
in  (OPTIONAL) Enter the keyword `in` to view only events on inbound BGP messages.
out (OPTIONAL) Enter the keyword `out` to view only events on outbound BGP messages.
```

Command Modes

EXEC Privilege

Command History

```
Version 8.4.2.1  Introduced on C-Series and S4810.
Version 8.2.1.0  Introduced on E-Series ExaScale
Version 7.4.1.0  Introduced on E-Series TeraScale
```

Usage Information

Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

Related Commands

```
show ip bgp ipv6 unicast dampened-paths
```

View BGP dampened routes.

dependent on ip bgp ipv6 unicast soft-reconfiguration

Enable soft-reconfiguration debugging for IPv6 unicast routes.

Syntax

```
dependent on ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration
```

To disable debugging, use the `no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration` command.
Parameters

ipv4-address | ipv6-address

peer-group-name

ipv6 unicast

Defaults

Disabled

Command Modes

EXEC Privilege

Usage Information

This command turns on BGP soft-reconfiguration inbound debugging for IPv6 unicast routes. If no neighbor is specified, debug is turned on for all neighbors.

Command History

Version 8.4.1.0 Added support for IPv4 multicast and IPv6 unicast routes
Version 7.8.1.0 Introduced support on S4810
Version 7.7.1.0 Introduced support on C-Series
Version 7.2.1.0 Introduced on the E-Series TeraScale

debug ip bgp keepalives

Allows you to view information about BGP keepalive messages.

Syntax

dbgip bgp [ipv6-address | peer-group peer-group-name] keepalives [in | out]

To disable debugging, use the no debug ip bgp [ipv6-address | peer-group peer-group-name] keepalives [in | out] command.

Parameters

ipv6-address

(peer-group peer-group-name)

in

out

Command Modes

EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale
debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name] notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

Parameters

- `ipv6-address` (OPTIONAL) Enter the IPv6 address in the `x:x:x:x::x` format followed by the prefix length in the `/x` format.
  
  Range: `/0` to `/128`

  The `::` notation specifies successive hexadecimal fields of zeros.

- `peer-group peer-group-name` (OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.

- `in` (OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.

- `out` (OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors.

Command Modes

- EXEC Privilege

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

data:debug ip bgp updates

Allows you to view information about BGP updates.

Syntax

```
debug ip bgp [ipv6-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]]
   updates [in | out | prefix-list prefix-list-name]
```

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]] updates [in | out]` command.
The default-metric command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

- bgp always-compare-med
- redistribute

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale
description

Enter a description of the BGP routing protocol

Syntax

```
description {description}
```

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

Parameters

- `description` Enter a description to identify the BGP protocol (80 characters maximum).

Defaults

No default behavior or values

Command Modes

ROUTER BGP

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

Related Commands

- `router bgp` Enter ROUTER mode on the switch.

distance bgp

Configure three administrative distances for routes.

Syntax

```
distance bgp external-distance internal-distance local-distance
```

To return to default values, enter `no distance bgp`.

Parameters

- `external-distance` Enter a number to assign to routes learned from a neighbor external to the AS.
  Range: 1 to 255.
  Default: 20

- `internal-distance` Enter a number to assign to routes learned from a router within the AS.
  Range: 1 to 255.
  Default: 200

- `local-distance` Enter a number to assign to routes learned from networks listed in the `network` command.
  Range: 1 to 255.
  Default: 200

Defaults

- `external-distance` = 20; `internal-distance` = 200; `local-distance` = 200.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale
Usage Information

Caution: Dell Force10 recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax

```
maximum-paths {ebgp | ibgp} number
```

To return to the default values, enter `no maximum-paths`.

Parameters

<table>
<thead>
<tr>
<th>ebgp</th>
<th>Enter the keyword <code>ebgp</code> to enable multipath support for External BGP routes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibgp</td>
<td>Enter the keyword <code>ibgp</code> to enable multipath support for Internal BGP routes.</td>
</tr>
</tbody>
</table>

| number | Enter a number as the maximum number of parallel paths. Range: 1 to 16  
        | Default: 1 |

Defaults

```
1
```

Command Modes

```
ROUTER BGPV6-ADDRESS FAMILY
```

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
<td></td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale.</td>
<td></td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale.</td>
<td></td>
</tr>
</tbody>
</table>

Usage Information

If you enable this command, use the `capture bgp-pdu max-buffer-size` command to recompute the best path.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Syntax

```
neighbor {ipv6-address | peer-group-name} activate
```

To disable, use the `no neighbor {ipv6-address | peer-group-name} activate` command.

Parameters

| ipv6-address | Enter the IPv6 address in the X:XX:XX::X format.  
The :: notation specifies successive hexadecimal fields of zeros. |

Default: 1
IPv6 Border Gateway Protocol (IPv6 BGP)

The IPv6 Border Gateway Protocol (IPv6 BGP) is a routing protocol for IPv6 networks. It is used to exchange routing information between autonomous systems. The protocol is similar to IPv4 BGP, but with modifications to support the IPv6 address format and other IPv6-specific features.

### Defaults
By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using the `activate` command, the neighbor/peer group is enabled for AFI/SAFI.

### Command Modes
- **ROUTER BGPV6-ADDRESS FAMILY**

### History
- **Version 8.4.2.1** Introduced on C-Series and S4810.
- **Version 8.2.1.0** Introduced on E-Series ExaScale
- **Version 7.4.1.0** Introduced on E-Series TeraScale

### Usage
- **neighbor advertisement-interval**

  Set the advertisement interval between BGP neighbors or within a BGP peer group.

  **Syntax**

  ```
  neighbor {ipv6-address | peer-group-name} advertisement-interval seconds
  ```

  **Parameters**

  - **ipv6-address**
    - Enter the IPv6 address in the `X::X::X::X` format.
    - The `::` notation specifies successive hexadecimal fields of zeros.
  - **peer-group-name**
    - Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
  - **seconds**
    - Enter a number as the time interval, in seconds, between BGP advertisements.
    - Range: 0 to 600 seconds.
    - Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

  **Defaults**
  - `seconds` = 5 seconds (internal peers); `seconds` = 30 seconds (external peers)

  **Command Modes**
  - **ROUTER BGPV6-ADDRESS FAMILY**

  **History**
  - **Version 8.4.2.1** Introduced on C-Series and S4810.
  - **Version 8.2.1.0** Introduced on E-Series ExaScale
  - **Version 7.4.1.0** Introduced on E-Series TeraScale
neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

Syntax

neighbor \{ip-address | peer-group-name\} allowas-in number

To return to the default value, use the no neighbor \{ip-address | peer-group-name\} allowas-in command.

Parameters

- **ip-address**: Enter the IPv6 address in the `x:x:x:x::x` format.
  - The `::` notation specifies successive hexadecimal fields of zeros.
- **peer-group-name**: Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- **number**: Enter a number of times to allow this neighbor ID to use the AS path.
  - Range: 1 to 10.

Defaults

Not configured.

Command Modes

ROUTER BGP

Related Commands

- **bgp four-octet-as-support**: Enable 4-Byte support for the BGP process.

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

Syntax

neighbor \{ipv6-address | peer-group-name\} default-originate \[route-map map-name\]

To remove a default route, use the no neighbor \{ipv6-address | peer-group-name\} default-originate \[route-map map-name\] command.

Parameters

- **ipv6-address**: Enter the IPv6 address in the `x:x:x:x::x` format.
  - The `::` notation specifies successive hexadecimal fields of zeros.
- **peer-group-name**: Enter the name of the peer group to set the default route of all routers in that peer group.
- **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 BGPV6-ADDRESS FAMILY
If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

**neighbor description**

Assign a character string describing the neighbor or group of neighbors (peer group).

**Syntax**

```plaintext
neighbor {ipv6-address | peer-group-name} description text
```

To delete a description, use the `no neighbor {ipv6-address | peer-group-name} description text` command.

**Parameters**

- `ipv6-address`
  - Enter the IPv6 address in the `x:x:x:x::x` format.
  - The `::` notation specifies successive hexadecimal fields of zeros.

- `peer-group-name`
  - Enter the name of the peer group.

- `text`
  - Enter a continuous text string up to 80 characters.

**Defaults**

Not configured.

**Command Modes**

- `ROUTER BGP`

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**neighbor distribute-list**

Distribute BGP information via an established prefix list.

**Syntax**

```plaintext
neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}
```

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

**Parameters**

- `ipv6-address`
  - Enter the IPv6 address in the `x:x:x:x::x` format.
  - The `::` notation specifies successive hexadecimal fields of zeros.

- `peer-group-name`
  - Enter the name of the peer group.

- `prefix-list-name`
  - Enter the name of an established prefix list.
  - If the prefix list is not configured, the default is permit (to allow all routes).
neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax

neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]

Parameters

ipv6-address

Enter the IPv6 address in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name

Enter the name of the peer group.

ttl

(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. Range: 1 to 255. Default: 255

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

To prevent loops, the neighbor ebgp-multihop command will not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.
neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

Syntax

neighbor {ipv6-address | peer-group-name} fall-over

To disable, use the no neighbor {ipv6-address | peer-group-name} fall-over command.

Parameters

- ipv6-address: Enter the IPv6 address in the X:XX:XXX::X format. The :: notation specifies successive hexadecimal fields of zeros.
- peer-group-name: Enter the name of the peer group.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

When fall-over is enabled, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (i.e., no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands

show ip bgp ipv6 unicast neighbors
Display IPv6 routing information exchanged by BGP neighbors.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

Syntax

neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out}

To delete a BGP filter, use the no neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out} command.

Parameters

- ipv6-address: Enter the IPv6 address in the X:XX:XX::X format. The :: notation specifies successive hexadecimal fields of zeros.
- peer-group-name: Enter the name of the peer group to apply the filter to all routers in the peer group.
- as-path-name: Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is permit (to allow routes). (16 characters maximum)
- in: Enter the keyword in to filter inbound BGP routes.
- out: Enter the keyword out to filter outbound BGP routes.

Defaults

Not configured.
neighbor maximum-prefix

Control the number of network prefixes received.

Syntax

```
neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]
```

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]` command.

Parameters

- `ipv6-address`: Enter the IPv6 address in the `X::X::X::X` format. The `::` notation specifies successive hexadecimal fields of zeros.
- `peer-group-name`: Enter the name of the peer group.
- `maximum`: Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
- `threshold` *(OPTIONAL)*: Enter a number to be used as a percentage of the `maximum` value. When the number of prefixes reaches this percentage of the `maximum` value, the E-Series software sends a message. Range: 1 to 100 percent. Default: 75
- `warning-only` *(OPTIONAL)*: Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults

`threshold = 75`

Usage Information

If the `neighbor maximum-prefix` is configured and the neighbor receives more prefixes than allowed by the `neighbor maximum-prefix` command configuration, the neighbor goes down and the `show ip bgp ipv6 unicast summary` command displays `(prfxd)` in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the `capture bgp-pdu max-buffer-size` command for the neighbor or the peer group to which the neighbor belongs or you enter `neighbor shutdown` and `neighbor no shutdown` commands.
neighbor X:X::X password

Enable TCP MD5 Authentication for an IPv6 BGP peer session.

Syntax neighbor x:x::x password {<encrypt-pass> | <clear-pass>}

To return to the default setting, use the no neighbor x:x::x password command.

Parameters

- encrypt-pass Enter the encrypted password.
- clear-pass Enter the clear text password.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series TeraScale

Usage Information

The TCP session is authentication and hence prevents the data from being compromised.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

Syntax neighbor {ipv6-address | peer-group-name} next-hop-self

To return to the default setting, use the no neighbor {ipv6-address | peer-group-name} next-hop-self command.

Parameters

- ipv6-address Enter the IPv6 address in the X::X::X::X format.
  - The :: notation specifies successive hexadecimal fields of zeros.
- peer-group-name (OPTIONAL) Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale
If the `set ipv6 next-hop` command in the ROUTE-MAP mode is configured, its configuration takes precedence over the `neighbor next-hop-self` command.

### neighbor peer-group (assigning peers)

Allows you to assign one peer to an existing peer group.

**Syntax**

```plaintext
neighbor ipv6-address peer-group peer-group-name
```

To delete a peer from a peer group, use the `no neighbor ipv6-address peer-group peer-group-name` command.

**Parameters**

- `ipv6-address` Enter the IPv6 address in the `X::X::X::X` format. The `::` notation specifies successive hexadecimal fields of zeros.
- `peer-group peer-group-name` Enter the keyword `peer-group` followed by the name of a configured peer group. (maximum 16 characters)

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Command History**

- **Version 8.4.2.1** Introduced on C-Series and S4810.
- **Version 8.2.1.0** Introduced on E-Series ExaScale
- **Version 7.4.1.0** Introduced on E-Series TeraScale

**Usage Information**

You can assign up to 64 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group’s configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval
- neighbor distribute-list out
- neighbor filter-list out
- neighbor next-hop-self
- neighbor route-map out
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor’s configuration is more specific than the peer group’s, and the neighbor’s configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

**Related Commands**

- `capture bgp-pdu max-buffer-size` Resets BGP sessions.
- `neighbor peer-group (creating group)` Create a peer group.
### neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

**Syntax**

```
neighbor peer-group-name peer-group
```

To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>Enter a text string up to 16 characters long as the name of the peer group.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

**Usage Information**

When a peer group is created, it is disabled (shut mode).

**Related Commands**

- `neighbor peer-group (assigning peers)` Assign routers to a peer group.
- `neighbor remote-as` Assign a indirectly connected AS to a neighbor or peer group.
- `neighbor shutdown` Disable a peer or peer group.

### neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but will respond to one.

**Syntax**

```
neighbor peer-group-name peer-group passive
```

To delete a passive peer-group, use the `no neighbor peer-group-name peer-group passive` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>Enter a text string up to 16 characters long as the name of the peer group.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

Syntax

```
neighbor {ipv6-address | peer-group-name} remote-as number
```

Parameters

- **ipv6-address**: Enter the IPv6 address in the X:XX:XX::X format.
  The :: notation specifies successive hexadecimal fields of zeros.

- **peer-group-name**: Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.

- **number**: Enter a number of the AS.
  Range: 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

- Version 8.4.2.1: Introduced on C-Series and S4810.
- Version 8.2.1.0: Introduced on E-Series ExaScale
- Version 7.4.1.0: Introduced on E-Series TeraScale

Usage Information

If the number parameter is the same as the AS number used in the router bgp command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (shutdown).

Related Commands

```
router bgp
```

Enter the ROUTER BGP mode and configure routes in an AS.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax

```
neighbor {ipv6-address | peer-group-name} remove-private-as
```

Related Commands

```
router bgp
```

Enter the ROUTER BGP mode and configure routes in an AS.
To return to the default, use the no neighbor {ipv6-address | peer-group-name} remove-private-as command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>Enter the IPv6 address in the X::X::X::X format. The :: notation specifies successive hexadecimal fields of zeros.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group to remove the private AS numbers.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled (that is, private AS number are not removed).

**Command Modes**

ROUTER BGPV6-ADDRESS FAMILY

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Usage Information**

Applies to EBGP neighbors only.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535.

**neighbor route-map**

C E S4810

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

**Syntax**

```
neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}
```

To remove the route map, use the no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out} command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>Enter the IPv6 address in the X::X::X::X format. The :: notation specifies successive hexadecimal fields of zeros.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group.</td>
</tr>
<tr>
<td>map-name</td>
<td>Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).</td>
</tr>
<tr>
<td>in</td>
<td>Enter the keyword in to filter inbound routes.</td>
</tr>
<tr>
<td>out</td>
<td>Enter the keyword out to filter outbound routes.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGPV6-ADDRESS FAMILY
When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

Syntax

```
neighbor {ipv6-address | peer-group-name} route-reflector-client
```

Parameters

- `ipv6-address`: Enter the IPv6 address in the `X::X::X::X` format. The `::` notation specifies successive hexadecimal fields of zeros.

- `peer-group-name`: Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

Syntax

```
neighbor {ipv6-address | peer-group-name} send-community
```

To disable sending a COMMUNITY attribute, use the `no neighbor {ipv6-address | peer-group-name} send-community` command.
neighbor shutdown

Disable a BGP neighbor or peer group.

Syntax

```
neighbor {ipv6-address | peer-group-name} shutdown
```

To enable a disabled neighbor or peer group, use the no `neighbor {ipv6-address | peer-group-name} shutdown` command.

Parameters

- `ipv6-address`: Enter the IPv6 address in the `x:x:x:x::x` format.
  The '::' notation specifies successive hexadecimal fields of zeros.

- `peer-group-name`: Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults

Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes

ROUTER BGP

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp ipv6 unicast summary` command to confirm its status.

Related Commands

- `show ip bgp ipv6 unicast summary`: Display the current BGP configuration.
- `show ip bgp ipv6 unicast neighbors`: Display IPv6 routing information exchanged by BGP neighbors.
neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv6 unicast routes.

Syntax

```
neighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound
```

Parameters

- `ipv4-address | ipv6-address`: Enter the IP address of the neighbor for which you want to start storing inbound routing updates.
- `peer-group-name`: Enter the name of the peer group for which you want to start storing inbound routing updates.

Defaults

Disabled

Command Modes

ROUTER BGPv6 ADDRESS FAMILY (conf-router_bgpv6_af)

Usage Information

This command enables soft-reconfiguration for the specified BGP neighbor. BGP will store all updates for inbound IPv6 unicast routes received by the neighbor but will not reset the peer-session.

Caution: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.

Related Commands

- `show ip bgp ipv6 unicast neighbors`: Display IPv6 routing information exchanged by BGP neighbors.

Command History

- Version 8.4.1.0: Added support for IPv4 multicast and IPv4 unicast address families
- Version 7.8.1.0: Introduced support on S4810
- Version 7.7.1.0: Introduced support on C-Series
- Version 7.4.1.0: Introduced

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic

Syntax

```
neighbor peer-group-name subnet subnet-number mask
```

To remove passive peering, use the `no neighbor peer-group-name subnet subnet-number mask` command.

Parameters

- `subnet-number`: Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group.
  To allow all addresses, enter 0:0/0.
- `mask`: Enter a prefix mask in /prefix-length format (/x).

Defaults

Not configured.

Command Modes

ROUTER BGP
**neighbor timers**

Set keepalive and hold time timers for a BGP neighbor or a peer group.

**Syntax**

```plaintext
neighbor {ipv6-address | peer-group-name} timers keepalive holdtime
```

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} timers` command.

**Parameters**

- `ipv6-address` Enter the IPv6 address in the `X:X::X::X` format. The `::` notation specifies successive hexadecimal fields of zeros.
- `peer-group-name` Enter the name of the peer group to set the timers for all routers within the peer group.
- `keepalive` Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers.
  - Range: 1 to 65535
  - Default: 60 seconds
- `holdtime` Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead.
  - Range: 3 to 65535
  - Default: 180 seconds

**Defaults**

`keepalive = 60` seconds; `holdtime = 180` seconds.

**Command Modes**

- ROUTER BGP

**Usage Information**

Timer values configured with the `neighbor timers` command override the timer values configured with the `timers bgp` command.

When two neighbors, configured with different `keepalive` and `holdtime` values, negotiate for new values, the resulting values will be as follows:

- the lower of the `holdtime` values is the new `holdtime` value, and
- whichever is the lower value; one-third of the new `holdtime` value, or the configured `keepalive` value is the new `keepalive` value.

---

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>
neighbor update-source

Enable the E-Series software to use Loopback interfaces for TCP connections for BGP sessions.

Syntax

```
neighbor {ipv6-address | peer-group-name} update-source loopback interface
```

To use the closest interface, use the `no neighbor {ipv6-address | peer-group-name} update-source loopback interface` command.

Parameters

- `ipv6-address`: Enter the IPv6 address in the `x:x:x::x` format. The `::` notation specifies successive hexadecimal fields of zeros.
- `peer-group-name`: Enter the name of the peer group to disable all routers within the peer group.
- `loopback interface`: Enter the keyword `loopback` followed by a number of the loopback interface. Range: 0 to 16383.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

- Introduced on E-Series TeraScale
- Introduced on E-Series ExaScale
- Introduced on C-Series and S4810.

Usage Information

Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

Syntax

```
neighbor {ipv6-address | peer-group-name} weight weight
```

To remove a weight value, use the `no neighbor {ipv6-address | peer-group-name} weight weight` command.

Parameters

- `ipv6-address`: Enter the IPv6 address in the `x:x:x::x` format. The `::` notation specifies successive hexadecimal fields of zeros.
- `peer-group-name`: Enter the name of the peer group to disable all routers within the peer group.
- `weight`: Enter a number as the weight. Range: 0 to 65535. Default: 0

Defaults

0
In the FTOS best path selection process, the path with the highest weight value is preferred.

**Note:** Reset the neighbor connection (capture bgp-pdu max-buffer-size * command) to apply the weight to the connection and recompute the best path.

---

**network**

Specify the networks for the BGP process and enter them in the BGP routing table.

**Syntax**

```
network ipv6-address prefix-length [route-map map-name]
```

To remove a network, use the no network ip-address mask [route-map map-name] command.

**Parameters**

- **ipv6-address prefix-length**
  - Enter the IPv6 address in the X:X:X::X format followed by the prefix length in the /x format.
  - Range: /0 to /128
  - The :: notation specifies successive hexadecimal fields of zeros.

- **mask**
  - Enter the mask of the IP address in the slash prefix length format (for example, /24).
  - The mask appears in command outputs in dotted decimal format (A.B.C.D).

- **route-map map-name**
  - (OPTIONAL) Enter the keyword route-map followed by the name of an established route map.
  - Only the following ROUTE-MAP mode commands are supported:
    - match ipv6 address
    - match ipv6 next-hop
    - match ipv6 route-source
    - set ipv6 next-hop
  - If the route map is not configured, the default is deny (to drop all routes).

**Defaults**

Not configured.

---

**Command Modes**

ROUTER BGPV6-ADDRESS FAMILY

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

**Usage Information**

The E-Series software resolves the network address configured by the network command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.
### network backdoor

Specify this IGP route as the preferred route.

**Syntax**
```
network ipv6-address prefix-length backdoor
```

To remove a network, use the `no network ipv6-address prefix-length backdoor` command.

**Parameters**
- `ipv6-address prefix-length`: Enter the IPv6 address in the `X:XX:XX::X` format followed by the prefix length in the `/X` format.
  - Range: `/0` to `/128`
  - The `::` notation specifies successive hexadecimal fields of zeros.

**Defaults**
Not configured.

**Command Modes**
- ROUTER BGPV6-ADDRESS FAMILY

**Command History**
- Introduced on C-Series and S4810.

**Usage Information**
Though Dell Networking OS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

### redistribute

Redistribute routes into BGP.

**Syntax**
```
redistribute {connected | static} [route-map map-name]
```

To disable redistribution, use the `no redistribution {connected | static} [route-map map-name]` command.

**Parameters**
- `connected`: Enter the keyword `connected` to redistribute routes from physically connected interfaces.
- `static`: Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
- `route-map map-name`: (OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map.
  Only the following ROUTE-MAP mode commands are supported:
  - `match ipv6 address`
  - `match ipv6 next-hop`
  - `match ipv6 route-source`
  - `set ipv6 next-hop`
  If the route map is not configured, the default is deny (to drop all routes).
IPv6 Border Gateway Protocol (IPv6 BGP) | 787

Defaults
Not configured.

Command Modes
ROUTER BGPV6-ADDRESS FAMILY

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

Usage Information
If you do not configure default-metric command, in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0:0/0) configure the neighbor default-originate command.

Related Commands
neighbor default-originate Inject the default route.

redistribute isis
Redistribute IS-IS routes into BGP.

Syntax
redistribute isis [level-1 | level-1-2 | level-2] [metric metric-value | metric-type {external | internal}] [route-map map-name]

Parameters
- level-1 | level-1-2 | level-2 (OPTIONAL) Enter the type (level) of routes to redistribute.
- metric (OPTIONAL) Assign metric to an interface for use with IPv6 information
- metric-type (OPTIONAL) The external link type associated with the default route advertised into a routing domain. You must specify one of the following:
  - external
  - internal (Default)
- route-map map-name (OPTIONAL) Enter the keyword route-map followed by the name of an established route map.

To stop redistribution of IS-IS routes, use the no redistribute isis command.

Parameters

Defaults
Not configured.

Command Modes
ROUTER BGPV6-ADDRESS FAMILY

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>
**redistribute ospf**

Redistribute OSPFv3 routes into BGP.

**Syntax**

```
redistribute ospf process-id [[match external {1 | 2}] [match internal]] [route-map map-name]
```

To stop redistribution of OSPF routes, use the `no redistribute ospf process-id` command.

**Parameters**

- `process-id` Enter the number of the OSPFv3 process.  
  Range: 1 to 65535
- `match external {1 | 2}` (OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
- `match internal` (OPTIONAL) Enter the keywords `match internal` to redistribute OSPFv3 internal routes only.
- `route-map map-name` (OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map.  
  Only the following ROUTE-MAP mode commands are supported:
  - `match ipv6 address`  
  - `match ipv6 next-hop`  
  - `match ipv6 route-source`  
  - `set ipv6 next-hop`  
  If the route map is not configured, the default is deny (to drop all routes).

**Defaults**

Not configured.

**Command Modes**

ROUTER BGPV6-ADDRESS FAMILY

**Command History**

- Version 8.4.2.1  Introduced on C-Series and S4810.
- Version 8.2.1.0  Introduced on E-Series ExaScale
- Version 7.4.1.0  Introduced on E-Series TeraScale

**Usage Information**

When you enter `redistribute ospf process-id` command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

**router bgp**

Enter ROUTER BGP mode to configure and enable BGP.

**Syntax**

```
router bgp as-number
```

To disable BGP, use the `no router bgp as-number` command.

**Parameters**

- `as-number` Enter the AS number.  
  Range: 1 to 65535.

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION
**show capture bgp-pdu neighbor**

Display BGP packet capture information for an IPv6 address on the E-Series.

**Syntax**

```
show capture bgp-pdu neighbor ipv6-address
```

**Parameters**

- `ipv6-address` Enter the IPv6 address (X:X:X::X) of a BGP neighbor.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

**Related Commands**

- `capture bgp-pdu neighbor (ipv6)` Enable capture of an IPv6 BGP neighbor packet.
- `capture bgp-pdu max-buffer-size` Specify a size for the capture buffer.

**show config**

View the current ROUTER BGP configuration.

**Syntax**

```
show config
```

**Command Modes**

- ROUTER BGPV6-ADDRESS FAMILY
show ip bgp ipv6 unicast

View the current BGP routing table for the E-Series.

Syntax

```
show ip bgp ipv6 unicast [network [network-mask] [longer-prefixes]]
```

Parameters

- **network** (OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
- **network-mask** (OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
- **longer-prefixes** (OPTIONAL) Enter the keyword longer-prefixes to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

When you enable bgp non-deterministic-med command, the show ip bgp command output for a BGP route does not list the INACTIVE reason.
show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

Syntax
show ip bgp ipv6 unicast cluster-list [cluster-id]

Parameters

cluster-id (OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes
EXEC
EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast community

View information on all routes with Community attributes or view specific BGP community groups.

Syntax
show ip bgp ipv6 unicast community [community-number] [local-as] [no-export] [no-advertise]

Parameters

community-number Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.

local-AS Enter the keywords local-AS to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise Enter the keywords no-advertise to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.

no-export Enter the keywords no-export to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes
EXEC
EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale
Usage Information
To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast` summary command. The text line above the route table states the number of COMMUNITY attributes found.

show ip bgp ipv6 unicast community-list
View routes that are affected by a specific community list.

Syntax
```
show ip bgp ipv6 unicast community-list community-list-name [exact-match]
```

Parameters
- `community-list-name` Enter the name of a configured IP community list.
- `exact-match` (OPTIONAL) Enter `exact-match` to display only for an exact match of the communities.

Command Modes
- EXEC
- EXEC Privilege

Command History
- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast dampened-paths
View BGP routes that are dampened (non-active).

Syntax
```
show ip bgp ipv6 unicast dampened-paths
```

Command Modes
- EXEC
- EXEC Privilege

Command History
- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast detail
Display BGP internal information for IPv6 Unicast address family.

Syntax
```
show ip bgp ipv6 unicast detail
```

Defaults
none

Command Modes
- EXEC
- EXEC Privilege
### show ip bgp ipv6 unicast extcommunity-list

View information on all routes with Extended Community attributes.

**Syntax**

```
show ip bgp ipv6 unicast extcommunity-list [list name]
```

**Parameters**

- `list name`: Enter the extended community list name you wish to view.

**Command Modes**

- EXEC
- EXEC Privilege

**Usage Information**

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast` summary command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp ipv6 unicast community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp ipv6 unicast` command output.

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

### show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

**Syntax**

```
show ip bgp ipv6 unicast filter-list as-path-name
```

**Parameters**

- `as-path-name`: Enter the name of an AS-PATH.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale
### show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

**Syntax**

```
show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-length] [filter-list as-path-name] [regexp regular-expression]
```

**Parameters**

- `ipv6-address prefix-length` Enter the IPv6 address in the X:XX:XX::X format followed by the prefix length in the /X format.
  - Range: /0 to /128
  - The :: notation specifies successive hexadecimal fields of zeros.

- `filter-list as-path-name` (OPTIONAL) Enter the keyword `filter-list` followed by the name of a configured AS-PATH ACL.

- `regexp regular-expression` Enter a regular expression then use one or a combination of the following characters to match:
  - `.` (period) any single character (including a white space)
  - `*` (asterisk) the sequences in a pattern (0 or more sequences)
  - `+` (plus) the sequences in a pattern (1 or more sequences)
  - `?` (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
  - `[ ]` (brackets) a range of single-character patterns.
  - `^` (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - `$` (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

### show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

**Syntax**

```
show ip bgp ipv6 unicast inconsistent-as
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale
### show ip bgp ipv6 unicast neighbors

Displays information on IPv6 unicast routes exchanged by BGP neighbors.

#### Syntax

```
show ip bgp ipv6 unicast neighbors

[ipv4-neighbor-addr | ipv6-neighbor-addr]
[advertised-routes | dampened-routes | detail | flap-statistics | routes | received-routes
 [network [network-mask]] | denied-routes [network [network-mask]]]
```

#### Parameters

- **ipv6 unicast**: Enter the `ipv6 unicast` keywords to view information only related to IPv6 unicast routes.
- **ipv4-neighbor-addr | ipv6-neighbor-addr**: (OPTIONAL) Enter the IP address of the neighbor to view only BGP route information exchanged with that neighbor.
- **advertised-routes**: (OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
- **dampened-routes**: (OPTIONAL) Enter the keyword `dampened-routes` to view information on dampened routes from the BGP neighbor.
- **detail**: (OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv4 Unicast address family.
- **flap-statistics**: (OPTIONAL) Enter the keyword `flap-statistics` to view flap statistics on the neighbor’s routes.
- **routes**: (OPTIONAL) Enter the keywords `routes` to view only the neighbor’s feasible routes.
- **received-routes [network [network-mask]]**: (OPTIONAL) Enter the keywords `received-routes` followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. **Note**: `neighbor soft-reconfiguration inbound` must be configured prior to viewing all the information received from the neighbors.
- **denied-routes [network [network-mask]]**: (OPTIONAL) Enter the keywords `denied-routes` followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

#### Command Modes

- EXEC
- EXEC Privilege

#### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv4 multicast and IPv6 unicast address families</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S4810</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added <code>detail</code> option and output now displays default MED value</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Added received and denied route options</td>
</tr>
<tr>
<td>6.3.10</td>
<td>The output is changed to display the total number of advertised prefixes</td>
</tr>
</tbody>
</table>
Example 1  

**Figure 27-2. Command Example: show ip bgp ipv6 unicast neighbors**

FTOS#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
BGP version 4, remote router ID 5.5.5.3
BGP state ESTABLISHED, in this state for 00:00:32
Last read 00:00:32, last write 00:00:32
Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
3 opens, 1 notifications, 1394 updates
6 keepalives, 0 route refresh requests
Sent 48 messages, 0 in queue
3 opens, 2 notifications, 0 updates
43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast:

- MULTIPROTO_EXT(1)
- ROUTE_REFRESH(2)
- CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv6 Unicast:

- MULTIPROTO_EXT(1)
- ROUTE_REFRESH(2)
- CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
BGP table version 12, neighbor version 12
2 accepted prefixes consume 32 bytes
Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 3; dropped 2
Last reset 00:00:39, due to Closed by neighbor

Notification History

- OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:10::4, Local port: 179
Foreign host: 5ffe:10::3, Foreign port: 35470

Notification History

- 'Connection Reset' Sent : 1 Recv: 0

BGP neighbor is 5ffe:11::3, remote AS 1, external link
BGP version 4, remote router ID 5.5.5.3
BGP state ESTABLISHED, in this state for 00:00:28
Last read 00:00:28, last write 00:00:28
Hold time is 180, keepalive interval is 60 seconds
Received 27 messages, 3 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Received 8 updates, Sent 0 updates
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast:

- MULTIPROTO_EXT(1)
- ROUTE_REFRESH(2)
- CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv6 Unicast:

- MULTIPROTO_EXT(1)
- ROUTE_REFRESH(2)
- CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
BGP table version 12, neighbor version 12
2 accepted prefixes consume 32 bytes
Prefix advertised 0, rejected 0, withdrawn 0
Connections established 3; dropped 2
Last reset 00:00:41, due to Closed by neighbor

Notification History

- OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:11::4, Local port: 179
Table 27-1. Command Example fields: show ip bgp ipv6 unicast neighbors

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version (always version 4) and the remote router ID.</td>
</tr>
<tr>
<td>BGP state</td>
<td>Displays the neighbor’s BGP state and the amount of time in hours:minutes:seconds it has been in that state.</td>
</tr>
<tr>
<td>Last read</td>
<td>This line displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• last read is the time (hours:minutes:seconds) the router read a message from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• hold time is the number of seconds configured between messages from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.</td>
</tr>
<tr>
<td>Received messages</td>
<td>This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Sent messages</td>
<td>The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Received updates</td>
<td>This line displays the number of BGP updates received and sent.</td>
</tr>
<tr>
<td>Soft reconfiguration</td>
<td>This line indicates that soft reconfiguration inbound is configured.</td>
</tr>
<tr>
<td>Minimum time</td>
<td>Displays the minimum time, in seconds, between advertisements.</td>
</tr>
<tr>
<td>(List of inbound and outbound policies)</td>
<td>Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.</td>
</tr>
<tr>
<td>For address family:</td>
<td>Displays IPv6 Unicast as the address family.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the which version of the primary BGP routing table the router and the neighbor are using.</td>
</tr>
<tr>
<td>Prefixes accepted</td>
<td>Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.</td>
</tr>
<tr>
<td>Prefixes advertised</td>
<td>Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.</td>
</tr>
<tr>
<td>Local host:</td>
<td>Displays the peering address of the local router and the TCP port number.</td>
</tr>
<tr>
<td>Foreign host:</td>
<td>Displays the peering address of the neighbor and the TCP port number.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp ipv6 unicast</td>
<td>View the current BGP routing table.</td>
</tr>
</tbody>
</table>
show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

Syntax

show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>(OPTIONAL) Enter the name of a peer group to view information about that peer group only.</td>
</tr>
<tr>
<td>detail</td>
<td>(OPTIONAL) Enter the keyword <code>detail</code> to view peer-group-specific information for the IPv6 address family.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword <code>summary</code> to view status information of the peers in that peer group. The output is the same as that found in <code>show ip bgp ipv6 unicast summary</code> command</td>
</tr>
</tbody>
</table>

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

Example

Figure 27-3.  show ip bgp peer-group Command Example

```
FTOS#show ip bgp peer-group
Peer-group RR-CLIENT, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds
  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
  9000::4:

Peer-group RR-CLIENT-PASSIV, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds
  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
  9000::9:2*

FTOS#
```
**show ip bgp ipv6 unicast summary**

Allows you to view the status of all BGP connections.

**Syntax**

```
show ip bgp ipv6 unicast summary
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced</td>
<td>on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced</td>
<td>on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
<td>on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Example**

Figure 27-4. show ip bgp summary Command Example

```
FTOS# show ip bgp summary
BGP router identifier 55.55.55.55, local AS number 18508
BGP table version is 0, main routing table version 0
6 BGP path attribute entrie(s) using 392 bytes of memory
6 BGP AS-PATH entrie(s) using 294 bytes of memory
6 BGP community entrie(s) using 234 bytes of memory

Neighbor     AS       MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down   State/Pfx
1109::33     18508    0        0        0       0     0     never     Active
2222::220     18508    0        0        0       0     0     never     Active
4000::33      18508    0        0        0       0     0     never     Active
4000::60      18508    0        0        0       0     0     never     Active
9000::4:2     18508    0        0        0       0     0     never     Active
9000::5:2     18508    35       32       0       0     0     00:16:42   0
9000::6:2     18508    35       32       0       0     0     00:16:39   0
9000::7:2     18508    35       32       0       0     0     00:16:41   0
9000::8:2     18508    35       32       0       0     0     00:16:42   0
9000::9:2     18508    35       32       0       0     0     00:16:41   0
9000::a:2     18508    35       32       0       0     0     00:16:43   0
9000::b:14    18508    35       32       0       0     0     00:16:42   0
FTOS#
```

**show ip bgp next-hop**

View all next hops (via learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

**Syntax**

```
show ip bgp next-hop [local-routes]
```

**Parameters**

- `local-routes` (OPTIONAL) Show next-hop information for local routes

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced</td>
<td>on C-Series and S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced</td>
<td>on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
<td>on E-Series TeraScale</td>
</tr>
</tbody>
</table>
**Example**

**Example Figure 27-5. show ip bgp next-hop Command Example**

<table>
<thead>
<tr>
<th>Next-hop</th>
<th>Via</th>
<th>RefCount</th>
<th>Cost</th>
<th>Flaps</th>
<th>Time Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>9000::5:2</td>
<td>9000::5:2, Gi 8/38</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>00:23:22</td>
</tr>
<tr>
<td>9000::6:2</td>
<td>9000::6:2, Gi 8/38</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>00:23:22</td>
</tr>
<tr>
<td>9000::7:2</td>
<td>9000::7:2, Gi 8/38</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>00:23:22</td>
</tr>
<tr>
<td>9000::8:2</td>
<td>9000::8:2, Gi 8/38</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>00:23:22</td>
</tr>
<tr>
<td>9000::9:2</td>
<td>9000::9:2, Gi 8/38</td>
<td>6000</td>
<td>0</td>
<td>0</td>
<td>00:23:16</td>
</tr>
<tr>
<td>9000::a:2</td>
<td>9000::a:2, Gi 8/38</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>00:23:22</td>
</tr>
</tbody>
</table>

**show ip bgp paths**

View all the BGP path attributes in the BGP database.

**Syntax**

```
show ip bgp paths [regexp regular-expression]
```

**Parameters**

- `regexp` component
  - `regular-expression` Enter a regular expression then use one or a combination of the following characters to match:
    - `.` = (period) any single character (including a white space)
    - `*` = (asterisk) the sequences in a pattern (0 or more sequences)
    - `+` = (plus) the sequences in a pattern (1 or more sequences)
    - `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).
    - `[ ]` = (brackets) a range of single-character patterns.
    - `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
    - `$` = (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 8.2.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series TeraScale

**show ip bgp paths as-path**

View all unique AS-PATHs in the BGP database.

**Syntax**

```
show ip bgp paths as-path
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

Syntax  show ip bgp paths community

Command Modes EXEC
            EXEC Privilege

Command History

Version 8.4.2.1  Introduced on C-Series and S4810.
Version 8.2.1.0  Introduced on E-Series ExaScale
Version 7.4.1.0  Introduced on E-Series TeraScale

show ip bgp paths extcommunity

View all unique Extended community information in the BGP database.

Syntax  show ip bgp paths extcommunity

Command Modes EXEC
            EXEC Privilege

Command History

Version 8.4.2.1  Introduced on C-Series and S4810.
Version 8.2.1.0  Introduced on E-Series ExaScale
Version 7.4.1.0  Introduced on E-Series TeraScale

show ip bgp regexp

Allows you to view the subset of BGP routing table matching the regular expressions specified.

Syntax  show ip bgp regexp regular-expression [character]
**Parameters**

`regular-expression [character]`  
Enter a regular expression then use one or a combination of the following characters to match:

- `. ` (period) any single character (including a white space)
- `* ` (asterisk) the sequences in a pattern (0 or more sequences)
- `+ ` (plus) the sequences in a pattern (1 or more sequences)
- `? ` (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
- `[] ` (brackets) a range of single-character patterns.
- `^ ` (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$ ` (dollar sign) the end of the output string.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>C-Series and S4810</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series TeraScale</td>
</tr>
</tbody>
</table>

**timers bgp**

C E S4810

Allows you to adjust the BGP network timers for all neighbors.

**Syntax**

`timers bgp keepalive holdtimer`

To return to the default values, use the no `timers bgp` command.

**Parameters**

`keepalive`  
Enter the time interval in seconds between which the E-Series sends keepalive messages.

Range: 1 to 65535  
Default: 60 seconds

`holdtimer`  
Enter the time interval in seconds which the E-Series waits since the last keepalive message before declaring a BGP peer dead.

Range: 3 to 65535  
Default: 180 seconds

**Defaults**

`keepalive = 60 seconds; holdtimer = 180 seconds`

**Command Modes**

ROUTER BGP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>C-Series and S4810</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Related Commands**

`neighbor timers`  
Adjust BGP timers for a specific peer or peer group.
IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). Dell Networking OS MBGP is implemented as per IETF RFC 1858. The MBGP commands are:

- address family
- aggregate-address
- bgp dampening
- clear ip bgp ipv6 unicast
clear ip bgp ipv6 unicast dampening
clear ip bgp ipv6 unicast flap-statistics
debug ip bgp ipv6 unicast dampening
debug ip bgp ipv6 unicast peer-group updates
debug ip bgp ipv6 unicast updates
distance bgp
neighbor activate
neighbor advertisement-interval
neighbor default-originate
neighbor distribute-list
neighbor filter-list
neighbor maximum-prefix
neighbor next-hop-self
neighbor remove-private-as
neighbor route-map
neighbor route-reflector-client
network
redistribute
show ip bgp ipv6 unicast
show ip bgp ipv6 unicast cluster-list
show ip bgp ipv6 unicast community
show ip bgp ipv6 unicast community-list
show ip bgp ipv6 unicast dampened-paths
show ip bgp ipv6 unicast detail
show ip bgp ipv6 unicast filter-list
show ip bgp ipv6 unicast flap-statistics
show ip bgp ipv6 unicast inconsistent-as
show ip bgp ipv6 unicast neighbors
show ip bgp ipv6 unicast peer-group
show ip bgp ipv6 unicast summary

address family

This command changes the context to SAFI (Subsequent Address Family Identifier).

Syntax    address family ipv6 unicast
To remove SAFI context, use the `no address family ipv6 unicast` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>Enter the keyword <code>ipv6</code> to specify the address family as IPv6.</td>
</tr>
<tr>
<td>unicast</td>
<td>Enter the keyword <code>unicast</code> to specify multicast as SAFI.</td>
</tr>
</tbody>
</table>

**Defaults**
IPv6 Unicast

**Command Modes**
ROUTER BGPV6-ADDRESS FAMILY

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Usage Information**
All subsequent commands will apply to this address family once this command is executed. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering `exit` and returning to the Router BGP context.

---

**aggregate-address**

Summarize a range of prefixes to minimize the number of entries in the routing table.

**Syntax**

```
aggregate-address ipv6-address prefix-length [advertise-map map-name] [as-set]
[attribute-map map-name] [summary-only] [suppress-map map-name]
```

**Parameters**

- **ipv6-address prefix-length**
  - Enter the IPv6 address in the `x:x:x:x::x` format followed by the prefix length in the `/x` format.
  - Range: `/0` to `/128`
  - The `::` notation specifies successive hexadecimal fields of zeros.

- **advertise-map map-name**
  - (OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.

- **as-set**
  - (OPTIONAL) Enter the keyword `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

- **attribute-map map-name**
  - (OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.

- **summary-only**
  - (OPTIONAL) Enter the keyword `summary-only` to advertise only the aggregate address. Specific routes will not be advertised.

- **suppress-map map-name**
  - (OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

**Defaults**
Not configured.

**Command Modes**
ROUTER BGPV6-ADDRESS FAMILY
At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate. If routes within the aggregate are constantly changing, the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppressed; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected via the `network` command, that route will still appear in the routing table if the summary-only parameter is configured in the `aggregate-address` command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

### bgp dampening

Enable MBGP route dampening.

**Syntax**
```
bgp dampening [half-life time] [route-map map-name]
```

To disable route dampening, use the `no bgp dampening [half-life time] [route-map map-name]` command.

**Parameters**

- `half-life time` (OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires.
  
  Range: 1 to 45.
  
  Default: 15 minutes

- `route-map map-name` (OPTIONAL) Enter the keyword `route-map` followed by the name of a configured route map.
  
  Only match commands in the configured route map are supported.

**Defaults**

Disabled.

**Command Modes**

- ROUTER BGPV6-ADDRESS FAMILY

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

### clear ip bgp ipv6 unicast

Reset MBGP sessions.
### clear ip bgp ipv6 unicast * ipv6-address prefix-length [dampening | flap-statistics] peer-group

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Enter the character * to clear all peers.</td>
</tr>
<tr>
<td>ipv6-address prefix-length</td>
<td>Enter the IPv6 address in the X: X::X format followed by the prefix length in the /x format. Range: /0 to /128. The :: notation specifies successive hexadecimal fields of zeros.</td>
</tr>
<tr>
<td>dampening</td>
<td>(OPTIONAL) Enter the keyword dampening to clear route flap dampening information.</td>
</tr>
<tr>
<td>flap-statistics</td>
<td>(OPTIONAL) Enter the keyword flap-statistics to reset the flap statistics on all prefixes from that neighbor.</td>
</tr>
<tr>
<td>peer-group</td>
<td>(OPTIONAL) Enter the keyword peer-group to clear all members of a peer-group.</td>
</tr>
</tbody>
</table>

### Command Modes

EXEC Privilege

### Command History

- **Version 8.4.2.0** Introduced on C-Series and S4810.
- **Version 7.4.1.0** Introduced.

### clear ip bgp ipv6 unicast dampening

Clear information on route dampening.

**Syntax**

```
clear ip bgp dampening ipv6 unicast [network network-mask]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>(OPTIONAL) Enter the IPv6 network address in X: X::X format.</td>
</tr>
<tr>
<td>network-mask</td>
<td>If you enter the network address, then enter the network mask, from 0 to 128.</td>
</tr>
</tbody>
</table>

### Command Modes

EXEC Privilege

### Command History

- **Version 8.4.2.1** Introduced on C-Series and S4810.
- **Version 7.4.1.0** Introduced on E-Series TeraScale

### clear ip bgp ipv6 unicast flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

**Syntax**

```
clear ip bgp ipv6 unicast flap-statistics [network | filter-list list | regexp regexp]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>(OPTIONAL) Enter the IPv6 network address in X: X::X format to clear flap statistics.</td>
</tr>
</tbody>
</table>

**Command History**

- **Version 8.4.2.0** Introduced on C-Series and S4810.
- **Version 7.4.1.0** Introduced.
### debug ip bgp ipv6 unicast dampening

View information on routes being dampened.

**Syntax**
```
debug ip bgp ipv6 unicast dampening
```

To disable debugging, enter `no debug ip bgp ipv6 unicast dampening`

**Parameters**
- `dampening` Enter the keyword `dampening` to clear route flap dampening information.

**Command Modes**
- EXEC Privilege

**Command History**
- Version 8.4.2.0 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced

### debug ip bgp ipv6 unicast peer-group updates

View information about BGP peer-group updates.

**Syntax**
```
debug ip bgp ipv6 unicast peer-group peer-group-name updates [in | out]
```

To disable debugging, enter `no debug ip bgp ipv6 unicast peer-group peer-group-name updates [in | out]` command.

**Parameters**
- `peer-group` Enter the keyword `peer-group` followed by the name of the peer-group.
- `peer-group-name` Enter the name of the peer-group.
- `updates` Enter the keyword `updates` to view BGP update information.
debug ip bgp ipv6 unicast updates

View information about BGP updates.

Syntax

```
debug ip bgp ipv6 unicast ipv6-address prefix-length updates [in | out]
```

To disable debugging, enter `no debug ip bgp ipv6 unicast ipv6-address prefix-length updates [in | out]` command.

Parameters

- **ipv6-address**
  - Enter the IPv6 address in the `x:X:X::X` format followed by the prefix length in the `/x` format.
  - Range: /0 to /128
  - The `:` notation specifies successive hexadecimal fields of zeros

- **updates**
  - Enter the keyword `updates` to view BGP update information.

- **in**
  - (OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.

- **out**
  - (OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Defaults

Disabled.

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

distance bgp

Define an administrative distance for routes.

Syntax

```
distance bgp external-distance internal-distance local-distance
```

To return to default values, enter `no distance bgp`. 
**Parameters**

- **external-distance**
  - Enter a number to assign to routes learned from a neighbor external to the AS.
  - Range: 1 to 255.
  - Default: 20

- **internal-distance**
  - Enter a number to assign to routes learned from a router within the AS.
  - Range: 1 to 255.
  - Default: 200

- **local-distance**
  - Enter a number to assign to routes learned from networks listed in the network command.
  - Range: 1 to 255.
  - Default: 200

**Defaults**

- **external-distance** = 20; **internal-distance** = 200; **local-distance** = 200.

**Command Modes**

- ROUTER BGPV6-ADDRESS FAMILY

**Command History**

- **Version 8.4.2.1** Introduced on C-Series and S4810.
- **Version 7.4.1.0** Introduced on E-Series TeraScale

**Usage Information**

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

**neighbor activate**

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

**Syntax**

```
neighbor [ipv6-address | peer-group-name] activate
```

To disable, use the no neighbor [ipv6-address | peer-group-name] activate command.

**Parameters**

- **ipv6-address**
  - (OPTIONAL) Enter the IPv6 address in the X:XX::X format.
  - The :: notation specifies successive hexadecimal fields of zeros.

- **peer-group-name**
  - (OPTIONAL) Enter the name of the peer group

- **activate**
  - Enter the keyword activate to enable the neighbor/peer group in the new AFI/SAFI.

**Defaults**

- Disabled

**Command Modes**

- ROUTER BGPV6-ADDRESS FAMILY

**Command History**

- **Version 8.4.2.1** Introduced on C-Series and S4810.
- **Version 7.4.1.0** Introduced on E-Series TeraScale
Usage Information
By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using **activate** in the new context, the neighbor/peer group is enabled for AFI/SAFI.

Related Commands

| address family | Changes the context to SAFI |

**neighbor advertisement-interval**

Set the advertisement interval between BGP neighbors or within a BGP peer group.

**Syntax**

```
neighbor {ipv6-address | peer-group-name} advertisement-interval seconds
```

To return to the default value, use the **no neighbor {ipv6-address | peer-group-name} advertisement-interval** command.

**Parameters**

| ipv6-address | (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zeros. |
| peer-group-name | Enter the name of the peer group to set the advertisement interval for all routers in the peer group. |
| seconds | Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers. |

**Defaults**

seconds = 5 seconds (internal peers); seconds = 30 seconds (external peers)

**Command Modes**

ROUTER BGPV6-ADDRESS FAMILY

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

**neighbor default-originate**

Inject the default route to a BGP peer or neighbor.

**Syntax**

```
neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]
```

To remove a default route, use the **no neighbor {ipv6-address | peer-group-name} default-originate** command.

**Parameters**

| ipv6-address | (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zeros. |
| peer-group-name | Enter the name of the peer group to set the default route of all routers in that peer group. |
| route-map | (OPTIONAL) Enter the keyword route-map followed by the name of a configured route map. |
| map-name | |

**Related Commands**

| address family | Changes the context to SAFI |
Defaults
Not configured.

Command Modes
ROUTER BGPV6-ADDRESS FAMILY

Command History

<table>
<thead>
<tr>
<th>Version 8.4.2.1</th>
<th>Introduced on C-Series and S4810.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**neighbor distribute-list**
Distribute BGP information via an established prefix list.

**Syntax**
`neighbor [ipv6-address | peer-group-name] distribute-list prefix-list-name [in | out]`

To delete a neighbor distribution list, use the `no neighbor [ipv6-address | peer-group-name] distribute-list prefix-list-name [in | out]` command.

**Parameters**
- **ipv6-address**: (OPTIONAL) Enter the IPv6 address in the `X:X:X:X::X` format. The `::` notation specifies successive hexadecimal fields of zeros.
- **peer-group-name**: Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
- **prefix-list-name**: Enter the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).
- **in**: Enter the keyword `in` to distribute only inbound traffic.
- **out**: Enter the keyword `out` to distribute only outbound traffic.

**Defaults**
Not configured.

**Command Modes**
ROUTER BGPV6-ADDRESS FAMILY

**Command History**

<table>
<thead>
<tr>
<th>Version 8.4.2.1</th>
<th>Introduced on C-Series and S4810.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Usage Information**
Other BGP filtering commands include: `neighbor filter-list` and `neighbor route-map`.

**Related Commands**
- `neighbor filter-list` Assign a AS-PATH list to a neighbor or peer group.
- `neighbor route-map` Assign a route map to a neighbor or peer group.

**neighbor filter-list**
Configure a BGP filter based on the AS-PATH attribute.

**Syntax**
`neighbor [ipv6-address | peer-group-name] filter-list aspath access-list-name [in | out]`

To delete a BGP filter, use the `no neighbor [ipv6-address | peer-group-name] filter-list aspath access-list-name [in | out]` command.
neighbor maximum-prefix

Control the number of network prefixes received.

Syntax

neighbor ipv6-address | peer-group-name maximum-prefix maximum [threshold] [warning-only]

To return to the default values, use the no neighbor ipv6-address | peer-group-name maximum-prefix maximum command.

Parameters

- **ipv6-address**: Enter the IPv6 address in the XX:XX:XX::X format. The :: notation specifies successive hexadecimal fields of zeros.
- **peer-group-name**: Enter the name of the peer group.
- **maximum**: Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
- **threshold**: Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the E-Series software sends a message. Range: 1 to 100 percent. Default: 75.
- **warning-only**: Enter the keyword warning-only to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults

- **threshold = 75**

Command Modes

- ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 7.4.1.0 Introduced on E-Series TeraScale
neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor.

Syntax

```
neighbor ipv6-address | peer-group-name next-hop-self
```

To return to the default setting, use the no neighbor ipv6-address | peer-group-name next-hop-self command.

Parameters

- `ipv6-address` (OPTIONAL) Enter the IPv6 address in the X::X::X::X format.
  The :: notation specifies successive hexadecimal fields of zeros.

- `peer-group-name` (OPTIONAL) Enter the name of the peer group.

Defaults

Disabled.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

If the set ipv6 next-hop command in the ROUTE-MAP mode is configured, its configuration takes precedence over the neighbor next-hop-self command.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax

```
neighbor ipv6-address | peer-group-name remove-private-as
```

To return to the default, use the no neighbor ipv6-address | peer-group-name remove-private-as command.

Parameters

- `ipv6-address` (OPTIONAL) Enter the IPv6 address in the X::X::X::X format.
  The :: notation specifies successive hexadecimal fields of zeros.

- `peer-group-name` (OPTIONAL) Enter the name of the peer group to remove the private AS numbers

Defaults

Disabled (that is, private AS number are not removed).

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale
neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax

```
neighbor ipv6-address | peer-group-name route-map map-name [in | out]
```

To remove the route map, use the `no neighbor [ipv6-address | peer-group-name] route-map map-name [in | out]` command.

Parameters

- `ipv6-address` (OPTIONAL) Enter the IPv6 address in the X::X::X::X format. The :: notation specifies successive hexadecimal fields of zeros.
- `peer-group-name` (OPTIONAL) Enter the name of the peer group.
- `map-name` Enter the name of an established route map.
  - If the Route map is not configured, the default is deny (to drop all routes).
- `in` Enter the keyword `in` to filter inbound routes.
- `out` Enter the keyword `out` to filter outbound routes.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

Syntax

```
neighbor ipv6-address | peer-group-name route-reflector-client
```

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor ipv6-address | peer-group-name route-reflector-client` command.

Parameters

- `ipv6-address` (OPTIONAL) Enter the IPv6 address in the X::X::X::X format. The :: notation specifies successive hexadecimal fields of zeros.
- `peer-group-name` (OPTIONAL) Enter the name of the peer group.

Defaults

Not configured.
Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax

network ipv6-address [route-map map-name]

To remove a network, use the no network ipv6-address [route-map map-name] command.

Parameters

ipv6-address Enter the IPv6 address in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zeros.

route-map map-name (OPTIONAL) Enter the keyword route-map followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported:

• match ipv6 address
• match ipv6 next-hop
• match ipv6 route-source
• set ipv6 next-hop

If the route map is not configured, the default is deny (to drop all routes).

Defaults

Not configured.

Related Commands

redistribute Redistribute routes into BGP.
**redistribute**

Redistribute routes into BGP.

**Syntax**

```
redistribute [connected | static] [route-map map-name]
```

To disable redistribution, use the `no redistribution [connected | static] [route-map map-name]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>connected</code></td>
<td>Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.</td>
</tr>
<tr>
<td><code>route-map</code></td>
<td>(OPTIONAL) Enter the keyword <code>route-map</code> followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • <code>match ipv6 address</code> • <code>match ipv6 next-hop</code> • <code>match ipv6 route-source</code> • <code>set ipv6 next-hop</code> If the route map is not configured, the default is deny (to drop all routes).</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER BGPV6-ADDRESS FAMILY

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Usage Information**

If you do not configure `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0:0/0) configure the `neighbor default-originate` command.

**Related Commands**

- `neighbor default-originate`: Inject the default route.

---

**show ip bgp ipv6 unicast**

View the current MBGP routing table for the E-Series.

**Syntax**

```
show ip bgp ipv6 unicast [network [network-mask] [length]]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network</code></td>
<td>(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.</td>
</tr>
<tr>
<td><code>network-mask</code></td>
<td>(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.</td>
</tr>
<tr>
<td><code>longer-prefixes</code></td>
<td>(OPTIONAL) Enter the keyword <code>longer-prefixes</code> to view all routes with a common prefix.</td>
</tr>
</tbody>
</table>
Command Modes

- EXEC
- EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

Example

**Figure 27-6. show ip bgp ipv6 unicast**

```
FTOS#show ip bgp ipv6 unicast
BGP table version is 8, local router ID is 5.5.10.4

Network       Next Hop          Metric  LocPrf Weight Path
---           ------            -----   ------  ------  ----
h  dead:1::/100  5ffe:10::3  0      0          1  i
h  5ffe:11::3  0      0          1  i
*>  dead:2::/100  5ffe:10::3  0      0          1  i
*   5ffe:11::3  0      0          1  i
*>  dead:3::/100  5ffe:10::3  0      0          1  i
*   5ffe:11::3  0      0          1  i
h  dead:4::/100  5ffe:10::3  0      0          1  i
h  5ffe:11::3  0      0          1  i
```

FTOS#show ip bgp ipv6 unicast dead:3::/100
BGP routing table entry for dead:3::/100, version 3
Paths: (2 available, table Default-MBGP-Routing-Table.)
Not advertised to any peer

Received from:
5ffe:10::3 (5.5.5.3) Best
AS_PATH : 1

Next-Hop : 5ffe:10::3, Cost : 0
Origin IGP, Metric 0, LocalPref 100, Weight 0, external

5ffe:11::3 (5.5.5.3)
AS_PATH : 1

Next-Hop : 5ffe:11::3, Cost : 0
Origin IGP, Metric 0, LocalPref 100, Weight 0, external
Inactive reason: Peer IP address

```
Table 27-2. show ip bgp Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Displays the next hop address of the BGP router. If 0:0/0 is listed in this column, then local routes exist in the routing table.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

Related Commands

- `show ip bgp ipv6 unicast community` View BGP communities.
show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

Syntax

```
show ip bgp ipv6 unicast cluster-list [cluster-id]
```

Parameters

```
cluster-id (OPTIONAL) Enter the cluster id in dotted decimal format.
```

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast community

View information on all routes with Community attributes or view specific BGP community groups.

Syntax

```
show ip bgp ipv6 unicast community [community-number] [local-as] [no-export] [no-advertise]
```

Parameters

```
community-number Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.

llocal-AS Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.

no-export Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
```

Command Modes

- EXEC

EXEC Privilege

Command History

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.
**show ip bgp ipv6 unicast community-list**

View routes that are affected by a specific community list.

**Syntax**

```plaintext
show ip bgp ipv6 unicast community-list community-list-name
```

**Parameters**

- `community-list-name` Enter the name of a configured IP community list.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

---

**show ip bgp ipv6 unicast dampened-paths**

View BGP routes that are dampened (non-active).

**Syntax**

```plaintext
show ip bgp ipv6 unicast dampened-paths
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale

---

**show ip bgp ipv6 unicast detail**

Display detailed BGP information.

**Syntax**

```plaintext
show ip bgp ipv6 unicast detail
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.2.1 Introduced on C-Series and S4810.
- Version 7.4.1.0 Introduced on E-Series TeraScale
Example

Example Figure 27-7. show ip bgp ipv6 unicast detail Command Example (Partial)

R2_Training#show ip bgp ipv6 unicast detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmpP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics 327741 :
NhLocAS 1 : NdState 2 : NdRPFPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedMissVal -1 :
NdIgnoreId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTb1P 0x41a19088
NdASPTb1P 0x41a19090 : NdCommTb1P 0x41a19098 : NhOptTransTb1P 0x41a190a0 :
NdRRClsTb1P 0x41a190a8
NdPktEA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP : NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a6c000 : NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 : NdComSortHdP
0x41a19d04 : NdHopDFrdHdP 0x41a1a3e0 : NumNhDfrd 0 : CfgHdrAFMask 1

show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

Syntax

show ip bgp ipv6 unicast filter-list as-path-name

Parameters

as-path-name Enter the name of an AS-PATH.

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.

Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

Syntax

show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-length] [filter-list
as-path-name] [regexp regular-expression]
IPv6 Border Gateway Protocol (IPv6 BGP) | 821

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv6-address</strong></td>
<td>(OPTIONAL) Enter the IPv6 address in the X::X::X::X format followed by the prefix length in the /x format.</td>
</tr>
<tr>
<td><strong>prefix-length</strong></td>
<td>Range: /0 to /128</td>
</tr>
<tr>
<td><strong>filter-list as-path-name</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>filter-list</strong> followed by the name of a configured AS-PATH ACL.</td>
</tr>
</tbody>
</table>
| **regexp regular-expression** | Enter a regular expression then use one or a combination of the following characters to match:  
  - . = (period) any single character (including a white space)  
  - * = (asterisk) the sequences in a pattern (0 or more sequences)  
  - + = (plus) the sequences in a pattern (1 or more sequences)  
  - ? = (question mark) sequences in a pattern (either 0 or 1 sequences). You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.  
  - [ ] = (brackets) a range of single-character patterns.  
  - ^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.  
  - $ = (dollar sign) the end of the output string. |

### Command Modes

- **EXEC**
- **EXEC Privilege**

### Command History

- **Version 8.4.2.1** Introduced on C-Series and S4810.
- **Version 7.4.1.0** Introduced on E-Series TeraScale

### Example

**Figure 27-8. show ip bgp ipv6 unicast flap-statistics command**

```
FTOS#show ip bgp ipv6 unicast flap-statistics
BGP table version is 8, local router ID is 5.5.10.4
Status codes: s suppressed, S stale, d damped, h history, * valid, > best Path
source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>From</th>
<th>Flaps</th>
<th>Duration</th>
<th>Reuse</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>h dead:1::/100</td>
<td>Sffe:10::3</td>
<td>1</td>
<td>00:03:20</td>
<td></td>
<td>1 i</td>
</tr>
<tr>
<td>h dead:1::/100</td>
<td>Sffe:11::3</td>
<td>1</td>
<td>00:03:20</td>
<td></td>
<td>1 i</td>
</tr>
<tr>
<td>h dead:4::/100</td>
<td>Sffe:10::3</td>
<td>1</td>
<td>00:04:39</td>
<td></td>
<td>1 i</td>
</tr>
<tr>
<td>h dead:4::/100</td>
<td>Sffe:11::3</td>
<td>1</td>
<td>00:04:39</td>
<td></td>
<td>1 i</td>
</tr>
</tbody>
</table>
```

FTOS#
show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax

show ip bgp ipv6 unicast inconsistent-as

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast neighbors

Allows you to view the information exchanged by BGP neighbors.

Syntax

show ip bgp ipv6 unicast neighbors [ipv6-address prefix-length | advertised-routes | dampened-routes | detail | flap-statistics | routes]

Parameters

ipv6-address
prefix-length
(OPTIONAL) Enter the IPv6 address in the X::X::X::X format followed by the prefix length in the /x format.
Range: /0 to /128
The :: notation specifies successive hexadecimal fields of zeros.

advertised-routes
(OPTIONAL) Enter the keywords advertised-routes to view only the routes the neighbor sent.

dampened-routes
(OPTIONAL) Enter the keyword dampened-routes to view information on dampened routes from the BGP neighbor.

flap-statistics
(OPTIONAL) Enter the keyword flap-statistics to view flap statistics on the neighbor’s routes.

detail
(OPTIONAL) Display detailed neighbor information.

routes
(OPTIONAL) Enter the keywords routes to view only the neighbor’s feasible routes.

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.4.2.1 Introduced on C-Series and S4810.
Version 7.5.1.0 Modified: Added detail option; added information to output.
Version 7.4.1.0 Introduced on E-Series TeraScale
Example

Figure 27-9.  show ip bgp ipv6 unicast neighbors Command Example (Partial)

FTOS#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
BGP version 4, remote router ID 5.5.5.3
BGP state ESTABLISHED, in this state for 00:00:32
Last read 00:00:32, last write 00:00:32
Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
  3 opens, 1 notifications, 1394 updates
  6 keepalives, 0 route refresh requests
Sent 48 messages, 0 in queue
  3 opens, 2 notifications, 0 updates
  43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv6 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
BGP table version 12, neighbor version 12
2 accepted prefixes consume 32 bytes
Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 3; dropped 2
Last reset 00:00:39, due to Closed by neighbor

Notification History
'OPEN error/Bad AS' Sent : 0  Recv: 1

Local host: 5ffe:10::4, Local port: 179
Foreign host: 5ffe:10:13, Foreign port: 35470

BGP neighbor is 5ffe:11::3, remote AS 1, external link
BGP version 4, remote router ID 5.5.5.3
BGP state ESTABLISHED, in this state for 00:00:28
Last read 00:00:28, last write 00:00:28
Hold time is 180, keepalive interval is 60 seconds
Received 27 messages, 3 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Received 8 updates, Sent 0 updates
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds
Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv6 Unicast:
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
BGP table version 12, neighbor version 12
2 accepted prefixes consume 32 bytes
Prefix advertisement 0, rejected 0, withdrawn 0
Connections established 3; dropped 2
Last reset 00:00:41, due to Closed by neighbor

Notification History
'OPEN error/Bad AS' Sent : 0  Recv: 1

Local host: 5ffe:11::4, Local port: 179
### Table 27-3. show ip bgp neighbors Command Fields

<table>
<thead>
<tr>
<th>Lines beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version (always version 4) and the remote router ID.</td>
</tr>
<tr>
<td>BGP state</td>
<td>Displays the neighbor’s BGP state and the amount of time in hours:minutes:seconds it has been in that state.</td>
</tr>
<tr>
<td>Last read</td>
<td>This line displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• last read is the time (hours:minutes:seconds) the router read a message from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• hold time is the number of seconds configured between messages from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.</td>
</tr>
<tr>
<td>Received messages</td>
<td>This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Sent messages</td>
<td>The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.</td>
</tr>
<tr>
<td>Received updates</td>
<td>This line displays the number of BGP updates received and sent.</td>
</tr>
<tr>
<td>Minimum time</td>
<td>Displays the minimum time, in seconds, between advertisements.</td>
</tr>
<tr>
<td>(list of inbound and outbound policies)</td>
<td>Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.</td>
</tr>
<tr>
<td>For address family:</td>
<td>Displays IPv6 Unicast as the address family.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays which version of the primary BGP routing table the router and the neighbor are using.</td>
</tr>
<tr>
<td>accepted prefixes</td>
<td>Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.</td>
</tr>
<tr>
<td>Prefix advertised</td>
<td>Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.</td>
</tr>
<tr>
<td>Local host:</td>
<td>Displays the peering address of the local router and the TCP port number.</td>
</tr>
<tr>
<td>Foreign host:</td>
<td>Displays the peering address of the neighbor and the TCP port number.</td>
</tr>
</tbody>
</table>

**Related Commands**

| show ip bgp ipv6 unicast | View the current BGP routing table. |
show ip bgp ipv6 unicast peer-group

`show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-group-name</td>
<td>(OPTIONAL) Enter the name of a peer group to view information about that peer group only.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword <code>summary</code> to view status information of the peers in that peer group. The output is the same as that found in <code>show ip bgp ipv6 unicast summary</code> command</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Related Commands**

- `neighbor peer-group (assigning peers)` Assign peer to a peer-group.
- `neighbor peer-group (creating group)` Create a peer group.

---

show ip bgp ipv6 unicast summary

`show ip bgp ipv6 unicast summary` allows you to view the status of all BGP connections.

**Syntax**

`show ip bgp ipv6 unicast summary`

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on C-Series and S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>

**Example**

**Figure 27-10. show ip bgp summary Command Example**

```
FTOS#show ip bgp ipv6 unicast summary
BGP router identifier 5.5.10.4, local AS number 100
BGP table version is 12, main routing table version 12
2 network entrie(s) and 4 paths using 536 bytes of memory
1 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths, 0 penalized paths

Neighbor     AS  MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/Pfx
5ffe:10::3   1   28      0   12    0   0 00:01:01         2
5ffe:11::3   1   27      0   12    0   0 00:00:55         2
FTOS#
```
### Table 27-4. show ip bgp summary Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP router identifier</td>
<td>Displays the local router ID and the AS number.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the BGP table version and the main routing table version.</td>
</tr>
<tr>
<td>network entries</td>
<td>Displays the number of network entries and route paths and the amount of memory used to process those entries.</td>
</tr>
<tr>
<td>BGP path attribute entries</td>
<td>Displays the number of BGP path attributes and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP AS-PATH entries</td>
<td>Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP community entries</td>
<td>Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The <code>show ip bgp ipv6 unicast community</code> command provides more details on the COMMUNITY attributes.</td>
</tr>
<tr>
<td>Dampening enabled</td>
<td>Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Displays the BGP neighbor address.</td>
</tr>
<tr>
<td>AS</td>
<td>Displays the AS number of the neighbor.</td>
</tr>
<tr>
<td>MsgRecvd</td>
<td>Displays the number of BGP messages that neighbor received.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Displays the number of BGP messages that neighbor sent.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Displays the version of the BGP table that was sent to that neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Displays the number of messages from that neighbor waiting to be processed.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.</td>
</tr>
<tr>
<td>State/Pfx</td>
<td>If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the neighbor maximum-prefix command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm) When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.</td>
</tr>
</tbody>
</table>
Intermediate System to Intermediate System (IS-IS)

Overview

Intermediate System to Intermediate System Protocol (IS-IS) for IPv4 and IPv6 is supported only on the E-Series platform, as indicated by the E character under each command heading.

IS-IS is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an intermediate system. Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

IS-IS protocol standards are listed in the Standard Compliance chapter in the Dell Networking OS Configuration Guide.

Note: The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

Commands

The following are the Dell Networking OS commands to enable IS-IS.

• adjacency-check
• advertise
• area-password
• clear config
• clear isis
• clns host
• debug isis
• debug isis adj-packets
• debug isis local-updates
• debug isis snp-packets
• debug isis spf-triggers
• debug isis update-packets
- default-information originate
- description
- distance
- distribute-list in
- distribute-list out
- distribute-list redistributed-override
- domain-password
- graceful-restart ietf
- graceful-restart interval
- graceful-restart t1
- graceful-restart t2
- graceful-restart t3
- graceful-restart restart-wait
- hello padding
- hostname dynamic
- ignore-lsp-errors
- ip router isis
- ipv6 router isis
- isis circuit-type
- isis csnp-interval
- isis hello-interval
- isis hello-multiplier
- isis hello padding
- isis ipv6 metric
- isis metric
- isis network point-to-point
- isis password
- isis priority
- is-type
- log-adjacency-changes
- lsp-gen-interval
- lsp-mtu
- lsp-refresh-interval
- max-area-addresses
- max-lsp-lifetime
- maximum-paths
- metric-style
- multi-topology
- net
- passive-interface
- redistribute
- redistribute bgp
- redistribute ospf
- router isis
- set-overload-bit
- show config
• show isis database
• show isis graceful-restart detail
• show isis hostname
• show isis interface
• show isis neighbors
• show isis protocol
• show isis traffic
• spf-interval

adjacency-check

Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

Syntax adjacency-check

To disable adjacency check, use the no adjacency-check command.

Defaults Enabled

Command Modes ROUTER ISIS (for IPv4)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Introduced on E-Series</th>
</tr>
</thead>
</table>

Usage Information

Use this command to perform protocol-support consistency checks on hello packets. The adjacency-check is enabled by default.

advertise

Leak routes between levels (distribute IP prefixes between Level 1 and Level 2 and vice versa).

Syntax advertise {level1-into-level2 | level2-into-level1} prefix-list-name

To return to the default, use the no advertise {level1-into-level2 | level2-into-level1} [prefix-list-name] command.

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level1-into-level2</td>
<td>Enter the keyword level1-into-level2 to advertise Level 1 routes into Level 2 LSPs. This is the default.</td>
</tr>
<tr>
<td>level2-into-level1</td>
<td>Enter the keyword level2-into-level1 to advertise Level 2 inter-area routes into Level 1 LSPs. Described in RFC 2966.</td>
</tr>
<tr>
<td>prefix-list-name</td>
<td>Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.</td>
</tr>
</tbody>
</table>

Defaults level1-into-level2 (Level 1 to Level 2 leaking enabled.)
### area-password

Configure a Hash Message Authentication Code (HMAC) authentication password for an area.

**Syntax**

```
area-password [hmac-md5 | encryption-type] password
```

To delete a password, enter `no area-password`.

**Parameters**

- **hmac-md5** (OPTIONAL) Enter the keyword `hmac-md5` to encrypt the password.
- **encryption-type** (OPTIONAL) Enter 7 to encrypt the password using DES.
- **password** Enter a 1—16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text which only provides limited security.

**Defaults**

Not configured.

**Command Modes**

ROUTER ISIS

**Usage Information**

Use the `area-password` command on routers within an area to prevent the link state database from receiving incorrect routing information from unauthorized routers.

The password configured is injected into Level 1 LSPs, CSNPs, and PSNPs.

**Related Commands**

- **domain-password** Allows you to set the authentication password for a routing domain.
- **isis password** Allows you to configure an authentication password for an interface.

### clear config

Clear IS-IS configurations that display under the `router isis` heading of the `show running-config` command output.

**Syntax**

```
clear config
```
clear isis

Restart the IS-IS process. All IS-IS data is cleared.

Syntax

```
clear isis [tag] {* | database | traffic}
```

Parameters

- `tag` (Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
- `*` Enter the keyword * to clear all IS-IS information and restarts the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation will be done.
- `database` Clears IS-IS LSP database information.
- `traffic` Clears IS-IS counters.

Command Modes

EXEC Privilege

clns host

Define a name-to-network service mapping point (NSAP) mapping that can then be used with commands that require NSAPs and system IDs.

Syntax

```
clns host name nsap
```

Parameters

- `name` Enter an alphanumeric string to identify the name-to-NSAP mapping.
- `nsap` Enter a specific NSAP address that will be associated with the `name` parameter.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Usage Information

Use this command to configure a shortcut name that can used instead of entering a long string of numbers associated with an NSAP address.

Related Commands

- `hostname dynamic` Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostnames in LSPs.

debug isis

Enable debugging for all IS-IS operations.

Syntax

```
debug isis
```

Intermediate System to Intermediate System (IS-IS) | 831
To disable debugging of IS-IS, enter `no debug isis`.

**Command Modes**

EXEC Privilege

**Usage Information**

Entering `debug isis` enables all debugging parameters.

Use this command to display all debugging information in one output. To turn off debugging, you normally enter separate `no` forms of each command. Enter the `no debug isis` command to disable all debug messages for IS-IS at once.

---

**debug isis adj-packets**

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

**Syntax**

`debug isis adj-packets [interface]`

To turn off debugging, use the `no debug isis adj-packets [interface]` command.

**Parameters**

- `interface` (OPTIONAL) Identifies the interface type slot/port as one of the following:
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - S-Series: Range: 1-128
    - E-Series: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes**

EXEC Privilege

---

**debug isis local-updates**

Enables debugging on a specific interface and provides diagnostic information to debug IS-IS local update packets.

**Syntax**

`debug isis local-updates [interface]`

To turn off debugging, enter the `no debug isis local-updates [interface]` command.
Parameters:

- **interface** (OPTIONAL) Identifies the interface type slot/port as one of the following:
  - For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword **sonet** followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
  - For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes:

- EXEC Privilege

**debug isis snp-packets**

Enable debugging on a specific interface and provides diagnostic information to debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets.

Syntax:

```
debug isis snp-packets [interface]
```

Parameters:

- **interface** (OPTIONAL) Identifies the interface type slot/port as one of the following:
  - For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword **sonet** followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
  - For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes:

- EXEC Privilege

**debug isis spf-triggers**

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

Syntax:

```
debug isis spf-triggers
```

Parameters:

**Command Modes**

- EXEC Privilege

To turn off debugging, enter **no debug isis spf-triggers**.
**debug isis update-packets**

Enable debugging on Link State PDUs (LSPs) that are detected by a router.

**Syntax**

```
debug isis update-packets [interface]
```

To turn off debugging, enter the `no debug isis update-packets [interface]` command.

**Parameters**

- `interface` (OPTIONAL) Identifies the interface type slot/port as one of the following:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes**

EXEC Privilege

---

**default-information originate**

Generate a default route into an IS-IS routing domain and controls the distribution of default information.

**Syntax**

```
default-information originate [always] [metric metric] [route-map map-name]
```

To disable the generation of a default route into the specified IS-IS routing domain, enter the `no default-information originate [always] [metric metric] [route-map map-name]` command.

**Parameters**

- `always` (OPTIONAL) Enter the keyword `always` to have the default route always advertised

- `metric metric` (OPTIONAL) Enter the keyword `metric` followed by a number to assign to the route. Range: 0 to 16777215

- `route-map map-name` (OPTIONAL) A default route will be generated by the routing process if the route map is satisfied.

**Defaults**

Not configured.

**Command Modes**

ROUTER ISIS (for IPv4)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Introduced IPv6 ISIS support</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
Usage Information

When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route is advertised depends on how on the configuration of the metric-style command. If the metric-style is set for narrow mode and the metric value in the default-information originate command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the metric-style is set for wide mode, their the metric value in the default-information originate command is advertised.

Related Commands

- redistribute
  - Redistribute routes from one routing domain to another routing domain.
- isis metric
  - Configure a metric for an interface
- metric-style
  - Set the metric style for the router.
- show isis database
  - Display the IS-IS link state database.

---

**description**

Enter a description of the IS-IS routing protocol

**Syntax**

description {description}

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

**Parameters**

description  Enter a description to identify the IS-IS protocol (80 characters maximum).

**Defaults**

No default behavior or values

**Command Modes**

ROUTER ISIS

**Command History**

- pre-7.7.1.0  Introduced

**Related Commands**

- router isis  Enter ROUTER mode on the switch.

---

**distance**

Define the administrative distance for learned routes.

**Syntax**

distance weight [ip-address mask [prefix-list]]

To return to the default values, enter the no distance weight command.
**weight**

The administrative distance value indicates the reliability of a routing information source.

Range: 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.)

Default: 115

**ip-address mask**

(Optional) Enter an IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.

**prefix-list**

(Optional) Enter the name of a prefix list name.

---

**distribute-list in**

Filter network prefixes received in updates.

**Syntax**

distribute-list prefix-list-name in [interface]

To return to the default values, enter the **no distribute-list prefix-list-name in [interface]** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-list-name</td>
<td>Specify the prefix list to filter prefixes in routing updates.</td>
</tr>
<tr>
<td>interface</td>
<td>(OPTIONAL) Identifies the interface type slot/port as one of the following:</td>
</tr>
<tr>
<td></td>
<td>• For 1Gigabit Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <strong>port-channel</strong> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For a SONET interface, enter the keyword <strong>sonet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <strong>TenGigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN, enter the keyword <strong>vlan</strong> followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

ROUTER ISIS (for IPv6)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)
**distribute-list out**

Supress network prefixes from being advertised in outbound updates.

**Syntax**

```
distribute-list prefix-list-name out [connected | bgp as number | ospf process-id | rip | static]
```

To return to the default values, enter the no `distribute-list prefix-list-name out [bgp as number connected | ospf process-id | rip | static]` command.

**Parameters**

- `prefix-list-name`: Specify the prefix list to filter prefixes in routing updates.
- `connected`: (OPTIONAL) Enter the keyword `connected` for directly connected routing process.
- `ospf process-id`: (OPTIONAL) Enter the OSPF process-ID number. Range: 1 to 65535
- `bgp as number`: (OPTIONAL) Enter the BGP followed by the AS Number. Range: 1 to 65535
- `rip`: (OPTIONAL) Enter the keyword `rip` for RIP routes.
- `static`: (OPTIONAL) Enter the keyword `static` for user-configured routing process.

**Defaults**

Not configured.

**Command Modes**

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Usage Information**

You can assign a name to a routing process so a prefix list will be applied to only the routes derived from the specified routing process.

**Related Commands**

- `distribute-list in`: Filters networks received in updates.
- `redistribute`: Redistributes routes from one routing domain to another routing domain.

**distribute-list redistributed-override**

Suppress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.
Syntax  
`distribute-list redistributed-override in`
To return to the default, use the `no distribute-list redistributed-override in` command.

Defaults  
No default behavior or values

Command Modes  
ROUTER ISIS (for IPv4)

COMMAND HISTORY

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version 7.8.1.0</strong></td>
<td>Introduced IPv6 ISIS support</td>
</tr>
<tr>
<td><strong>Version 6.3.1.0</strong></td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information  
When the command is executed, IS-IS will not download the route to the routing table if the same route was redistributed into IS-IS routing protocol on the same router.

**domain-password**

Set the authentication password for a routing domain.

Syntax  
`domain-password [hmac-md5 | encryption-type] password`
To disable the password, enter `no domain-password`.

Parameters  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hmac-md5</code></td>
<td>(OPTIONAL) Enter the keyword <code>hmac-md5</code> to encrypt the password using MD5.</td>
</tr>
<tr>
<td><code>encryption-type</code></td>
<td>(OPTIONAL) Enter 7 to encrypt the password using DES.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Enter an alphanumeric string up to 16 characters long.</td>
</tr>
</tbody>
</table>

Usage Information  
The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands  

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area-password</code></td>
<td>Configure an IS-IS area authentication password.</td>
</tr>
<tr>
<td><code>isis password</code></td>
<td>Configure the authentication password for an interface.</td>
</tr>
</tbody>
</table>

**graceful-restart ietf**

Enable Graceful Restart on an IS-IS router.

Syntax  
`graceful-restart ietf`
To return to the default, use the `no graceful-restart ietf` command.
A Restart TLV included in every Graceful Restart enabled router’s HELLO PDUs. This enables the (re)starting as well as the existing ISIS peers to detect the GR capability of the routers on the connected network. A flag in the Restart TLV contains Restart Request (RR), Restart Acknowledge (RA) and Suppress Adjacency Advertisement (SA) bit flags.

The ISIS Graceful Restart enabled router can co-exist in mixed topologies where some routers are Graceful Restart enabled and others are not. For neighbors that are not Graceful Restart enabled, the restarting router brings up the adjacency per the usual methods.

**graceful-restart interval**

Set the Graceful Restart grace period, the time during which all Graceful Restart attempts are prevented.

**Syntax**

```
graceful-restart interval minutes
```

To return to the default, use the `no graceful-restart interval` command.

**Parameters**

| `minutes` | Range: 1-20 minutes  
| Default: 5 minutes |

**Defaults**

5 minutes

**Command Modes**

ROUTER ISIS

**Command History**

Version 8.3.1.0 Introduced on the E-Series

---

**graceful-restart t1**

Set the Graceful Restart wait time before unacknowledged restart requests are generated. This is the interval before the system sends a Restart Request (an IIH with RR bit set in Restart TLV) until the CSNP is received from the helping router.

**Syntax**

```
graceful-restart t1 {interval seconds | retry-times value}
```

To return to the default, use the `no graceful-restart t1` command.
**graceful-restart t2**

Configure the wait time for the Graceful Restart timer T2 that a restarting router uses as the wait time for each database to synchronize.

**Syntax**

```
graceful-restart t2 {level-1 | level-2} seconds
```

To return to the default, use the `no graceful-restart t2` command.

**Parameters**

- `level-1, level-2` Enter the keyword `level-1` or `level-2` to identify the database instance type to which the wait interval applies.
- `seconds` Range: 5-120 seconds
  Default: 30 seconds

**Defaults**

30 seconds

**Command Modes**

ROUTER ISIS

**Command History**

Version 8.3.1.0 Introduced on the E-Series

---

**graceful-restart t3**

Configure the overall wait time before Graceful Restart is completed.

**Syntax**

```
graceful-restart t3 {adjacency | manual} seconds
```

To return to the default, use the `no graceful-restart t3` command.

---

**Parameters**

- `interval` Enter the keyword `interval` to set the wait time.
  Range: 5-120 seconds
  Default: 5 seconds
- `retry-times` Enter the keyword `retry-times` to set the number of times the request interval is extended until a CSNP is received from the helping router.
  Range: 1-10 attempts
  Default: 1

**Defaults**

see above

**Command Modes**

ROUTER ISIS

**Command History**

Version 8.3.1.0 Introduced on the E-Series
The running router sets remaining time value to the current adjacency hold time. This can be overridden by implementing this command.

Override the default restart-wait time by entering the `no graceful-restart restart-wait` command. When restart-wait is disabled, the current adjacency hold time is used.

Be sure to set the **t3** timer to adjacency on the restarting router when implementing this command. The restarting router gets the remaining time value from its peer and adjusts its T3 value accordingly only when you have configured `graceful-restart t3 adjacency`.

---

**Related Commands**

`graceful-restart restart-wait`  
Enable the Graceful Restart maximum wait time before a restarting peer comes up.

---

**graceful-restart restart-wait**

Enable the Graceful Restart maximum wait time before a restarting peer comes up.

Be sure to set the **t3** timer to adjacency on the restarting router when implementing this command.

**Syntax**

```
graceful-restart restart-wait seconds
```

To return to the default, use the `no graceful-restart restart-wait` command.

**Parameters**

- **seconds**  
  Range: 5-300 seconds  
  Default: 30 seconds

**Defaults**

30 seconds

**Command Modes**

ROUTER ISIS

**Command History**

Version 8.3.1.0  
Introduced on the E-Series

**Related Commands**

- `graceful-restart t3`: Configure the overall wait time before Graceful Restart is completed.
hello padding

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

Syntax

```plaintext
hello padding [multi-point | point-to-point]
```

To return to default, use ```no hello padding [multi-point | point-to-point]```.

Parameters

- **multi-point**: (OPTIONAL) Enter the keyword `multi-point` to pad only LAN hello PDUs.
- **point-to-point**: (OPTIONAL) Enter the keyword `point-to-point` to pad only point-to-point PDUs.

Defaults

Both LAN and point-to-point hello PDUs are padded.

Command Modes

ROUTER ISIS

Usage Information

IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands

- `isis hello padding`: Turn ON or OFF hello padding on an interface basis.

hostname dynamic

Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

Syntax

```plaintext
hostname dynamic
```

To disable this command, enter ```no hostname dynamic```.

Defaults

Enabled.

Command Modes

ROUTER ISIS

Usage Information

Use this command to build name-to-systemID mapping tables through the protocol. All `show` commands that display systems also display the hostname.

Related Commands

- `clns host`: Define a name-to-NSAP mapping.

ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

Syntax

```plaintext
ignore-lsp-errors
```

To return to the default values, enter ```no ignore-lsp-errors```.
In IS-IS, the default deletes LSPs with internal checksum errors (no ignore-lsp-errors).

**Command Modes**

ROUTER ISIS

**Usage Information**

IS-IS normally purges LSPs with an incorrect data link checksum, causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This could cause disruption to your system operation.

**ip router isis**

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

**Syntax**

```
ip router isis [tag]
```

To disable IS-IS on an interface, enter the `no ip router isis [tag]` command.

**Parameters**

- `tag` (OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.

**Defaults**

No processes are configured.

**Command Modes**

INTERFACE

**Command History**

Version 7.5.1.0 Introduced

**Usage Information**

You must use the `net` command to assign a network entity title to enable IS-IS.

**Related Commands**

- `net` Configures an IS-IS network entity title (NET) for the routing process.
- `router isis` Enables the IS-IS routing protocol.

**ipv6 router isis**

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

**Syntax**

```
ipv6 router isis [tag]
```

To disable IS-IS routing, enter `no router isis [tag]`.

**Parameters**

- `tag` (OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.

**Defaults**

Not configured.

**Command Modes**

ROUTER ISIS

**Command History**

Version 7.5.1.0 Introduced on E-Series
Usage Information

You must configure a network entity title (the net command) to specify the area address and the router system ID.

You must enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

Only one IS-IS routing process can be configured to perform Level 2 routing. A level-1-2 designation performs Level 1 and Level 2 routing at the same time.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net</td>
<td>Configure an IS-IS network entity title (NET) for a routing process.</td>
</tr>
<tr>
<td>is-type</td>
<td>Assign a type for a given area.</td>
</tr>
</tbody>
</table>

**isis circuit-type**

Configure the adjacency type on interfaces.

Syntax

```plaintext
isis circuit-type {level-1 | level-1-2 | level-2-only}
```

To return to the default values, enter `no isis circuit-type`.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, then a Level 2 adjacency is established. This is the default.</td>
</tr>
<tr>
<td>level-2-only</td>
<td>You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.</td>
</tr>
</tbody>
</table>

Defaults

level-1-2

Command Modes

INTERFACE

Usage Information

Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system should be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

**isis csnp-interval**

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

Syntax

```plaintext
isis csnp-interval seconds [level-1 | level-2]
```

To return to the default values, enter the `no isis csnp-interval [seconds] [level-1 | level-2]` command.
Parameters

- **seconds**: Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system.
  - Range: 0 to 65535
  - Default: 10

- **level-1**: (OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.

- **level-2**: (OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults

- **seconds** = 10; **level-1** (if not otherwise specified)

Command Modes

- INTERFACE

Usage Information

The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

Level 1 and Level 2 CSNP intervals can be configured independently.

**isis hello-interval**

Specify the length of time between hello packets sent.

Syntax

```
isis hello-interval seconds [level-1 | level-2]
```

To return to the default values, enter the `no isis hello-interval [seconds] [level-1 | level-2]` command.

Parameters

- **seconds**: Allows you to set the length of time between hello packet transmissions.
  - Range: 1 to 65535
  - Default: 10

- **level-1**: (OPTIONAL) Select this value to configure the hello interval for Level 1.
  - This is the default.

- **level-2**: (OPTIONAL) Select this value to configure the hello interval for Level 2.

Defaults

- **seconds** = 10; **level-1** (if not otherwise specified)

Command Modes

- INTERFACE

Usage Information

Hello packets are held for a length of three times the value of the hello interval. Use a high hello interval seconds to conserve bandwidth and CPU usage. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).

Related Commands

- `isis hello-multiplier`: Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.
**isis hello-multiplier**

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

**Syntax**

```
isis hello-multiplier multiplier [level-1 | level-2]
```

To return to the default values, enter `no isis hello-multiplier [multiplier] [level-1 | level-2].`

**Parameters**

- **multiplier**
  - Specifies an integer that sets the multiplier for hello holding time.
  - Never configure a hello-multiplier lower than the default (3).
  - Range: 3 to 1000
  - Default: 3

- **level-1**
  - (OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies.
  - This is the default.

- **level-2**
  - (OPTIONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

**Defaults**

```
multiplier =3; level-1 (if not otherwise specified)
```

**Command Modes**

```
INTERFACE
```

**Usage Information**

The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

**Related Commands**

- `isis hello-interval` Specify the length of time between hello packets.

**isis hello padding**

Turn ON or OFF padding of hello PDUs from the interface mode.

**Syntax**

```
isis hello padding
```

To return to the default, use the `no isis hello padding`.

**Defaults**

Padding of hello PDUs is enabled (ON).

**Command Modes**

```
INTERFACE
```

**Usage Information**

Hello PDUs are “padded” only when both the global and interface padding options are ON. Turning either one OFF will disable padding for the corresponding interface(s).

**Related Commands**

- `hello padding` Turn ON or OFF padding for LAN and point-to-point hello PDUs.
**isis ipv6 metric**

Assign metric to an interface for use with IPv6 information.

**Syntax**

```plaintext
isis ipv6 metric defaul\-metric [level-1 | level-2]
```

To return to the default values, enter `no ipv6 isis metric [default-metric] [level-1 | level-2]` command.

**Parameters**

- **default-metric**
  - Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations.
  - You can configure this metric for Level 1 or Level 2 routing.
  - Range: 0 to 16777215
  - Default: 10

- **level-1**
  - (OPTIONAL) Enter `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing.
  - This is the default.

- **level-2**
  - (OPTIONAL) Enter `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

**Defaults**

```
default-metric = 10; level-1 (if not otherwise specified)
```

**Command Modes**

`INTERFACE`

**Command History**

- `Version 7.5.1.0` Introduced on E-Series

**Usage Information**

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

**isis metric**

Assign a metric to an interface.

**Syntax**

```plaintext
isis metric defaul\-metric [level-1 | level-2]
```

To return to the default values, enter `no isis metric [default-metric] [level-1 | level-2]`.

**Parameters**

- **default-metric**
  - Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations.
  - You can configure this metric for Level 1 or Level 2 routing.
  - Range: 0 to 63 for narrow and transition metric styles; 0 to 16777215 for wide metric styles.
  - Default: 10

- **level-1**
  - (OPTIONAL) Enter `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing.
  - This is the default.

- **level-2**
  - (OPTIONAL) Enter `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

**Defaults**

```
default-metric = 10; level-1 (if not otherwise specified)
```
isis network point-to-point

Enable the software to treat a broadcast interface as a point-to-point interface.

Syntax  

`isis network point-to-point`

To disable the feature, enter `no isis network point-to-point`.

Defaults

Not enabled.

Command Modes

INTERFACE

Usage Information

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis password

Configure an authentication password for an interface.

Syntax

`isis password [hmac-md5] password [level-1 | level-2]`

To delete a password, enter the `no isis password [password] [level-1 | level-2]` command.

Parameters

- `encryption-type`
  - (OPTIONAL) Enter 7 to encrypt the password using DES.
- `hmac-md5`
  - (OPTIONAL) Enter the keyword `hmac-md5` to encrypt the password using MD5.
- `password`
  - Assign the interface authentication password.
- `level-1`
  - (OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This is the default.
- `level-2`
  - (OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

Defaults

No default password. `level-1` (if not otherwise specified)

Command Modes

INTERFACE

Usage Information

To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the `level-1` and `level-2` keywords.

The `no` form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords `level-1` or `level-2`.

This password provides limited security as it is processed as plain text.
### isis priority

Set priority of the designated router you select.

**Syntax**

```plaintext
isis priority value [level-1 | level-2]
```

To return to the default values, enter the `no isis priority [value] [level-1 | level-2]` command.

**Parameters**

- **value**
  - This value sets the router priority. The higher the value, the higher the priority.
  - Range: 0 to 127
  - Default: 64

- **level-1** (OPTIONAL)
  - Specify the priority for Level 1.
  - This is the default.

- **level-2** (OPTIONAL)
  - Specify the priority for Level 2.

**Defaults**

- `value` = 64; `level-1` (if not otherwise specified)

**Command Modes**

- INTERFACE

**Usage Information**

You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN will be the designated router. Priorities are advertised within hellos. The router with the highest priority will become the designated intermediate system (DIS).

*Routers with a priority of 0 cannot be a designated router.* Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address will become DIS even though its priority is 0.

### is-type

Configure IS-IS operating level for a router.

**Syntax**

```plaintext
is-type {level-1 | level-1-2 | level-2-only}
```

To return to the default values, enter `no is-type`.

**Parameters**

- **level-1**
  - Allows a router to act as a Level 1 router.

- **level-1-2**
  - Allows a router to act as both a Level 1 and Level 2 router.
  - This is the default.

- **level-2-only**
  - Allows a router to act as a Level 2 router.

**Defaults**

- `level-1-2`

**Command Modes**

- ROUTER ISIS

**Usage Information**

The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. The IS type can be configured as Level 1.
log-adjacency-changes

Generate a log messages for adjacency state changes.

Syntax

```
log-adjacency-changes
```

To disable this function, enter `no log-adjacency-changes`.

Defaults

Adjacency changes are not logged.

Command Modes

ROUTER ISIS

Usage Information

This command enables you to monitor adjacency state changes, which is useful when you monitor large networks. Messages are logged in the system error message facility.

lsp-gen-interval

Set the minimum interval between successive generations of link-state packets (LSPs).

Syntax

```
lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the `no lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

Parameters

- **level-1**
  - (OPTIONAL) Enter the keyword `level-1` to apply the configuration to generation of Level-1 LSPs.
- **level-2**
  - (OPTIONAL) Enter the keyword `level-2` to apply the configuration to generation of Level-2 LSPs.
- **interval seconds**
  - Enter the maximum number of seconds between LSP generations.
    - Range: 0 to 120 seconds
    - Default: 5 seconds
- **initial_wait_interval seconds**
  - (OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation.
    - Range: 0 to 120 seconds
    - Default: 1 second
- **second_wait_interval seconds**
  - (OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation.
    - Range: 0 to 120 seconds
    - Default: 5 seconds

Defaults

Defaults as above

Command Modes

ROUTER ISIS

Command History

- **Version 7.5.1.0**
  - Expanded to support LSP Throttling Enhancement
**Usage Information**

LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (interval seconds). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

**lsp-mtu**

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs generated by this router.

**Syntax**

```
lsp-mtu size
```

To return to the default values, enter `no lsp-mtu`.

**Parameters**

- `size` 
  - The maximum LSP size, in bytes.
  - Range: 128 to 1497 for non-jumbo mode; 128 to 9195 for jumbo mode.
  - Default: 1497

**Defaults**

1497 bytes

**Command Modes**

ROUTER ISIS

**Command History**

Version 7.5.1.0 Expanded to support LSP Throttling Enhancement

**Usage Information**

The link MTU (mtu command) and the LSP MTU size must be the same.

Since each device can generate a maximum of 255 LSPs, consider carefully whether the `lsp-mtu` command should be configured.

**lsp-refresh-interval**

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their max-lsp-lifetime reaches zero and then LSPs will be purged.

**Syntax**

```
lsp-refresh-interval seconds
```

To restore the default refresh interval, enter `no lsp-refresh-interval`.

**Parameters**

- `seconds` 
  - The LSP refresh interval, in seconds. This value has to be less than the seconds value specified with the max-lsp-lifetime command.
  - Range: 1 to 65535 seconds.
  - Default: 900
Defaults 900 seconds

Command Modes ROUTER ISIS

Command History

| Version 7.5.1.0 | Expanded to support LSP Throttling Enhancement |

Usage Information

The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the max-lsp-lifetime command.

A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization caused by the flooding of refreshed packets.

Related Commands

max-lsp-lifetime Sets the maximum interval that LSPs persist without being refreshed

max-area-addresses

Configure manual area addresses.

Syntax max-area-addresses number

To return to the default values, enter no max-area-addresses.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Set the maximum number of manual area addresses. Range: 3 to 6. Default: 3</td>
</tr>
</tbody>
</table>

Defaults

3 addresses

Command Modes ROUTER ISIS

Usage Information

Use this command to configure the number of area addresses on router. This value should be consistent with routers in the same area, or else, the router will form only Level 2 adjacencies. The value should be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

Syntax max-lsp-lifetime seconds

To restore the default time, enter no max-lsp-lifetime.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>The maximum lifetime of LSP in seconds. This value must be greater than the lsp-refresh-interval. The higher the value the longer the LSPs are kept. Range: 1 to 65535 Default: 1200</td>
</tr>
</tbody>
</table>
### Defaults

| Command Modes | ROUTER ISIS |

### Usage Information

| Command | 1200 seconds |

| Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval. |

| The seconds parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links. |

### Related Commands

| Command | lsp-refresh-interval |

| Use this command to set the link-state packet (LSP) refresh interval. |

---

**maximum-paths**

**Syntax**

maximum-paths number

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. Range: 1 to 16. Default: 4</td>
</tr>
</tbody>
</table>

| Defaults | 4 |

| Command Mode | ROUTER ISIS (for IPv4) |

| Command Mode | CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6) |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Introduced MT ISIS support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced MT ISIS support</td>
</tr>
<tr>
<td>Version 6.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

---

**metric-style**

| Syntax | metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2] |

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>narrow</td>
<td>Allows you to configure the E-Series to generate and accept old-style TLVs. Metric range: 0 to 63</td>
</tr>
<tr>
<td>transition</td>
<td>Allows you to configure the E-Series to generate both old-style and new-style TLVs. Metric range: 0 to 63</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Introduced MT ISIS support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced MT ISIS support</td>
</tr>
<tr>
<td>Version 6.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
**Command Modes**

ROUTER ISIS

**Usage Information**

If you enter the **metric-style wide** command, the Dell Networking OS generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs.

The new-style TLVs have wider metric fields than old-style TLVs.

**Related Commands**

- **isis metric**
  
  Use this command to configure a metric for an interface.

---

**multi-topology**

Enables Multi-Topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

**Syntax**

```
multi-topology [transition]
```

To return to a single topology configuration, enter **no multi-topology [transition]**.

**Parameters**

transition

**Defaults**

Disabled

**Command Modes**

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

**Command History**

Version 7.8.1.0 Introduced

---

**net**

Use this mandatory command to configure an IS-IS network entity title (NET) for a routing process. If a NET is not configured, the IS-IS process will not start.

**Syntax**

```
net network-entity-title
```

To remove a net, enter **no net network-entity-title**.

**Parameters**

- **network-entity-title**
  
  Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.
Defaults
Not configured.

Command Modes
ROUTER ISIS

passive-interface

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

Syntax
passive-interface interface

To delete a passive interface configuration, enter the no passive-interface interface command.

Parameters
- **interface**: Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For Loopback interface, enter the keyword loopback followed by a number from zero (0) to 16383.
  - For a Port Channel interface, enter the keyword port-channel followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword sonet followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

Defaults
Not configured.

Command Modes
ROUTER ISIS

Usage Information
Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in IS-IS updates sent via other interfaces.

redistribute

Redistribute routes from one routing domain to another routing domain.

Syntax
redistribute {static | connected | rip} [level-1 | level-1-2 | level-2] [metric metric-value] [metric-type {external | internal}] [route-map map-name]

To end redistribution or disable any of the specified keywords, enter the no redistribute {static | connected | rip} [metric metric-value] [metric-type {external | internal}] [level-1 | level-1-2 | level-2] [route-map map-name] command.

Parameters
- **connected**: Enter the keyword connected to redistribute active routes into IS-IS.
- **rip**: Enter the keyword rip to redistribute RIP routes into IS-IS.
- **static**: Enter the keyword static to redistribute user-configured routes into IS-IS.
To redistribute a default route (0.0.0.0/0), configure the `default-information originate` command.

Changing or disabling a keyword in this command will not affect the state of the other command keywords.

When an LSP with an internal metric is received, the FTOS considers the route cost taking into consideration the advertised cost to reach the destination.

Redistributed routing information is filtered with the `distribute-list out` command to ensure that the routes are properly passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for narrow or transition mode and the metric value in the `redistribute` command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the `metric-style` command is set for wide mode, the metric value in the `redistribute` command is advertised.

### Defaults

- **metric** `metric-value` *(OPTIONAL)* Assign a value to the redistributed route.
  - Range: 0 to 16777215
  - Default: 0. You should use a value that is consistent with the destination protocol.

- **metric-type** *(OPTIONAL)* The external link type associated with the default route advertised into a routing domain. You must specify one of the following:
  - `external`
  - `internal`

- **level-1** *(OPTIONAL)* Routes are independently redistributed into IS-IS as Level 1 routes.

- **level-1-2** *(OPTIONAL)* Routes are independently redistributed into IS-IS as Level-1-2 routes.

- **level-2** *(OPTIONAL)* Routes are independently redistributed into IS-IS as Level 2 routes. This is the default.

- **route-map** `map-name` *(OPTIONAL)* If the `route-map` argument is not entered, all routes are redistributed. If a `map-name` value is not specified, then no routers are imported.

### Command Modes

**ROUTER ISIS** *(for IPv4)*

**CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6** *(for IPv6)*

### Command History

- **Version 7.5.1.0** Introduced IPv6 ISIS support
- **Version 6.3.1.0** Introduced

### Usage Information

To redistribute a default route (0.0.0.0/0), configure the `default-information originate` command.

Changing or disabling a keyword in this command will not affect the state of the other command keywords.

When an LSP with an internal metric is received, the FTOS considers the route cost taking into consideration the advertised cost to reach the destination.

Redistributed routing information is filtered with the `distribute-list out` command to ensure that the routes are properly passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for narrow or transition mode and the metric value in the `redistribute` command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the `metric-style` command is set for wide mode, the metric value in the `redistribute` command is advertised.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-information originate</code></td>
<td>Generate a default route for the IS-IS domain.</td>
</tr>
<tr>
<td><code>distribute-list out</code></td>
<td>Suppress networks from being advertised in updates. Redistributed routing information is filtered by this command.</td>
</tr>
</tbody>
</table>
Redistribute routing information from a BGP process. (new command in Release 6.3.1)

**Syntax**

```
redistribute bgp AS number [level-1] [level-1-2] [level-2] [metric metric-value] [metric-type {external | internal}] [route-map map-name]
```

To return to the default values, enter the no redistribute bgp command with the appropriate parameters.

**Parameters**

- **AS number**
  - Enter a number that corresponds to the Autonomous System number.
  - Range: 1 to 65535

- **level-1**
  - (OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only

- **level-1-2**
  - (OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.

- **level-2**
  - (OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only.
  - This is the default.

- **metric metric-value**
  - (OPTIONAL) The value used for the redistributed route. You should use a metric value that is consistent with the destination protocol.
  - Range: 0 to 16777215
  - Default: 0.

- **metric-type {external | internal}**
  - (OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are:
    - external
    - internal

- **route-map map-name**
  - map-name is an identifier for a configured route map.
  - The route map should filter imported routes from the source routing protocol to the current routing protocol.
  - If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.

**Defaults**

IS-IS Level 2 routes only

**Command Modes**

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Example**

```
FTOS(conf-router_isis)#router is
FTOS(conf-router_isis)#redistribute bgp 1 level-1 metric 32 metric-type external
route-map rmap-isis-to-bgp
FTOS(conf-router_bgp)#show running-config isis

    !
    router is
    redistribute bgp 1 level-1 metric 32 metric-type external route-map rmap-isis-to-bgp
```

**Command History**

- Version 7.5.1.0 Introduced IPv6 ISIS support
- Version 6.3.1.0 Introduced
BGP to IS-IS redistribution supports “match” options using route maps. The metric value, level, and metric-type of redistributed routes can be set by the redistribution command. More advanced “set” options can be performed using route maps.

**redistribute ospf**

Redistribute routing information from an OSPF process.

**Syntax**

```plaintext
redistribute ospf process-id [level-1 | level-1-2 | level-2] [match {internal | external}] [metric metric-value] [metric-type {external | internal}] [route-map map-name]
```

To return to the default values, enter the `no redistribute ospf process-id [level-1 | level-1-2 | level-2] [match {internal | external}] [metric metric-value] [metric-type {external | internal}] [route-map map-name]` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter a number that corresponds to the OSPF process ID to be redistributed. Range: 1 to 65535</td>
</tr>
<tr>
<td>metric metric-value</td>
<td>(OPTIONAL) The value used for the redistributed route. You should use a metric value that is consistent with the destination protocol. Range: 0 to 16777215 Default: 0.</td>
</tr>
</tbody>
</table>
| metric-type {external | internal}                                   | (OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are:  
• external  
• internal |
| level-1             | (OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.                                                                 |
| level-1-2           | (OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.                                                            |
| level-2             | (OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This is the default.                                            |
| match {external | internal}                                   | (OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are  
• internal  
• external |
| route-map map-name  | `map-name` is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol.  
If you do not specify a `map-name`, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported. |

**Defaults**

As above

**Command Modes**

`ROUTER ISIS (for IPv4)`

`CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)`
How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for narrow mode and the metric value in the `redistribute ospf` command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the `metric-style` command is set for wide mode, an the metric value in the `redistribute ospf` command is advertised.

**set-overload-bit**

Configure the router to set the overload bit in its non-pseudonode LSPs. This prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

**Syntax**

```
set-overload-bit
```

To return to the default values, enter `no set-overload-bit`.

**Defaults**

Not set.
show config

Display the changes you made to the IS-IS configuration. Default values are not shown.

Syntax

```
show config
```

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Examples

**Figure 28-2. Command Example: show config (router-isis mode)**

```
FTOS(conf-router_isis)#show config
! router isis
  clns host ISIS 49.0000.0001.F100.E120.0013.00
  log-adjacency-changes
  net 49.0000.0001.F100.E120.0013.00
  !
  address-family ipv6 unicast
   maximum-paths 16
   multi-topology transition Identifies that Multi-Topology IS-IS is enabled in transition
   set-overload-bit
   spf-interval level-1 100 15 20
   spf-interval level-2 120 20 25
   exit-address-family
```

**Figure 28-3. Command Example: show config (address-family-ipv6 mode)**

```
FTOS(conf-router_isis-af_ipv6)#show conf
!
  address-family ipv6 unicast
  maximum-paths 16
  multi-topology transition Identifies that Multi-Topology
  set-overload-bit IS-IS is enabled in transition
  spf-interval level-1 100 15 20
  spf-interval level-2 120 20 25
  exit-address-family
```

show isis database

Display the IS-IS link state database.

Syntax

```
show isis database [level-1 | level-2] [local] [detail | summary] [Lspid]
```
Intermediate System to Intermediate System (IS-IS) | 861

**Parameters**

- **level-1** (OPTIONAL) Displays the Level 1 IS-IS link-state database.
- **level-2** (OPTIONAL) Displays the Level 2 IS-IS link-state database.
- **local** (OPTIONAL) Displays local link-state database information.
- **detail** (OPTIONAL) Displays detailed link-state database information of each LSP when specified. If not specified, a summary displays.
- **summary** (OPTIONAL) Displays summary of link-state database information when specified.
- **lspid** (OPTIONAL) Displays only the specified LSP.

**Command Modes**

- EXEC
- EXEC Privilege

**Example**

**Figure 28-4. Command Example: show isis database**

FTOS#show isis database

**IS-IS Level-1 Link State Database**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISIS.00-00</td>
<td>* 0x00000006</td>
<td>0xCF43</td>
<td>580</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

**IS-IS Level-2 Link State Database**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISIS.00-00</td>
<td>* 0x00000006</td>
<td>0xCF43</td>
<td>580</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

! FTOS#show isis database detail ISIS.00-00

**IS-IS Level-1 Link State Database**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISIS.00-00</td>
<td>* 0x00000002B</td>
<td>0x853B</td>
<td>1075</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

Area Address: 49.0000.0001
NLSPID: 0xCC 0x8E
IP Address: 10.1.1.1
IPv6 Address: 1011::1
Topology: IPv4 (0x00) IPv6 (0x8002)
Metric: 10 IS OSPF.00
Metric: 10 IS (MT-IPv6) OSPF.00
Metric: 10 IP 15.1.1.0 255.255.255.0
Metric: 10 IPv6 (MT-IPv6) 1511::/64
Metric: 10 IPv6 (MT-IPv6) 2511::/64
Metric: 10 IPv6 1011::/64
Metric: 10 IP 10.1.1.0 255.255.255.0
Hostname: ISIS

**IS-IS Level-2 Link State Database**

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISIS.00-00</td>
<td>* 0x00000002D</td>
<td>0xB2CD</td>
<td>1075</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

Area Address: 49.0000.0001
NLSPID: 0xCC 0x8E
IP Address: 10.1.1.1
IPv6 Address: 1011::1
Topology: IPv4 (0x00) IPv6 (0x8002)
Metric: 10 IS OSPF.00
Metric: 10 IS (MT-IPv6) OSPF.00
Metric: 10 IP 10.1.1.0 255.255.255.0
Metric: 10 IP 15.1.1.0 255.255.255.0
Metric: 20 IP 10.3.3.0 255.255.255.0
Metric: 10 IPv6 (MT-IPv6) 1011::/64
Metric: 10 IPv6 (MT-IPv6) 1511::/64
Metric: 10 IPv6 (MT-IPv6) 2511::/64
Metric: 20 IPv6 (MT-IPv6) 1033::/64
Metric: 10 IPv6 2511::/64
Metric: 20 IPv6 1033::/64
Hostname: ISIS

FTOS#
Table 28-1. Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| IS-IS Level-1/Level-2 Link State Database | Displays the IS-IS link state database for Level 1 or Level 2.  
LSPID | Displays the LSP identifier. The first six octets are the System ID of the originating router. The next octet is the pseudonode ID. If this byte is not zero, then the LSP describes system links. If this byte is zero (0), then the LSP describes the state of the originating router. The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems. The last octet is the LSP number. An LSP will be divided into multiple LSP fragments if there is more data than cannot fit in a single LSP. Each fragment has a unique LSP number. An * after the LSPID indicates that an LSP was originated by the system where this command was issued. |
| LSP Seq Num                | This value is the sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.  
LSP Checksum                | This is the checksum of the entire LSP packet.  
LSP Holdtime                | This value is the amount of time, in seconds, that the LSP remains valid. A zero holdtime indicates that this is a purged LSP and is being removed from the link state database. A value between brackets indicates the duration that the purged LSP stays in the database before being removed.  
ATT                         | This value represents the Attach bit. This indicates that the router is a Level 2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point a default route to the closest Level 2 router.  
P                           | This value represents the P bit. This bit will always set be zero as Dell Force10 does not support area partition repair.  
OL                          | This value represents the overload bit, determining congestion. If the overload bit is set, other routers will not use this system as a transit router when calculating routes. |

show isis graceful-restart detail

Display detailed IS-IS Graceful Restart related settings.

**Syntax**

show isis graceful-restart detail

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.3.1.0 Introduced on the E-Series
Example Figure 28-5. Command Example: show isis graceful-restart detail

```
FTOS#show isis graceful-restart detail
Configured Timer Value
----------------------------
Graceful Restart : Enabled
T3 Timer : Manual
T3 Timeout Value : 30
T2 Timeout Value : 30 (level-1), 30 (level-2)
T1 Timeout Value : 5, retry count: 1
Adjacency wait time : 30

Operational Timer Value
----------------------------
Current Mode/State : Normal/RUNNING
T3 Time left : 0
T2 Time left : 0 (level-1), 0 (level-2)
Restart ACK rcv count : 0 (level-1), 0 (level-2)
Restart Req rcv count : 0 (level-1), 0 (level-2)
Suppress Adj rcv count : 0 (level-1), 0 (level-2)
Restart CSNP rcv count : 0 (level-1), 0 (level-2)
Database Sync count : 0 (level-1), 0 (level-2)
```

FTOS#

**show isis hostname**

Display IS-IS host names configured or learned on the E-Series.

**Syntax**

```
show isis hostname
```

**Command Modes**

EXEC

EXEC Privilege

**Example** Figure 28-6. Command Example: show isis hostname

```
FTOS#show isis hostname
System Id       Dynamic Name   Static Name
*F100.E120.0013 Dell Networking OS       ISIS
```

FTOS#

**show isis interface**

Display detailed IS-IS interface status and configuration information.

**Syntax**

```
show isis interface [interface]
```
show isis neighbors

Display information about neighboring (adjacent) routers.

**Syntax**

```
show isis neighbors [level-1 | level-2] [detail] [interface]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>(OPTIONAL) Displays information about Level 1 IS-IS neighbors.</td>
</tr>
<tr>
<td>level-2</td>
<td>(OPTIONAL) Displays information about Level 2 IS-IS neighbors.</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS>show isis int
GigabitEthernet 0/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
  Circuit Type: Level-1-2
  Interface Index 37847070, Local circuit ID 1
  Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
  Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
  Number of active level-1 adjacencies: 1
  Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
  Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
  Number of active level-2 adjacencies: 1
  Next IS-IS LAN Level-1 Hello in 2 seconds
  Next IS-IS LAN Level-2 Hello in 1 seconds
  LSP Interval: 33

GigabitEthernet 0/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
  Circuit Type: Level-1-2
  Interface Index 38371358, Local circuit ID 2
  Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
  Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
  Number of active level-1 adjacencies: 1
  Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
  Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
```

```
--More--
```
**detail**  
(Optional) Displays detailed information about neighbors.

**interface**  
(Optional) Identifies the interface type slot/port as one of the following:
- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - **C-Series** and **S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes**  
EXEC

EXEC Privilege

**Example**  
**Figure 28-8. Command Example: show isis neighbors**

```plaintext
FTOS#show isis neighbors  
System Id     Interface State     Type    Priority Uptime      Circuit Id  
TEST Gi 7/1    Up                  L1L2(M)   127    09:28:01    TEST.02

FTOS#show isis neighbors detail  
System Id     Interface State     Type    Priority Uptime      Circuit Id  
TEST Gi 7/1    Up                  L1L2(M)   127    09:28:04    TEST.02  
Area Address(es): 49.0000.0001
IP Address(es): 25.1.1.3*
MAC Address: 0000.0000.0000
Hold Time: 28
Link Local Address: fe80::201:e8ff:fe00:492c
Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
Adjacency being used for MTs: IPv4 IPv6

Identified Multi-Topology ISIS enabled
FTOS#
```

**Table 28-2. show isis neighbors Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>The value that identifies a system in an area.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface, slot, and port in which the router was discovered.</td>
</tr>
<tr>
<td>State</td>
<td>The value providing status about the adjacency state. The valid values are Up</td>
</tr>
<tr>
<td></td>
<td>and Init.</td>
</tr>
<tr>
<td>Type</td>
<td>This value displays the adjacency type (Layer 2, Layer 2 or both).</td>
</tr>
<tr>
<td>Priority</td>
<td>IS-IS priority advertised by the neighbor. The neighbor with highest priority</td>
</tr>
<tr>
<td></td>
<td>becomes the designated router for the interface.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Displays the interfaces uptime.</td>
</tr>
<tr>
<td>Circuit Id</td>
<td>The neighbor’s interpretation of the designated router for the interface.</td>
</tr>
</tbody>
</table>

**Usage Information**  
Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the `show isis neighbors` command.
show isis protocol

Display IS-IS routing information.

**Syntax**

```
show isis protocol
```

**Command Modes**

EXEC

EXEC Privilege

**Example**

Figure 28-9. Command Example: show isis protocol

```text
FTOS#show isis protocol
IS-IS Router: <Null Tag>  
System Id: F100.E120.0013  IS-Type: level-1-2  
Manual area address(es):  
49.0000.0001
Routing for area address(es):  
49.0000.0001
   Interfaces supported by IS-IS:  
   GigabitEthernet 1/0 - IP - IPv6  
   GigabitEthernet 1/1 - IP - IPv6  
   GigabitEthernet 1/10 - IP - IPv6  
   Loopback 0 - IP - IPv6
Redistributing:  
Distance: 115
Generate narrow metrics: level-1-2
Accept narrow metrics: level-1-2
Generate wide metrics: none
Accept wide metrics: none
Multi Topology Routing is enabled in transition mode.
FTOS#
```

show isis traffic

This command enables you to display IS-IS traffic interface information.

**Syntax**

```
show isis traffic [interface]
```

**Parameters**

`interface`  
(OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - **C-Series** and **S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes**

EXEC

EXEC Privilege
Example

Figure 28-10. Command Example: show isis traffic

FTOS#show isis traffic
IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
IS-IS: PTP Hellos (sent/rcvd) : 0/0
IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
IS-IS: Level-1 DR Elections : 4
IS-IS: Level-2 DR Elections : 4
IS-IS: Level-1 SPF Calculations : 0
IS-IS: Level-2 SPF Calculations : 389
IS-IS: LSP checksum errors received : 0
IS-IS: LSP authentication failures : 0
FTOS#

Table 28-3. Command Example Fields

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level-1/Level-2 Hellos (sent/rcvd)</td>
<td>Displays the number of Hello packets sent and received.</td>
</tr>
<tr>
<td>PTP Hellos (sent/rcvd)</td>
<td>Displays the number of point-to-point Hellos sent and received.</td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs sourced</td>
<td>Displays the number of new and refreshed LSPs.</td>
</tr>
<tr>
<td>(new/refresh)</td>
<td></td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs flooded</td>
<td>Displays the number of flooded LSPs sent and received.</td>
</tr>
<tr>
<td>(sent/rcvd)</td>
<td></td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs CSNPs (sent/rcvd)</td>
<td>Displays the number of CSNP LSPs sent and received.</td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs PSNPs (sent/rcvd)</td>
<td>Displays the number of PSNP LSPs sent and received.</td>
</tr>
<tr>
<td>Level-1/Level-2 DR Elections</td>
<td>Displays the number of times designated router elections ran.</td>
</tr>
<tr>
<td>Level-1/Level-2 SPF Calculations</td>
<td>Displays the number of shortest path first calculations.</td>
</tr>
<tr>
<td>LSP checksum errors received</td>
<td>Displays the number of checksum errors LSPs received.</td>
</tr>
<tr>
<td>LSP authentication failures</td>
<td>Displays the number of LSP authentication failures.</td>
</tr>
</tbody>
</table>

**spf-interval**

Specify the minimum interval between Shortest Path First (SPF) calculations.

**Syntax**

`spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds] [second_wait_interval seconds]`

To restore default values, use the `no spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds] [second_wait_interval seconds]` command.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>level-l</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>level-l</strong> to apply the configuration to Level-1 SPF calculations.</td>
</tr>
<tr>
<td><strong>level-2</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>level-2</strong> to apply the configuration to Level-2 SPF calculations.</td>
</tr>
<tr>
<td><strong>interval seconds</strong></td>
<td>Enter the maximum number of seconds between SPF calculations.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 120 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 10 seconds</td>
</tr>
<tr>
<td><strong>initial_wait_interval</strong></td>
<td>(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 120 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 5 second</td>
</tr>
<tr>
<td><strong>second_wait_interval</strong></td>
<td>(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 120 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: 5 seconds</td>
</tr>
</tbody>
</table>

### Defaults

Defaults as above

### Command Modes

- **ROUTER ISIS (for IPv4)**
- **CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)**

### Command History

- **Version 7.8.1.0** Introduced to support MT ISIS
- **Version 7.5.1.0** Expanded to support SPF Throttling Enhancement

### Usage Information

This command **spf-interval** in **CONFIG-ROUTER-ISIS-AF-IPV6** mode is used for IPv6 Multi-Topology route computation only. If using single topology mode, use the **spf-interval** command in **CONFIG-ROUTER-ISIS** mode for both IPv4 and IPv6 route computations.

SPF throttling slows down the frequency at which route calculation are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (**interval seconds**). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).
Link Aggregation Control Protocol (LACP)

Overview

This chapter contains commands for Dell Networking’s implementation of Link Aggregation Control Protocol (LACP) for the creation of dynamic link aggregation groups (LAGs — called port-channels in Dell Networking OS parlance). For static LAG commands, see 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 in this chapter generally are supported on all three Dell Networking platforms — C-Series, E-Series, and S-Series — as indicated by the following symbols under command headings: C E S

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

In addition, an Dell Networking OS option provides hitless dynamic LACP states (no noticeable impact to dynamic LACP states after an RPM failover) on E-Series. See redundancy protocol in the High Availability chapter.

clear lacp counters

Clear Port Channel counters.

**Syntax**

```
clear lacp [port-channel-number] counters
```

**Parameters**

- `port-channel-number` Enter a port-channel number:
  - **C-Series and S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
**Defaults**
Without a Port Channel specified, the command clears all Port Channel counters.

**Command Modes**
EXEC
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**
- `show lacp` Display the lacp configuration

---

**debug lacp**

**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** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port 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**
This command has no default values or behavior

**Command Modes**
EXEC
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code></td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
</tbody>
</table>
lACP long-timeout

Configures 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

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

Related Commands

- `show lACP` — Display the lACP configuration

lACP port-priority

Configures 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

- `priority-value` — Enter the port-priority value. The higher the value number the lower the priority.
  
  Range: 1 to 65535
  
  Default: 32768

Defaults

32768

Command Modes

INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
**lacr system-priority**

Configure the LACP system priority.

**Syntax**

```
lacp system-priority priority-value
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-value</td>
<td>Enter the system-priority value. The higher the value, the lower the priority.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 65535</td>
</tr>
<tr>
<td></td>
<td>Default: 32768</td>
</tr>
</tbody>
</table>

**Defaults**

32768

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**port-channel mode**

Configure the LACP port channel mode.

**Syntax**

```
port-channel number mode [active] [passive] [off]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the keyword <code>port-channel</code> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td>active</td>
<td>Enter the keyword <code>active</code> to set the mode to the active state.*</td>
</tr>
<tr>
<td>passive</td>
<td>Enter the keyword <code>passive</code> to set the mode to the passive state.*</td>
</tr>
<tr>
<td>off</td>
<td>Enter the keyword <code>off</code> to set the mode to the off state.*</td>
</tr>
</tbody>
</table>

* The LACP modes are defined in the table below.

**Defaults**

off

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

The LACP modes are defined in the following table.
Table 29-1. LACP Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.</td>
</tr>
<tr>
<td>passive</td>
<td>An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets.</td>
</tr>
<tr>
<td>off</td>
<td>An interface can not be part of a dynamic port channel in the off mode. LACP will not run on a port configured in the off mode.</td>
</tr>
</tbody>
</table>

```
port-channel-protocol lacp
```

Enable LACP on any LAN port.

Syntax:

```
port-channel-protocol lacp
```

To disable LACP on a LAN port, use the `no port-channel-protocol lacp` command.

Command Modes:

```
INTERFACE
```

Command History:

```
Version 6.2.1.1 Introduced
```

Related Commands:

```
show lacp Display the LACP information.
show interfaces port-channel Display information on configured Port Channel groups.
```

```
show lacp
```

Display the LACP matrix.

Syntax:

```
show lacp port-channel-number [sys-id | counters]
```

Parameters:

- `port-channel-number` Enter a port-channel number:
  - **C-Series and S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- `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 7.6.1.0 Support added for S-Series
```
Example 1  Figure 29-1.  show lacp port-channel-number command

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 Gi 10/6 is enabled, LACP is enabled and mode is lacp
Actor   Oper: State ACENHJLMP Key 1      Priority 128
        Admin: State ACEGIKNP Key 1      Priority 128
Partner Oper: State BCEGIKNP Key 1      Priority 128
        Admin: State BDHFLJMP Key 0      Priority 0
FTOS#

Example 2  Figure 29-2.  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 29-3.  show lacp counter command Example

FTOS#show lacp 1 counters
LACP PDU          Marker PDU          Unknown Illegal
<table>
<thead>
<tr>
<th>Port</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Pkts Rx</th>
<th>Pkts Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 10/6</td>
<td>200</td>
<td>200</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
FTOS#

clear lacp counters Clear the LACP counters.
show interfaces port-channel Display information on configured Port Channel groups.

Related Commands

Version 7.5.1.0 Support added for C-Series
Version 6.2.1.1 Introduced
Layer 2

Overview

This chapter describes commands to configure Layer 2 features. It contains the following sections:

- MAC Addressing Commands
- Virtual LAN (VLAN) Commands

Some MAC addressing commands are supported only on the E-Series, some on all three Dell Networking platforms and some on two Dell Networking platforms. Support is indicated by these characters, where appropriate, under each command heading: c e s

The VLAN commands are supported on all three Dell Networking platforms — c e s

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses:

- clear mac-address-table dynamic
- mac accounting destination
- mac-address-table aging-time
- mac-address-table static
- mac-address-table station-move threshold
- mac-address-table station-move time-interval
- mac-address-table station-move refresh-arp
- mac cam fib-partition
- mac learning-limit
- mac learning-limit learn-limit-violation
- mac learning-limit station-move-violation
- mac learning-limit reset
- show cam mac linecard (count)
- show cam maccheck linecard
- show cam mac linecard (dynamic or static)
- show cam mac stack-unit
- show mac-address-table
- show mac-address-table aging-time
- show mac accounting destination
- show mac cam
clear mac-address-table dynamic

Clear the MAC address table of all MAC address learned dynamically.

Syntax

clear mac-address-table dynamic {address mac-address | all | interface interface | vlan vlan-id}

Parameters

- **address mac-address**: Enter the keyword address followed by a MAC address in nn:nn:nn:nn:nn:nn format.
- **all**: Enter the keyword all to delete all MAC address entries in the MAC address table.
- **interface interface**: Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For a Port Channel interface, enter the keyword port-channel followed by a number:
    - C-Series and S-Series: Range: 1-128
    - E-Series: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword sonet followed by the 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.
- **vlan vlan-id**: Enter the keyword vlan followed by a VLAN ID number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

- Version 8.4.6.0: Added support for the keyword fortyGigE.
- Version 7.6.1.0: Introduced on S-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.1: Introduced on E-Series

mac accounting destination

Configure a destination counter for Layer 2 traffic.

Syntax

mac accounting destination {mac-address vlan vlan-id | vlan} [bytes | packets]

To delete a destination counter, enter no mac accounting destination.
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.
  - E-Series Range from CONFIGURATION mode: 10 - 1000000
  - E-Series Range from INTERFACE VLAN mode: 1 - 1000000
  - C-Series and S-Series Range: 10 - 1000000
  - Default: 1800 seconds

Defaults: 1800 seconds

Command Modes:
- CONFIGURATION
- INTERFACE VLAN (E-Series only)

Command History:
- Version 8.3.1.0 On the E-Series, available in INTERFACE VLAN context and reduced minimum aging time in INTERFACE VLAN context from 10 seconds to 1 second.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

Related Commands:
- `mac learning-limit` Set the MAC address learning limits for a selected interface.
- `show mac-address-table aging-time` Display 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.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.</td>
</tr>
<tr>
<td>output interface</td>
<td>Enter the keyword <strong>output</strong> followed by one of the following interfaces:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <strong>GigabitEthernet</strong></td>
</tr>
<tr>
<td></td>
<td>followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <strong>port-channel</strong> followed</td>
</tr>
<tr>
<td></td>
<td>by a number:</td>
</tr>
<tr>
<td></td>
<td>C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to</td>
</tr>
<tr>
<td></td>
<td>512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For a SONET interface, enter the keyword <strong>sonet</strong> followed by the slot/</td>
</tr>
<tr>
<td></td>
<td>port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <strong>TenGigabitEthernet</strong></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 <strong>fortyGigE</strong></td>
</tr>
<tr>
<td></td>
<td>followed by the slot/port information.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>Enter the keyword <strong>vlan</strong> followed by a VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 4094.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for the keyword <strong>fortyGigE</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td></td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac-address-table</td>
<td>Displays the MAC address table.</td>
</tr>
</tbody>
</table>
mac-address-table station-move threshold

Change the frequency with which the MAC address station-move trap is sent after a MAC address changes in a VLAN. A trap is sent if a station move is detected above a threshold number of times in a given interval.

Syntax

```
[no] mac-address-table station-move threshold number interval count
```

Parameters

- `threshold number` Enter the keyword threshold followed by the number of times MAC addresses in VLANs can change before an SNMP trap is sent.
  - Range: 1 to 10
- `interval seconds` Enter the keyword interval followed by the number of seconds.
  - Range: 5 to 60

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

Usage Information

For information on the specific trap sent and the corresponding Syslog refer to Appendix .

mac-address-table station-move time-interval

Reduce the amount of time Dell Networking OS takes to detect aged entries and station moves.

Syntax

```
[no] mac-address-table station-move time-interval number
```

Parameters

- `time-interval number` Select the interval of the successive scans of the MAC address table that are used to detect a aged entries and station moves.
  - Range: 500 to 5000ms

Defaults

5000ms

Command Modes

CONFIGURATION

Command History

- Version 7.8.1.0 Introduced on E-Series

Usage Information

Dell Networking OS takes 4 to 5 seconds to detect aged entries and station moves because the MAC address table scanning routine runs every 5000 ms by default. To achieve faster detection, reduce the scanning interval.

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
```

Layer 2 | 879
| **Defaults** | No default values or behavior |
| **Command Modes** | CONFIGURATION |

**Command History**

| Version 7.7.1.0 | Introduced on S-Series |
| Version 7.6.1.0 | Introduced on C-Series |
| Version 7.4.1.0 | Introduced on E-Series |

**Usage Information**

See the “NIC Teaming” section of the Layer 2 chapter in the *Dell Networking OS Configuration Guide* for details on using this command.
mac cam fib-partition

Reapportion the amount of Content Addressable Memory (CAM) available for MAC address learning (FIB) versus the amount available for MAC ACLs on a line card.

**Syntax**

```
mac cam fib-partition \{25 | 50 | 75 | 100\} slot-number
```

To return to the default setting, enter **no mac cam fib-partition**.

**Parameters**

- **25**
  - Enter the keyword 25 to set aside 25% of the CAM for MAC address learning.
- **50**
  - Enter the keyword 50 to set aside 50% of the CAM for MAC address learning.
- **75**
  - Enter the keyword 75 to set aside 75% of the CAM for MAC address learning.
- **100**
  - Enter the keyword 100 to set aside 100% of the CAM for MAC address learning.
  - With this configuration, no MAC ACLs are processed.

- **slot-number**
  - Enter the line card slot number.
  - Range: 0 to 13 for the E1200
  - 0 to 6 for the E600
  - 0 to 5 for the E300

**Defaults**

75 (75% of the MAC CAM for MAC address learning)

**Command Modes**

CONFIGURATION

**Usage Information**

After setting the CAM partition size, the line card resets.

**Related Commands**

- **show mac cam** Display the current MAC CAM partition values.

mac learning-limit

Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

**Note:** Sticky MAC is not supported on the S25 or S50 in Dell Networking OS release 8.4.2.6.

**Syntax**

```
mac learning-limit address_limit [vlan vlan-id] [dynamic] [no-station-move | station-move] [sticky]
```

**Parameters**

- **address_limit**
  - Enter the maximum number of MAC addresses that can be learned on the interface.
  - Range: 1 to 1000000
- **vlan vlan-id**
  - E-Series only: Enter the keyword followed by the VLAN ID.
  - Range: 1-4094
- **dynamic**
  - (OPTIONAL) Enter the keyword dynamic to allow aging of MACs even though a learning limit is configured.
- **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.
On C-Series, the default behavior is **no-station-move** + static.

On E-Series, the default behavior is **station-move** + static.

“Static” means manually entered addresses, which do not age.

**Command Modes**

**INTERFACE**

**Defaults**

| **station-move** | (OPTIONAL) Enter the keyword station-move to allow a station move on learned MAC addresses. |
| **sticky** | (OPTIONAL) C-Series and S-Series only: Enter the keyword sticky to enable sticky MAC-address learning, which converts dynamically-learned MAC addresses on a port or port-channel interface to “sticky” MAC addresses that prevent trusted devices from moving to a different interface. |

This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

If the **vlan** option is not specified, then 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 keyword **no-station-move** option, MAC addresses learned through this feature on the selected interface will 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.

Once 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.

**Note:** If you configure this command on an interface in a routed VLAN, and once the MAC addresses learned reaches the limit set in the **mac learning-limit** command, IP protocols are affected. For example, VRRP sets multiple VRRP Masters, and OSPF may not come up.

When a channel member is added to a port-channel and there is not enough ACL CAM space, then 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.
When you enable sticky MAC-address learning (sticky), dynamically-learned MAC addresses of trusted devices are added to the running configuration and “stick” to the port or VLAN on which they are learned even if an interface goes down and comes back up. If you save sticky MAC addresses to the start-up configuration file by entering the `write config` command, the addresses are deleted from the running-configuration, do not have to be dynamically relearned, and do not change when the switch reboots. Any sticky MAC addresses learned after the `write config` is performed are not saved after a reboot.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters</td>
<td>Clear counters used in the <code>show interface</code> command</td>
</tr>
<tr>
<td>clear mac-address-table dynamic</td>
<td>Clear the MAC address table of all MAC address learned dynamically.</td>
</tr>
<tr>
<td>show mac learning-limit</td>
<td>Display MAC learning-limit configuration.</td>
</tr>
</tbody>
</table>

### mac learning-limit learn-limit-violation

Configure an action for a MAC address learning-limit violation.

**Syntax**

```
mac learning-limit learn-limit-violation {log | shutdown}
```

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**

No default behavior or values

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

This is supported on physical interfaces, static LAGs, and LACP LAGs.

**Related Commands**

- `show mac learning-limit`: Display details of the mac learning-limit
mac learning-limit station-move-violation

Specify the actions for a station move violation.

Syntax

```
mac learning-limit station-move-violation {log | shutdown-both | shutdown-offending | shutdown-original}
```

To disable a configuration, use the `no mac learning-limit station-move-violation` command, followed by the configured keyword.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>log</code></td>
<td>Enter the keyword <code>log</code> to generate a syslog message on a station move violation.</td>
</tr>
<tr>
<td><code>shutdown-both</code></td>
<td>Enter the keyword <code>shutdown</code> to shut down both the original and offending interface and generate a syslog message.</td>
</tr>
<tr>
<td><code>shutdown-offending</code></td>
<td>Enter the keyword <code>shutdown-offending</code> to shut down the offending interface and generate a syslog message.</td>
</tr>
<tr>
<td><code>shutdown-original</code></td>
<td>Enter the keyword <code>shutdown-original</code> to shut down the original interface and generate a syslog message.</td>
</tr>
</tbody>
</table>

Defaults

No default behavior or values

Command Modes

```
INTERFACE (conf-if-interface-slot/port)
```

Command History

- **Version 8.2.1.0** Introduced on S-Series
- **Version 7.8.1.0** Introduced on C-Series
- **Version 7.5.1.0** Introduced on E-Series

Usage Information

This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands

```
show mac learning-limit
```
Display 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

No default behavior or values

Command Modes

```
EXEC
```

EXEC Privilege

Command History

- **Version 8.2.1.0** Introduced on S-Series
- **Version 7.7.1.0** Introduced on C-Series
- **Version 7.5.1.0** Introduced on E-Series
show cam mac linecard (count)

Display the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

Syntax

```
show cam mac linecard slot port-set port-pipe count [vlan vlan-id] [interface interface]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>linecard slot</strong></td>
<td>(REQUIRED) Enter the keyword <strong>linecard</strong> followed by a slot number to select the linecard for which to gather information. E-Series range: 0 to 6.</td>
</tr>
<tr>
<td><strong>port-set port-pipe</strong></td>
<td>(REQUIRED) Enter the keyword <strong>port-set</strong> followed by a Port-Pipe number to select the Port-Pipe for which to gather information. E-Series range: 0 or 1</td>
</tr>
<tr>
<td><strong>count</strong></td>
<td>(REQUIRED) Enter the keyword <strong>count</strong> to display CAM usage by interface type.</td>
</tr>
</tbody>
</table>
| **interface interface** | (OPTIONAL) Enter the keyword **interface** followed by the interface type, slot and port information:  
  • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. 
  • For a Port Channel interface, enter the keyword **port-channel** followed by a number:  
    E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale. 
  • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. 
  • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** 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

- pre-Version 6.2.1.1 Introduced on E-Series

show cam maccheck linecard

Display the results of the BCMI2 check command.

Syntax

```
show cam maccheck linecard slot port-set port-pipe
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **linecard slot** | (REQUIRED) Enter the keyword **linecard** followed by a slot number to select the linecard for which to gather information.  
  C7008/C300 range: 0 to 7; C7004/C150 range: 0 to 4 |
| **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 or 1 |
Use this command to check various flags associated with each MAC address in the CAM.

**Example**

**Figure 30-1. show cam maccheck linecard Command Output Example**

```
FTOS#show cam maccheck linecard 2 port-set 0
Dumping entries. From 0 to 16383.
Progress . marks 100 memory table entries.
.........................Index 5576 (0x15c8) has valid entries (H: 2b9, E: 0)
<MAC_ADDR=0xffffffffffff,VLAN_ID=0xfff,PRI=0,CPU=0,DST_DISCARD=0,SRC_DISCARD=0,SCP
=-0,TGID LO=0,PORT_TGID=0,TGID_PORT=0,T=0,TGID_HI=0,L2MC_PTR=0,MODULE_ID=0,REMOTE_T
RUNK=0,L3=0,MAC_BLOCK_INDEX=0,STATIC_BIT=1,RPE=0,MIRROR=0,VALID=1,EVEN_PARITY=0,HIT
DA=0,HITSA=0>

........Index 6592 (0x19c0) has valid entries (H: 338, E: 0)
<MAC_ADDR=0xa0000000,VLAN_ID=0xffe,PRI=0,CPU=0,DST_DISCARD=0,SRC_DISCARD=0,SCP=0,T
GID LO=0,PORT_TGID=0,TGID_PORT=0,T=0,TGID_HI=0,L2MC_PTR=0,MODULE_ID=0x10,REMOTE_TR
UNK=0,L3=0,MAC_BLOCK_INDEX=0,STATIC_BIT=0,RPE=0,MIRROR=0,VALID=1,EVEN_PARITY=1,HIT
DA=1,HITSA=1>

!-------------output truncated-------------------!
```

**Usage Information**

Figure 30-1 shows information for two MAC addresses. The second entry is for MAC address 00:00:a0:00:00:00 (leading 0s are not shown), which is shown as learned on VLAN ID 4094 (0xfff), as shown below in Figure 30-2 and Figure 30-3. Above, “STATIC_BIT=0” means that the address is dynamically learned.

When an entry is listed as STATIC_BIT=1, its HIT_SA is 0, which signifies that this address is not getting continuously learned through traffic. The HIT_DA is set when a new learn happens, and after the first age sweep, it gets reset.

**Example**

**Figure 30-2. show mac-address-table Command Output Example**

```
FTOS#show mac-address-table
VlanId  Mac Address           Type   Interface        State
  4094   00:00:a0:00:00:00       Dynamic Gi 2/0          Active

!-------------output truncated-------------------!
```

**Example**

**Figure 30-3. show cam mac linecard Command Output Example**

```
FTOS#show cam mac linecard 2 port-set 0
VlanId  Mac Address      Region    Interface
  0      ff:ff:ff:ff:ff:ff   STATIC      00001
  4094   00:00:a0:00:00:00   DYNAMIC     Gi 2/0

!-------------output truncated-------------------!
```
show cam mac linecard (dynamic or static)

Display the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

Syntax

```
show cam mac linecard slot port-set port-pipe [address mac-addr | dynamic | interface interface | static | vlan vlan-id]
```

Parameters

- **linecard slot** (REQUIRED) Enter the keyword `linecard` followed by a slot number to select the linecard for which to gather information.
  - `C-Series` Range: 0 to 4 (C7004/C150); 0 to 8 (C7008/C300)
  - `E-Series` Range: 0 to 6
- **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 or 1
- **address mac-addr** (OPTIONAL) Enter the keyword `address` followed by a MAC address in the `nn:nn:nn:nn:nn:nn` format to display information on that MAC address.
- **dynamic** (OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses learned dynamically by the switch.
- **interface interface** (OPTIONAL) Enter the keyword `interface` followed by the interface type, slot and port information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - `C-Series` Range: 1-128
    - `E-Series` Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
- **static** (OPTIONAL) Enter the keyword `static` to display only those MAC addresses specifically configured on the switch.
- **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 8.4.6.0 Added support for the keyword `fortyGigE`.
- Version 7.5.1.0 Added support for C-Series
- pre-Version 6.2.1.1 Introduced on E-Series
### show cam mac linecard Command Example

Example Figure 30-4. show cam mac linecard Command Example

FTOS#show cam mac linecard 1 port-set 0
Port - (TableID) assignments:
00(01) 01(01) 02(01) 03(01) 04(01) 05(01) 06(01) 07(01) 08(01) 09(01) 10(01) 11(01) 12(01) 13(01) 14(01) 15(01) 16(01) 17(01) 18(01) 19(01) 20(01) 21(01) 22(01) 23(01)
Index Table ID  VlanId     Mac Address       Region   Interface
0      1       00:01:e8:0d:b7:3b   LOCAL_DA         1e000
1      1       00:01:e8:0d:b7:3a   LOCAL_DA         1e000
101    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
102    0       01:80:00:00:00:00  SYSTEM_STATIC    01c05
103    0       01:00:00:00:00:00  SYSTEM_STATIC    01c01
104    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
105    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
106    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
107    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
108    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
109    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
110    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
111    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
112    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
113    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
114    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
115    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
116    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
117    0       01:80:00:00:00:00  SYSTEM_STATIC    01c01
FTOS#

### 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 `linecard` followed by a stack member number to select the linecard for which to gather information.
  - **S-Series** Range: 0 to 1

- **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.
  - **S-Series** range: 0 or 1

- **address mac-addr** (OPTIONAL) Enter the keyword `address` followed by a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.

- **dynamic** (OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses learned dynamically by the switch.

- **static** (OPTIONAL) Enter the keyword `static` to display only those MAC addresses 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 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **S-Series** Range: 1-128
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` 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 7.6.1.0** This version of the command introduced for S-Series

**Note:** Sticky MAC is not supported on the S25 or S50 in Dell Networking OS release 8.4.2.6.

**Dynamic**

(Optional) Enter the keyword `dynamic` to display only those MAC addresses learned dynamically by the switch. Optionally, you can also add one of these combinations: `address/mac-address`, `interface/interface`, or `vlan vlan-id`.

**Static**

(Optional) Enter the keyword `static` to display only those MAC address specifically configured on the switch. Optionally, you can also add one of these combinations: `address/mac-address`, `interface/interface`, or `vlan vlan-id`.

**address mac-address**  
(Optional) Enter the keyword `address` followed by a MAC address in the `nn:nn:nn:nn:nn:nn` format to display information on that MAC address.
**interface interface**  (OPTIONAL) Enter the keyword `interface` followed by the interface type, slot and port information:
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword `sonet` followed by the 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.

**interface interface-type**  (OPTIONAL) Instead of entering the keyword `interface` followed by the interface type, slot and port information, as above, you can enter the interface type, followed by just a slot number.

**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.

**count**  (OPTIONAL) Enter the keyword `count`, followed optionally, by an interface or VLAN ID, to display total or interface-specific static addresses, dynamic addresses, and MAC addresses in use.

---

**Command Modes**

EXEC
EXEC Privilege

**Command History**

- Version 8.4.6.0 Added support for the keyword `fortyGigE`.
- Version 8.4.2.3 Added support for sticky-MAC learned addresses on the C-Series and S-Series.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

**Example**

**Figure 30-5.  show mac-address-table Command Example**

```
FTOS#show mac-address-table
VlanId  Mac Address           Type   Interface        State
999    00:00:00:00:00:19       Dynamic Gi 0/1          Active
999    00:00:00:00:00:29       Dynamic Gi 0/2          Active
10     00:00:00:11:11:11       Sticky Gi 0/3          Active

FTOS#show mac-address-table dynamic
Codes: *N - VLT Peer Synced MAC
VlanId  Mac Address           Type   Interface        State
182    00:01:e8:b3:ba:09       Dynamic (N)     Po 21          Active
183    00:01:e8:6b:76:5a       Dynamic (N)     Po 31          Active

FTOS#
```
Table 30-1. show mac-address-table 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), learned dynamically (Dynamic), or learned on a port configured for sticky-MAC learning (Sticky). An (N) indicates that the specified MAC address has been learnt by a neighbor and is synced to the node.</td>
</tr>
</tbody>
</table>
| Interface      | Displays the interface type and slot/port information. The following abbreviations describe the interface types:  
  • gi—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). |

Table 30-2. show mac-address-table count 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>

Related Commands

show mac-address-table aging-time  
Display MAC aging time.

display mac-address-table aging-time

C E S

Syntax

show mac-address-table aging-time [vlan vlan-id]
### Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vlan vlan-id</strong></td>
<td>On the E-Series, enter the keyword <strong>vlan</strong> 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

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>EXEC Privilege</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added the <strong>vlan</strong> option on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

### Example

**Figure 30-7. show mac-address-table aging-time Command Example**

```
FTOS#show mac-address-table aging-time
Mac-address-table aging time : 1800

FTOS#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac-address-table</td>
<td>Display the current MAC address configuration.</td>
</tr>
</tbody>
</table>
show mac accounting destination

Display destination counters for Layer 2 traffic (available on physical interfaces only).

**Syntax**

`show mac accounting destination [mac-address vlan vlan-id] [interface interface [mac-address vlan vlan-id] [vlan vlan-id]]`

**Parameters**

- **mac-address**: (OPTIONAL) Enter the MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
- **interface interface**: (OPTIONAL) Enter the keyword `interface` followed by the interface type, slot and port information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` 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 that VLAN. Range: 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- **pre-Version 6.2.1.1** Introduced on E-Series

**Usage Information**

MAC Accounting information can be accessed using SNMP via the Dell Networking OS Monitor MIB. For more information on enabling SNMP, refer to Chapter 3 of the Dell Networking OS Configuration Guide.

**Note**: Currently, the Dell Networking OS MONITOR MIB does not return the MAC addresses in an increasing order via SNMP. As a workaround, you can use the `-C c` option in `snmpwalk` or `snmpbulkwalk` to access the Dell Networking OS MONITOR MIB. For example:

```
% snmpwalk -C c -v 2c -c public 133.33.33.131 enterprise.6027.3.3.3
```

**Example**

```
Figure 30-8. show mac accounting destination Command Example

FTOS-1# show mac accounting destination interface gigabitethernet 2/1

<table>
<thead>
<tr>
<th>Destination</th>
<th>Out</th>
<th>Port</th>
<th>VLAN</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:44:00:00:00:02</td>
<td>Te</td>
<td>11/0</td>
<td>1000</td>
<td>10000</td>
<td>5120000</td>
</tr>
<tr>
<td>00:44:00:00:00:01</td>
<td>Te</td>
<td>11/0</td>
<td>1000</td>
<td>10000</td>
<td>5120000</td>
</tr>
<tr>
<td>00:22:00:00:00:00</td>
<td>Te</td>
<td>11/0</td>
<td>1000</td>
<td>10000</td>
<td>5120000</td>
</tr>
<tr>
<td>00:44:00:00:00:02</td>
<td>Te</td>
<td>11/0</td>
<td>2000</td>
<td>10000</td>
<td>5120000</td>
</tr>
<tr>
<td>00:44:00:00:00:01</td>
<td>Te</td>
<td>11/0</td>
<td>2000</td>
<td>10000</td>
<td>5120000</td>
</tr>
</tbody>
</table>

FTOS-1#
```

**Related Commands**

- `show mac accounting access-list` — Display MAC access list configurations and counters (if configured).
show mac cam

Display the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

Syntax

show mac cam

Command Modes

EXEC
EXEC Privilege

Command History

pre-Version 6.2.1.1 Introduced on E-Series

Example

Figure 30-9. show mac cam Command Example

FTOS#show mac cam
Slot  Type     MAC CAM Size   MAC FIB Entries   MAC ACL Entries
 0   E24PD     64K entries       48K (75%)           8K (25%)
 2   E24PD2   128K entries       64K (50%)          32K (50%)
11   EX2YD     64K entries       16K (25%)          24K (75%)
Note: All CAM entries are per portpipe.
FTOS#

Table 30-3. show mac cam Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>Lists the active line card slots.</td>
</tr>
<tr>
<td>Type</td>
<td>Lists the type of line card present in the slot.</td>
</tr>
<tr>
<td>MAC CAM Size</td>
<td>Displays the total CAM size available.</td>
</tr>
<tr>
<td>Note: A portion of the MAC CAM is used for system operations, therefore adding the MAC FIB and MAC ACL will be less than the MAC CAM.</td>
<td></td>
</tr>
<tr>
<td>MAC FIB Entries</td>
<td>Displays the amount and percentage of CAM available for MAC addresses.</td>
</tr>
<tr>
<td>MAC ACL Entries</td>
<td>Displays the amount and percentage of CAM available for MAC ACLs.</td>
</tr>
</tbody>
</table>

show mac learning-limit

Display MAC address learning limits set for various interfaces.

Syntax

show mac learning-limit [violate-action] [detail] [interface interface [vlan vlan-id]]

Parameters

violate-action  (OPTIONAL) 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**  
(OptionalAL) Enter the keyword **interface** with the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
- For SONET interfaces, enter the keyword **sonet** followed by the 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.
- For a Port Channel interface, enter the keyword **port-channel** followed by a number:

  **C-Series** Range: 1-128

  **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.

**vlan vlan-id**  
On the E-Series, enter the keyword **vlan** followed by the VLAN ID.

Range: 1-4094

---

**Command Modes**

**EXEC**

**EXEC Privilege**

**Command History**

- **Version 8.4.6.0**  Added support for the keyword **fortyGigE**.
- **Version 8.3.1.0**  Added **vlan** option on E-Series.
- **Version 7.7.1.0**  Introduced on C-Series
- **Version 7.5.1.0**  Added support for **violate-action** and **detail** options
- **Version 6.5.1.0**  Added support for Port Channel

---

**Example**

**E-Series output:**

```plaintext
FTOS#show mac learning-limit  
Interface  Vlan  Learning  Dynamic  Static  Unknown SA
Slot/port   Id    Limit    MAC count  MAC count  Drops
Gi 5/84     2     2        0         0         0
Gi 5/84     *     5        0         0         0
Gi 5/85     3     3        0         0         0
Gi 5/85     *     10       0         0         0
FTOS#show mac learning-limit interface gig 5/84  
Interface  Vlan  Learning  Dynamic  Static  Unknown SA
Slot/port   Id    Limit    MAC count  MAC count  Drops
Gi 5/84     2     2        0         0         0
Gi 5/84     *     5        0         0         0
FTOS#show mac learning-limit interface gig 5/84 vlan 2  
Interface  Vlan  Learning  Dynamic  Static  Unknown SA
Slot/port   Id    Limit    MAC count  MAC count  Drops
Gi 5/84     2     2        0         0         0
```

**Example**

**C-Series/S-Series output:**

```plaintext
FTOS#show mac learning-limit  
Interface  Learning  Dynamic  Static  Unknown SA
Slot/port   Limit    MAC count  MAC count  Drops
Gi 1/0      10        0         0         0
Gi 1/1      5          0         0         0
FTOS#show mac learning-limit interface gig 1/0  
Interface  Learning  Dynamic  Static  Unknown SA
Slot/port   Limit    MAC count  MAC count  Drops
Gi 1/0      10        0         0         0
```
Virtual LAN (VLAN) Commands

The following commands configure and monitor Virtual LANs (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 VRRP state of a VLAN interface may continually switch between Master and Backup.

- description
- default vlan-id
- default-vlan disable
- enable vlan-counters
- name
- show config
- show vlan
- tagged
- track ip
- untagged

See also VLAN Stacking and see VLAN-related commands, such as portmode hybrid, in Chapter 23, Interfaces.

description

Add a description about the selected VLAN.

Syntax
description description

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

Parameters
description Enter a text string description to identify the VLAN (80 characters maximum).

Defaults
No default behavior or values

Command Modes
INTERFACE VLAN

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Related Commands

- show vlan Display VLAN configuration.
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` syntax.

**Parameters**

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default vlan-id</code></td>
<td>Enter the VLAN ID number of the VLAN to become the new Default VLAN.</td>
</tr>
<tr>
<td><code>vlan-id</code></td>
<td>Range: 1 to 4094.</td>
</tr>
<tr>
<td><code>Default</code>: 1</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

The Default VLAN is VLAN 1.

**Command Modes**

CONFIGURATION

**Command History**

- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **pre-Version 6.2.1.1** Introduced on E-Series

**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><code>interface vlan</code></td>
<td>Configure 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 8.3.1.0** Introduced

**Usage Information**

`no default vlan disable` is not listed in the running-configuration, but when the default VLAN is disabled, `default-vlan disable` is listed in the running-configuration.

---

**enable vlan-counters**

Display VLAN counters for ingress and/or egress hardware. You must be in restricted mode to use this command.

**Syntax**

```
enable vlan-output-counters [ingress | egress | all]
```

To return to the default (disabled), use the `no enable vlan-output-counters` command.
**Defaults**  Disabled—VLAN counters are disabled in hardware (all linecards/port-pipes) by default.

**Command Modes**  
CONFIGURATION

**Command History**  

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.2</td>
<td>E600i</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>E1200i</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS(conf)#enable vlan-output-counters
FTOS(conf)#exit
FTOS#show interface vlan 101
Vlan 101 is down, line protocol is down
Address is 00:01:e8:26:e0:5b, Current address is 00:01:e8:26:e0:5b
Interface index is 1107787877
Internet address is not set
MTU 1554 bytes, IF MTU 1500 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:12:44
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
Output Statistics:
  0 packets, 0 bytes
Time since last interface status change: 01:12:44
FTOS#
```

```
FTOS#show interfaces vlan 1
Vlan 1 is down, line protocol is down
Address is 00:01:e8:13:a5:aa, Current address is 00:01:e8:13:a5:aa
Interface index is 1107787877
Internet address is not set
MTU 1554 bytes, IF MTU 1500 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:36:01
Queueing strategy: fifo
Input Statistics:
  100000 packets, 1000000 bytes
Output Statistics:
  200000 packets, 20800000 bytes
Time since last interface status change: 01:36:01
FTOS#
```

**Usage Information**  
Dell Networking OS supports a command to enable viewing of the VLAN input/output counters. This command also applies to SNMP requests. If the command is not enabled, IFM returns zero values for VLAN output counters.

SNMP counters differ from show interface counters as SNMP counters must maintain history. At any point, the value of SNMP counters reflect the amount of traffic being carried on the VLAN.

VLAN output counters may show higher than expected values because source-suppression drops are counted.

During an RPM failover event, all SNMP counters remain intact. The counters will sync over to the secondary RPM.
**name**

Assign a name to the VLAN.

**Syntax**

```
name vlan-name
```

To remove the name from the VLAN, enter `no name`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-name</code></td>
<td>Enter up to 32 characters as the name of the VLAN.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

INTERFACE VLAN

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**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` - Assign a descriptive text string to the interface.
- `interface vlan` - Configure a VLAN.
- `show vlan` - Display 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**

```
FTOS(conf-if-vl-100)#show config
!
interface Vlan 100
  no ip address
  no shutdown
FTOS(conf-if-vl-100)#
```

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
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

- **id vlan-id** (OPTIONAL) Enter the keyword **id** followed by a number from 1 to 4094. Only information on the VLAN specified is displayed.

- **name vlan-name** (OPTIONAL) Enter the keyword **name** followed by the name configured for the VLAN. Only information on the VLAN named is displayed.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Augmented to display PVLAN data for C-Series and S-Series; revised output to include Description field to display user-entered VLAN description</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series; revised output to display Native VLAN</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 30-11. show vlan Command Example**

```
FTOS#show vlan
Codes: * - Default VLAN, G - GVRP VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
    x - Dot1x untagged, X - Dot1x tagged
    G - GVRP tagged, M - Vlan-stack

NUM    Status    Description                     Q Ports
*   1      Inactive                       U Po1(Gi 13/0)
     2      Active                        T Po20(Gi 13/6), Gi 13/25
                T Gi 13/7
                T Po20(Gi 13/6)
                T Gi 13/7
                U Gi 13/1
                U Po2(Gi 13/2)
                T Po20(Gi 13/6)
                T Gi 13/7
                T Po20(Gi 13/6)
                T Gi 13/7
                U Gi 13/3
                U Po3(Gi 13/4)
                T Po20(Gi 13/6)
                T Gi 13/7
                T Po20(Gi 13/6)
                T Gi 13/7
                U Gi 13/5
                T Po1(Gi 0/1)
                T Gi 0/2
                T Gi 0/3
                T Gi 0/4
FTOS#
```

900 | Layer 2
Table 30-4. show vlan Information

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUM</td>
<td>Displays existing VLAN IDs.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the word <strong>Inactive</strong> for inactive VLANs and the word <strong>Active</strong> 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, Gi = gigabit ethernet, and Te = ten gigabit ethernet.</td>
</tr>
</tbody>
</table>

FTOS# show vlan id 40

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>40</td>
<td>Active</td>
<td></td>
<td>M Gi 13/47</td>
</tr>
</tbody>
</table>

FTOS# show vlan id 41

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>41</td>
<td>Active</td>
<td></td>
<td>T Gi 13/47</td>
</tr>
</tbody>
</table>

FTOS# show vlan id 42

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>42</td>
<td>Active</td>
<td></td>
<td>U Gi 13/47</td>
</tr>
</tbody>
</table>
Add a Layer 2 interface to a VLAN as a tagged interface.

**tagged interface**

To remove a tagged interface from a VLAN, use `no tagged interface` command.

### Parameters

- **interface**: Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` 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:
    - **C-Series** and **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

### Defaults

All interfaces in Layer 2 mode are untagged.

### Command Modes

- **INTERFACE VLAN**
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**

- `interface vlan`: Configure a VLAN.
- `untagged`: Specify which interfaces in a VLAN are untagged.

**track ip**

Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

**Syntax**

```plaintext
track ip interface
```

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **C-Series and S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.

**Defaults**

Not configured

**Command Modes**

INTERFACE VLAN

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **pre-Version 6.2.1.1** Introduced on E-Series

**Usage Information**

When this command is configured, the VLAN is operationally UP if any of the interfaces specified in the `track ip` command are operationally UP, and the VLAN is operationally DOWN if none of the tracking interfaces are operationally UP.
If the `track ip` command is not configured, 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>Configure a VLAN.</td>
</tr>
<tr>
<td><code>tagged</code></td>
<td>Specify 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

`untagged interface`

To remove an untagged interface from a VLAN, use the `no untagged 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 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` 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:  
    - **C-Series and S-Series** Range: 1-128  
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.  
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information. |

#### Defaults

All interfaces in Layer 2 mode are untagged.

#### Command Modes

**INTERFACE VLAN**

#### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

#### 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 the INTERFACE mode and use the `no switchport` command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface vlan</code></td>
<td>Configure a VLAN.</td>
</tr>
<tr>
<td><code>tagged</code></td>
<td>Specify which interfaces in a VLAN are tagged.</td>
</tr>
</tbody>
</table>
Link Layer Detection Protocol (LLDP)

Overview

Link Layer Detection 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 Networking OS implementation of LLDP is based on IEEE standard 801.1ab.

The basic LLDP commands are supported by Dell Networking OS on all Dell Networking systems, as indicated by the characters that appear below each command heading:

- C-Series: C
- E-Series: E
- S-Series: S

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
- 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 the 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.

See the Link Layer Discovery Protocol chapter of the Dell Networking OS Configuration Guide for details on implementing LLDP/LLDP-MED.

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>
<th>Defaults</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>
<td></td>
</tr>
<tr>
<td>port-vlan-id</td>
<td>Enter the keyword port-vlan-id to advertise the port VLAN identification TLV.</td>
<td></td>
</tr>
<tr>
<td>vlan-name</td>
<td>Enter the keyword vlan-name to advertise the vlan-name TLV. This keyword is only supported on C-Series and S-Series.</td>
<td></td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

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

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series, added vlan-name option.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol lldp (Configuration)</td>
<td>Enable LLDP globally.</td>
</tr>
<tr>
<td>debug lldp interface</td>
<td>Debug LLDP</td>
</tr>
<tr>
<td>show lldp neighbors</td>
<td>Display the LLDP neighbors</td>
</tr>
<tr>
<td>show running-config lldp</td>
<td>Display the LLDP running configuration</td>
</tr>
</tbody>
</table>

advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

Syntax

advertise dot3-tlv \{max-frame-size | power-via-mdi\}

To remove advertised dot3-tlv, use the no advertise dot3-tlv \{max-frame-size | power-via-mdi\} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>max-frame-size</td>
<td>Maximum data frame size of dot3 TLV.</td>
<td></td>
</tr>
<tr>
<td>power-via-mdi</td>
<td>Power via MDI</td>
<td></td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

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

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series, added vlan-name option.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol lldp (Configuration)</td>
<td>Enable LLDP globally.</td>
</tr>
<tr>
<td>debug lldp interface</td>
<td>Debug LLDP</td>
</tr>
<tr>
<td>show lldp neighbors</td>
<td>Display the LLDP neighbors</td>
</tr>
<tr>
<td>show running-config lldp</td>
<td>Display the LLDP running configuration</td>
</tr>
</tbody>
</table>
Parameters

- **max-frame-size** Enter the keyword `max-frame-size` to advertise the dot3 maximum frame size.
- **power-via-mdi** Enter the keyword `power-via-mdi` to advertise IEEE 802.3at power-via-mdi TLV.

Defaults

No default values or behavior

Command Modes

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

Command History

- Version 8.4.5.0 Introduced power-via-mdi option
- Version 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- Version 7.4.1.0 Introduced on E-Series

**advertise management**

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

- **system-capabilities** Enter the keyword `system-capabilities` to advertise the system capabilities TLVs.
- **system-description** Enter the keyword `system-description` to advertise the system description TLVs.
- **system-name** Enter the keyword `system-name` to advertise the system name TLVs.

Defaults

No default values or behavior

Command Modes

CONFIGURATION (conf-lldp)

Command History

- Version 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- Version 7.4.1.0 Introduced on E-Series

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
```

Link Layer Detection Protocol (LLDP) | 907
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 Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword `gigabitEthernet` followed by the 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.

**Defaults**
No default values or behavior

**Command Modes**
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
debug lldp interface

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

Syntax
debug lldp interface {interface | all} {events | packet {brief | detail} {tx | rx | both}}

To disable debugging, use the no debug lldp interface {interface | all} {events | packet {brief | detail} {tx | rx | both}} command.

Parameters

- **interface**: Enter the following keywords and slot/port or number information:
  - For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword **gigabitEthernet** followed by the 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.

  **Note**: The **FastEthernet** option is not supported on S-Series.

- **all**: (OPTIONAL) Enter the keyword **all** to display information on all interfaces.

- **events**: (OPTIONAL) Enter the keyword **events** to display major events such as timer events.

- **packet**: (OPTIONAL) Enter the keyword **packet** to display information regarding packets coming in or going out.

- **brief**: (OPTIONAL) Enter the keyword **brief** to display brief packet information.

- **detail**: (OPTIONAL) Enter the keyword **detail** to display detailed packet information.

- **tx**: (OPTIONAL) Enter the keyword **tx** to display transmit only packet information.

- **rx**: (OPTIONAL) Enter the keyword **rx** to display receive only packet information.

- **both**: (OPTIONAL) Enter the keyword **both** to display both receive and transmit packet information.

Defaults

No default values or behavior

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

disable

Enable or disable LLDP.

Syntax
disable

To enable LLDP, use the no disable

Defaults

Enabled, that is no disable
Command Modes

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

Command History

Version 7.7.1.0 Introduced on S-Series
Version 7.6.1.0 Introduced on C-Series
Version 7.4.1.0 Introduced on E-Series

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol lldp (Configuration)</td>
<td>Enable LLDP globally.</td>
</tr>
<tr>
<td>debug lldp interface</td>
<td>Debug LLDP</td>
</tr>
<tr>
<td>show lldp neighbors</td>
<td>Display the LLDP neighbors</td>
</tr>
<tr>
<td>show running-config lldp</td>
<td>Display 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 - 180 seconds
Default: 30 seconds

Defaults 30 seconds

Command Modes

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

Command History

Version 7.7.1.0 Introduced on S-Series
Version 7.6.1.0 Introduced on C-Series
Version 7.4.1.0 Introduced on E-Series

mode

Set LLDP to receive or transmit.

Syntax

mode \{tx | rx\}

To return to the default, use the no mode \{tx | rx\} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tx</td>
<td>Enter the keyword tx to set the mode to transmit.</td>
</tr>
<tr>
<td>rx</td>
<td>Enter the keyword rx to set the mode to receive.</td>
</tr>
</tbody>
</table>

Defaults Both transmit and receive

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)
### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

#### Related Commands

- **protocol lldp (Configuration)**  
  Enable LLDP globally.
- **show lldp neighbors**  
  Display the LLDP neighbors

### multiplier

Set the number of consecutive misses before LLDP declares the interface dead.

**Syntax**

`multiplier integer`

To return to the default, use the `no multiplier integer` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `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)
- INTERFACE (conf-if-interface-lldp)

### 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)
protocol lldp (Interface)

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.

Command Modes

INTERFACE (conf-if-interface-lldp)

Command History

```
<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
</tr>
<tr>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
</tr>
<tr>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>Version 7.4.1.0</td>
</tr>
<tr>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
```

Usage Information

LLDP must be enabled globally from CONFIGURATION mode, before it can be configured on an interface. This command places you in LLDP mode on the interface; it does not enable the protocol.

When you enter the LLDP protocol in the Interface context, it overrides global configurations. When you execute the `no protocol lldp` from the INTERFACE mode, interfaces will begin to inherit the configuration from the global LLDP CONFIGURATION mode.

show lldp neighbors

Syntax

```
show lldp neighbors [interface] [detail]
```

Parameters

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `gigabitEthernet` followed by the 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.

- **detail** (OPTIONAL) Enter the keyword `detail` to display all the TLV information, timers, and LLDP tx and rx counters. (LLDP-MED or IEEE 802.3at power-via-mdi.)

Defaults

No default values or behavior

Command Modes

EXEC Privilege

Command History

```
<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.6.0</td>
</tr>
<tr>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
</tr>
<tr>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
</tr>
<tr>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>Version 7.4.1.0</td>
</tr>
<tr>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
```
**Usage Information**  
Omitting the keyword **detail** displays only the remote chassis ID, Port ID, and Dead Interval.

### show lldp neighbors

Display LLDP neighbors.

**Syntax**

```
show lldp neighbors
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

- **Version 7.7.1.0** Introduced on S-Series
- **Version 7.6.1.0** Introduced on C-Series
- **Version 7.4.1.0** Introduced on E-Series

**Example**

```
R1(conf-if-gi-1/31)#do show lldp neighbors
Loc PortID   Rem Host Name       Rem Port Id           Rem Chassis Id
-------------------------------------------------------------------------
Gi 1/21      R2                  GigabitEthernet 2/11  00:01:e8:06:95:3e
Gi 1/31      R3                  GigabitEthernet 3/11  00:01:e8:09:c2:4a
```

### show lldp statistics

Display LLDP statistical information.

**Syntax**

```
show lldp statistics
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

- **Version 7.7.1.0** Introduced on S-Series
- **Version 7.6.1.0** Introduced on C-Series
- **Version 7.4.1.0** Introduced on E-Series

**Example**

```
FTOS#show lldp statistics
Total number of neighbors:   300
Last table change time   :   Mon Oct 02 16:00:52 2006
Number of Table Inserts  :   1621
Number of Table Deletes  :   200
Number of Table Drops    :   0
Number of Table Age Outs :   400
FTOS#
```

### show running-config lldp

Display the current global LLDP configuration.

**Syntax**

```
show running-config lldp
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

- **Version 7.7.1.0** Introduced on S-Series
- **Version 7.6.1.0** Introduced on C-Series
- **Version 7.4.1.0** Introduced on E-Series
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 15
   multiplier 3
   no disable
FTOS#

## LLDP-MED Commands

The LLDP-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

Dell Networking OS LLDP-MED (Media Endpoint Discovery) commands are an extension of the set of LLDP TLV advertisement commands. The C-Series and S-Series support all commands, as indicated by these symbols underneath the command headings:

- \([\text{C}]\) \([\text{S}]\)

The E-Series generally supports the commands, too, as indicated by the \([\text{E}]\) symbol under command headings. However, LLDP-MED commands are more useful on the C-Series and the S50V model of the S-Series, because they support Power over Ethernet (PoE) devices.

As defined by ANSI/TIA-1057, LLDP-MED provides organizationally specific TLVs (Type Length Value), so that endpoint devices and network connectivity devices can advertise their characteristics and configuration information. The Organizational Unique Identifier (OUI) for the Telecommunications Industry Association (TIA) is 00-12-BB.

- **LLDP-MED Endpoint Device**—any device that is on an IEEE 802 LAN network edge, can communicate using IP, and uses the LLDP-MED framework.
- **LLDP-MED Network Connectivity Device**—any device that provides access to an IEEE 802 LAN to an LLDP-MED endpoint device, and supports IEEE 802.1AB (LLDP) and TIA-1057 (LLDP-MED). The Dell Networking system is an LLDP-MED network connectivity device.

With regard to connected endpoint devices, LLDP-MED provides network connectivity devices with the ability to:

- manage inventory
- manage Power over Ethernet (POE)
- identify physical location
• identify network policy

advertise med guest-voice

Configure the system to advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support interactive voice services.

Syntax

```
advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}
```

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 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series and E-Series

Related Commands

- protocol lldp (Configuration) Enable LLDP globally.
- debug lldp interface Debug LLDP.
- show lldp neighbors Display the LLDP neighbors.
- show running-config lldp Display the LLDP running configuration.

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.
### advertise med location-identification

Configure the system to advertise a location identifier.

**Syntax**

```plaintext
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 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series and E-Series

**Related Commands**

- `debug lldp interface` Debug LLDP
- `show lldp neighbors` Display the LLDP neighbors
- `show running-config lldp` Display the LLDP running configuration
**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug lldp interface</td>
<td>Debug LLDP</td>
</tr>
<tr>
<td>show lldp neighbors</td>
<td>Display the LLDP neighbors</td>
</tr>
<tr>
<td>show running-config lldp</td>
<td>Display the LLDP running configuration</td>
</tr>
</tbody>
</table>

### advertise med power-via-mdi

**Configure the system to advertise the Extended Power via MDI TLV.**

**Syntax**

```plaintext
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**

- Introduced on C-Series in Version 8.4.5.0

**Usage Information**

Advertise the Extended Power via MDI on all ports that are connected to the 802.3af or 802.3at powered endpoint device.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug lldp interface</td>
<td>Debug LLDP</td>
</tr>
<tr>
<td>show lldp neighbors</td>
<td>Display the LLDP neighbors</td>
</tr>
<tr>
<td>show running-config lldp</td>
<td>Display the LLDP running configuration</td>
</tr>
</tbody>
</table>

### 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**

```plaintext
advertise med softphone-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med softphone-voice {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><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 (C-Series and E-Series only).</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 7</td>
</tr>
</tbody>
</table>
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 layer2_priority DSCP_value\} | \{priority-tagged number\}

To return to the default, use the no advertise med streaming-video \{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 (C-Series and E-Series only).
  - Range: 0 to 7

- **DSCP_value**
  - Enter the DSCP value (C-Series and E-Series only).
  - 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 7.7.1.0 Introduced on S-Series
Version 7.6.1.0 Introduced on C-Series and E-Series

Related Commands

debug lldp interface Debug LLDP
show lldp neighbors Display the LLDP neighbors
show lldp neighbors Display the LLDP running configuration
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 layer2_priority DSCP_value} | {priority-tagged number}

To return to the default, use the no advertise med video-conferencing {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters

- `vlan-id` Enter the VLAN ID.
  - Range: 1 to 4094
- `layer2_priority` Enter the Layer 2 priority (C-Series and E-Series only).
  - Range: 0 to 7
- `DSCP_value` Enter the DSCP value (C-Series and E-Series only).
  - 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 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series and E-Series

Related Commands

- debug lldp interface Debug LLDP
- show lldp neighbors Display the LLDP neighbors
- show running-config lldp Display 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 layer2_priority DSCP_value} | {priority-tagged number}

To return to the default, use the no advertise med video-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters

- `vlan-id` Enter the VLAN ID.
  - Range: 1 to 4094
- `layer2_priority` Enter the Layer 2 priority (C-Series and E-Series only).
  - Range: 0 to 7
**advertise med voice**

Configure the system to advertise a dedicated IP telephony handset or other appliances supporting interactive voice services.

**Syntax**

```plaintext
advertise med voice {vlan-id layer2_priority DSCP_value} | {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
- `layer2_priority` Enter the Layer 2 priority (C-Series and E-Series only).  
  Range: 0 to 7
- `DSCP_value` Enter the DSCP value (C-Series and E-Series only).  
  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 7.7.1.0** Introduced on S-Series
- **Version 7.6.1.0** Introduced on C-Series and E-Series

**Related Commands**

- `debug lldp interface` Debug LLDP
- `show lldp neighbors` Display the LLDP neighbors
- `show lldp neighbors` Display the LLDP running configuration
- `show running-config lldp` Display the LLDP running configuration
advertise med voice-signaling

Configure the system to advertise when voice control packets use a separate network policy than voice data.

**Syntax**

`advertise med voice-signaling {vlan-id layer2_priority DSCP_value} | {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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>Enter the VLAN ID. Range: 1 to 4094</td>
</tr>
<tr>
<td><code>layer2_priority</code></td>
<td>Enter the Layer 2 priority (C-Series and E-Series only). Range: 0 to 7</td>
</tr>
<tr>
<td><code>DSCP_value</code></td>
<td>Enter the DSCP value (C-Series and E-Series only). Range: 0 to 63</td>
</tr>
<tr>
<td><code>priority-tagged</code></td>
<td>Enter the keyword <code>priority-tagged</code> followed the Layer 2 priority. Range: 0 to 7</td>
</tr>
</tbody>
</table>

**Defaults**

unconfigured

**Command Modes**

CONFIGURATION (conf-lldp)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug lldp interface</code></td>
<td>Debug LLDP</td>
</tr>
<tr>
<td><code>show lldp neighbors</code></td>
<td>Display the LLDP neighbors</td>
</tr>
<tr>
<td><code>show lldp neighbors</code></td>
<td>Display the LLDP running configuration</td>
</tr>
</tbody>
</table>
Multicast Listener Discovery (MLD)

Overview

The platforms on which a command is supported is indicated by the character — E for the E-Series, C for the C-Series, and S for the S-Series — that appears below each command heading.

This chapter contains the following sections:

- MLD Commands
- MLD Snooping Commands

MLD Commands

The MLD commands are:

- clear ipv6 mld groups
- debug ipv6 mld
- ipv6 mld explicit-tracking
- ipv6 mld last-member-query-interval
- ipv6 mld querier-timeout
- ipv6 mld query-interval
- ipv6 mld query-max-resp-time
- ipv6 mld static-group
- ipv6 mld version
- show ipv6 mld interface

**clear ipv6 mld groups**

E Clear entries from the group cache table.

**Syntax**

```
clear ipv6 mld groups [interface | group-address]
```
debug ipv6 mld

Enable debugging on IPv6 MLD packets.

Syntax

ddebug ipv6 mld {group-address | interface}

To turn off debugging, use the no debug ipv6 mld {group-address | interface} command.

Parameters

- **group-address** (OPTIONAL) Enter the multicast group address in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For a Port Channel interface, enter the keyword port-channel followed by a number:
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword sonet followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
  - For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

Defaults

Disabled

Command Modes

EXEC Privilege
ipv6 mld explicit-tracking

Enable MLD explicit tracking of receivers.

Syntax

ipv6 mld explicit-tracking

To disable explicit tracking, use the no ipv6 mld explicit-tracking command.

Defaults

Disabled

Command Modes

INTERFACE (conf-if)

Usage Information

If snooping is enabled on the VLAN, this command has no effect. Enable ipv6 mld snooping explicit tracking instead.

ipv6 mld last-member-query-interval

Change the MAX Response Time inserted into the Group-Specific Queries sent in response to a Leave Group messages. This interval is also the interval between Group-Specific Query messages.

Syntax

ipv6 mld last-member-query-interval \{milliseconds\}

To return to the default, use the no ipv6 mld last-member-query-interval \{milliseconds\} command.

Parameters

milliseconds Enter the last member query interval in milliseconds.

Range: 200 - 60000
Default: 1000

Defaults

1000 milliseconds

Command Modes

INTERFACE (conf-if)

Command History

Version 7.4.1.0 Introduced

ipv6 mld 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

ipv6 mld querier-timeout \{seconds\}

To return to the default, use the no ipv6 mld querier-timeout command.
ipv6 mld query-interval

Change the transmission frequency of the MLD host.

**Syntax**

```
ipv6 mld query-interval {seconds}
```

To return to the default interval, use the `no ipv6 mld query-interval` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Enter the interval in seconds.</td>
</tr>
</tbody>
</table>

| Defaults    | 125 seconds                                                                 |

**Command Modes**

INTERFACE (conf-if)

**Command History**

Version 7.4.1.0 Introduced

---

ipv6 mld query-max-resp-time

Set the maximum query response time advertised in the general queries.

**Syntax**

```
ipv6 mld query-max-resp-time {seconds}
```

To return to the default, use the `no ipv6 mld query-max-resp-time` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Enter the interval in seconds.</td>
</tr>
</tbody>
</table>

| Defaults    | 10 seconds                                                                 |

**Command Modes**

INTERFACE (conf-if)

**Command History**

Version 7.4.1.0 Introduced
ipv6 mld static-group

Configure an MLD static group to exclude or include mode.

**Syntax**

```
ipv6 mld static-group group-address {exclude [source-address] | include source-address}
```

To return to default, use the no ipv6 mld static-group group-address {exclude [source-address] | include source-address} command.

**Parameters**

- **group-address**
  *(OPTIONAL)* Enter the multicast group address in the `x:x:x::x` format.
  The `::` notation specifies successive hexadecimal fields of zero.

- **exclude source-address**
  Enter the keyword `exclude` and optionally enter the source ip address in the `x:x:x::x` format.
  The `::` notation specifies successive hexadecimal fields of zero.

- **include source-address**
  Enter the keyword `include` followed by source ip address in the `x:x:x::x` format.
  The `::` notation specifies successive hexadecimal fields of zero.

**Defaults**

No default behavior or values

**Command Modes**

INTERFACE (conf-if)

**Command History**

- Version 7.4.1.0 Introduced

ipv6 mld version

Set the MLD version number on this interface.

**Syntax**

```
ipv6 mld version 1
```

**Defaults**

Version 2

**Command Modes**

INTERFACE (conf-if)

**Command History**

- Version 7.4.1.0 Introduced

**Usage Information**

Dell Networking OS supports MLD version 2 and is backward compatible with MLD version 1.

**show ipv6 mld groups**

View the configured MDL groups.

**Syntax**

```
show ipv6 mld groups [detail] [explicit] [link-local] [group-address] [interface interface [detail]] [summary]
```

Multicast Listener Discovery (MLD)
show ipv6 mld interface

View the configured MDL interfaces.

Syntax

```
show ipv6 mld interface [interface]
```

Parameters

- `explicit` Enter this keyword to display explicit tracking information.
- `link-local` Enter this keyword to display link-local groups.
- `group-address` Enter the group address for which you want to display information.
- `interface interface` Enter the keyword `interface` followed by the interface type.
- `detail` View detailed group information.
- `summary` View a summary of group information.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 7.4.1.0 Introduced

Example

```
FTOS#show ipv6 mld groups vlan 100 link-local ?
detail Detailed information
| Pipe through a command

show ipv6 mld groups explicit
Interface GigabitEthernet 2/14, Group ff02::1:ff00:0
   Reporter fe80::200:ff:fe00:0
   Uptime 00:00:19, Expires in 00:04:00
   Mode EXCLUDE
Interface GigabitEthernet 2/14, Group ff02::1:ff00:5
   Reporter fe80::200:ff:fe00:0
   Uptime 00:00:19, Expires in 00:04:00
   Mode EXCLUDE
Interface GigabitEthernet 2/14, Group ff3e:100::4000:1
   Reporter fe80::200:ff:fe00:0
   Uptime 00:00:16, Expires in 00:04:03
   Mode INCLUDE
      165:87:32::8
      165:87:32::9
      165:87:32::a
   Interface GigabitEthernet 2/14, Group ff3e:100::4000:2
   Reporter fe80::200:ff:fe00:0
   Uptime 00:00:16, Expires in 00:04:03
   Mode INCLUDE
      165:87:32::8
      165:87:32::9
      165:87:32::a
```

Figure 32-1. show ipv6 mld groups Command Example
Enter the keyword **interface** to display the configured MDL interfaces. Optionally, enter the keyword **interface** followed by one of the keywords below, with slot/port or number information, to display information for that specific interface:

- For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
- For a Port Channel interface, enter the keyword **port-channel** followed by a number:
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword **sonet** followed by the slot/port information.
- 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.

**Parameters**

**interface**

*interface*

Enter the keyword **interface** to display the configured MDL interfaces. Optionally, enter the keyword **interface** followed by one of the keywords below, with slot/port or number information, to display information for that specific interface:

- For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
- For a Port Channel interface, enter the keyword **port-channel** followed by a number:
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword **sonet** followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
- For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 7.4.1.0 Introduced

**Example**

**Figure 32-2.  show ipv6 mld interface Command Example**

`FTOS#show ipv6 mld interface
GigabitEthernet 2/14 is up, line protocol is up
  Interface address is fe80::201:e8ff:fe08:9a09/64
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier expiry time is 255 seconds
  MLD max query response time is 10 seconds
  Last member response interval is 1000 ms
  MLD explicit tracking is disabled
  MLD querying router is fe80::201:e8ff:fe08:9a09 (this router)
Port-channel 200 is up, line protocol is up
  Interface address is fe80::201:e8ff:fe08:9abd/64
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier expiry time is 255 seconds
  MLD max query response time is 10 seconds
  Last member response interval is 1000 ms
  MLD explicit tracking is disabled
  MLD querying router is fe80::201:e8ff:fe08:9abd (this router)
Vlan 200 is up, line protocol is up
  Interface address is fe80::201:e8ff:fe08:9abc/64
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier expiry time is 255 seconds
  MLD max query response time is 10 seconds
  Last member response interval is 1000 ms
  MLD explicit tracking is disabled
  MLD querying router is fe80::201:e8ff:fe08:9abc (this router)
FTOS#`
MLD Snooping Commands

The MLD Snooping commands are:

- ipv6 mld snooping enable
- ipv6 mld snooping flood
- ipv6 mld snooping
- ipv6 mld snooping explicit-tracking
- ipv6 mld snooping mrouter
- ipv6 mld snooping querier
- show ipv6 mld snooping groups
- show ipv6 mld snooping mrouter

ipv6 mld snooping enable

Enable MLD Snooping globally.

Syntax
ipv6 mld snooping enable

Defaults
Disabled

Command Modes
CONFIGURATION (conf)

Command History

Version 7.4.1.0 Introduced

ipv6 mld snooping flood

Enable MLD Snooping Flood globally.

Syntax
ipv6 mld snooping flood

To disable, use the no ipv6 mld snooping flood command.

Defaults
Enabled

Command Modes
CONFIGURATION (conf)

Usage Information

When flooding is enabled, unregistered multicast data is flooded on the VLAN.

When flooding is disabled, unregistered multicast data is forwarded only to mrouter ports on the VLAN.

Command History

Version 7.4.1.0 Introduced
ipv6 mld snooping

Enable MLD Snooping (v1 and v2) on a VLAN.

**Syntax**

```
ipv6 mld snooping
```

To disable MLD Snooping, use the `no ipv6 mld snooping` command.

**Defaults**

Enabled on all VLAN interfaces

**Command Modes**

INTERFACE VLAN (conf-if-vl-n)

**Command History**

Version 7.4.1.0 Introduced

**Usage Information**

Whether the switch is the Querier or not, if snooping is enabled, the switch tracks all MLD joins. It has separate explicit tracking table which contains group, source, interface, VLAN and reporter details.

**Related Commands**

- `ipv6 mld snooping mrouter`
- `show ipv6 mld snooping groups`

ipv6 mld snooping explicit-tracking

Enable explicit MLD Snooping tracking on an interface.

**Syntax**

```
ipv6 mld snooping explicit-tracking
```

To disable, use the `no ipv6 mld snooping explicit-tracking` command.

**Defaults**

Disabled

**Command Modes**

INTERFACE VLAN (conf-if-vl-n)

**Command History**

Version 7.4.1.0 Introduced

**Usage Information**

Whether the switch is the Querier or not, if snooping is enabled, the switch tracks all MLD joins. It has separate explicit tracking table which contains group, source, interface, VLAN and reporter details.

**Related Commands**

- `ipv6 mld snooping mrouter`
- `show ipv6 mld snooping groups`

ipv6 mld snooping mrouter

Configure a Layer 2 port as a multicast router port.

**Syntax**

```
ipv6 mld snooping mrouter interface {interface}
```

**Parameters**

- `interface` Enter the keyword `interface` to indicate the next-hop interface to the multicast router.

  **interface**
  
  Enter the following keywords and slot/port or number information:
  
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number: `E-Series` Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

  **Defaults**
  
  No default values or behavior
### Command Modes

**INTERFACE VLAN (conf-if-vl-)**

### Command History

Version 7.4.1.0  Introduced

### ipv6 mld snooping querier

Enable the MLD querier processing for the VLAN interface.

**Syntax**

```
ipv6 mld snooping querier
```

**Defaults**

Disabled

**Command Modes**

INTERFACE VLAN (conf-if-vl-)

**Command History**

Version 7.4.1.0  Introduced

**Usage Information**

This command enables the VLAN to send out periodic queries as a proxy querier. You must configure and IP address for the VLAN.

### show ipv6 mld snooping groups

Display the IPv6 MLD Snooping group information.

**Syntax**

```
show ipv6 mld snooping groups [group-address] [explicit] [link-local] [summary] [vlan]
```

**Parameters**

- **group-address**
  - (OPTIONAL) Enter the multicast group address in the `x:x::x` format. The :: notation specifies successive hexadecimal fields of zero.
- **explicit**
  - (OPTIONAL) Enter the keyword `explicit` to display explicit tracking information.
- **link-local**
  - (OPTIONAL) Enter the keyword `link-local` to display link local groups.
- **summary**
  - (OPTIONAL) Enter the keyword `summary` to display a summary of groups.
- **vlan**
  - (OPTIONAL) Enter the keyword `vlan` followed by the VLAN number to display information on that specific VLAN. Range: 1 - 4094

**Defaults**

No default values or behavior

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 7.4.1.0  Introduced
show ipv6 mld snooping mrouter

Display information on the MLD Snooping router.

Syntax

```
show ipv6 mld snooping mrouter [vlan]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>(OPTIONAL) Enter the keyword <code>vlan</code> followed by the VLAN number to display information on that specific VLAN. Range: 1 - 4094</td>
</tr>
</tbody>
</table>

Defaults

No default values or behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- Introduced in Version 7.4.1.0

Example

```
Figure 32-4. show ipv6 mld snooping mrouter Command Example

FTOS#show ipv6 mld snooping mrouter
Interface Ports (* - Dynamic)
Vlan 2 Gi 13/18
FTOS#
```
Multicast Source Discovery Protocol (MSDP)

Overview

MSDP (Multicast Source Discovery Protocol) connects multiple PIM Sparse-Mode (PIM-SM) domains together. MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections. Dell Networking OS supports MSDP commands on the E-Series only, as indicated by the character that appears below each command heading.

Commands

The commands are:

- clear ip msdp peer
- clear ip msdp sa-cache
- debug ip msdp
- ip msdp cache-rejected-sa
- ip msdp default-peer
- ip msdp log-adjacency-changes
- ip msdp mesh-group
- ip msdp originator-id
- ip msdp peer
- ip msdp redistribute
- ip msdp sa-filter
- ip msdp sa-limit
- ip msdp shutdown
- ip multicast-msdp
- show ip msdp
- show ip msdp sa-cache rejected-sa

**clear ip msdp peer**

Reset the TCP connection to the peer and clear all the peer statistics.

**Syntax**

```
clear ip msdp peer {peer address}
```

**Parameters**

<table>
<thead>
<tr>
<th>peer address</th>
<th>Enter the peer address in a dotted decimal format (A.B.C.D.)</th>
</tr>
</thead>
</table>

**33**
clear ip msdp sa-cache

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Syntax

```
clear ip msdp sa-cache [group-address | rejected-sa | local]
```

Parameters

- **group-address**: Enter the group IP address in dotted decimal format (A.B.C.D.)
- **rejected-sa**: Enter this keyword to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
- **local**: Enter this keyword to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults

Without any options, this command clears the entire source-active cache.

Command Modes

EXEC Privilege

Command History

- **Version 7.8.1.0**: Added **local** option.
- **Version 7.7.1.0**: Added **rejected-sa** option.
- **Version 6.2.1.1**: Introduced

debug ip msdp

Turn on MSDP debugging.

Syntax

```
depag ip msdp {event peer address | packet peer address | pim}
```

To turn debugging off, use the **no debug ip msdp {event peer address | packet peer address | pim}** command.

Parameters

- **event peer address**: Enter the keyword **event** followed by the peer address in a dotted decimal format (A.B.C.D.).
- **packet peer address**: Enter the keyword **packet** followed by the peer address in a dotted decimal format (A.B.C.D.).
- **pim**: Enter the keyword **pim** to debug advertisement from PIM.

Defaults

Not configured

Command Modes

EXEC Privilege
ip msdp cache-rejected-sa

Enable a MSDP cache for the rejected source-active entries.

Syntax

```
ip msdp cache-rejected-sa {number}
```

To clear the MSDP rejected source-active entries, use the `no ip msdp cache-rejected-sa {number}` command followed by the `ip msdp cache-rejected-sa {number}` command.

Parameters

- **number**: Enter the number of rejected SA entries to cache. 
  Range: 0 to 32766

Defaults

No default values or behavior

Command Modes

CONFIGURATION

Usage Information

If a list is not specified, all SA messages received from the default peer are accepted. You can enter multiple default peer commands.

Related Commands

- **show ip msdp sa-cache rejected-sa**: Description.
**ip msdp log-adjacency-changes**

Enable logging of MSDP adjacency changes.

**Syntax**

```
ip msdp log-adjacency-changes
```

To disable logging, use the **no ip msdp log-adjacency-changes** command.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION

**Command History**

| Version 6.2.1.1 | Introduced |

**ip msdp mesh-group**

Configure a peer to be a member of a mesh group.

**Syntax**

```
ip msdp mesh-group {name} {peer address}
```

To remove the peer from a mesh group, use the **no ip msdp mesh-group {name} {peer address}** command.

**Parameters**

- **name**
  - Enter a string of up to 16 characters long for as the mesh group name.

- **peer address**
  - Enter the peer address in a dotted decimal format (A.B.C.D.)

**Defaults**

Not configured

**Command Modes**

CONFIGURATION

**Command History**

| Version 6.2.1.1 | Introduced |

**Usage Information**

A MSDP mesh group is a mechanism for reducing SA flooding, typically in an intra-domain setting. When some subset of a domain’s MSDP speakers are fully meshed, they can be configured into a mesh-group. If member $X$ of a mesh-group receives a SA message from an MSDP peer that is also a member of the mesh-group, member $X$ accepts the SA message and forwards it to all of its peers that are not part of the mesh-group. However, member $X$ can not forward the SA message to other members of the mesh-group.

**ip msdp originator-id**

Configure the MSDP Originator ID.

**Syntax**

```
  ip msdp originator-id {interface}
```

To remove the originator-id, use the **no ip msdp originator-id {interface}** command.
Parameters

<table>
<thead>
<tr>
<th>interface</th>
<th>Enter the following keywords and slot/port or number information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For a Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a Loopback interface, enter the keyword loopback followed by a number from 0 to 16383.</td>
<td></td>
</tr>
<tr>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td>• For a SONET interface, enter the keyword sonet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.</td>
<td></td>
</tr>
</tbody>
</table>

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 6.2.1.1 Introduced

ip msdp peer

Configure an MSDP peer.

Syntax

```
ip msdp peer peer address [connect-source] [description] [sa-limit number]
``` 

To remove the MSDP peer, use the `no ip msdp peer peer address [connect-source interface] [description name] [sa-limit number]` command.

Parameters

<table>
<thead>
<tr>
<th>peer address</th>
<th>Enter the peer address in a dotted decimal format (A.B.C.D.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect-source interface</td>
<td>(OPTIONAL) Enter the keyword connect-source followed by one of the interfaces and slot/port or number information:</td>
</tr>
<tr>
<td>• For a Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a Loopback interface, enter the keyword loopback followed by a number from 0 to 16383.</td>
<td></td>
</tr>
<tr>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td>• For a SONET interface, enter the keyword sonet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
<td></td>
</tr>
<tr>
<td>• For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.</td>
<td></td>
</tr>
</tbody>
</table>
### Multicast Source Discovery Protocol (MSDP)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip msdp redistribute</td>
<td>Filter local PIM SA entries in the SA cache. SAs which are denied by the ACL will time out and not be refreshed. Until they time out, they will continue to reside in the MSDP SA cache.</td>
</tr>
</tbody>
</table>

#### Syntax

```
ip msdp redistribute [list acl-name]
```

#### Parameters

- **list acl-name**: Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

#### Defaults

Not configured

#### Command Modes

CONFIGURATION

#### Command History

Version 7.8.1.0 Introduced

#### Usage Information

Modifications to the ACL will not have an immediate affect on the sa-cache.

To apply the redistribute filter to entries already present in the SA cache, use `clear ip msdp sa-cache local`. 

### ip msdp redistribute

Filter local PIM SA entries in the SA cache. SAs which are denied by the ACL will time out and not be refreshed. Until they time out, they will continue to reside in the MSDP SA cache.

#### Syntax

```
ip msdp redistribute [list acl-name]
```

#### Parameters

- **list acl-name**: Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

#### Defaults

Not configured

#### Command Modes

CONFIGURATION

#### Command History

Version 7.8.1.0 Introduced

#### Usage Information

Modifications to the ACL will not have an immediate affect on the sa-cache.

To apply the redistribute filter to entries already present in the SA cache, use `clear ip msdp sa-cache local`. 

### description name

(Optional) Enter the keyword `description` followed by a description name (max 80 characters) to designate a description for the MSDP peer.

### sa-limit number

(Optional) Enter the maximum number of SA entries in SA-cache. Range: 1 to 500000 Default: 500000

#### Defaults

As above

#### Command Modes

CONFIGURATION

#### Command History

Version 7.5.1.0 Added option for SA upper limit and description option

Version 6.2.1.1 Introduced

#### Usage Information

The `connect-source` option is used to supply a source IP address for the TCP connection. When an interface is specified using the `connect-source` option, the primary configured address on the interface is used.

If the total number of SA messages received from the peer is already larger than the limit when this command is applied, those SA messages will continue to be accepted. To enforce the limit in such situation, use command `clear ip msdp peer` command to reset the peer.
ip msdp sa-filter

Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.

Syntax

```
ip msdp sa-filter {in | out} peer-address list [access-list name]
```

Remove this configuration using the command `no ip msdp sa-filter {in | out} peer address list [access-list name]`

Parameters

- **in**: Enter the keyword `in` to enable incoming SA filtering.
- **out**: Enter the keyword `out` to enable outgoing SA filtering.
- **peer-address**: Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.).
- **access-list name**: (OPTIONAL) Enter the IP extended access list name that defines from which peers SAs are to be permitted or denied.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

```
Version 7.7.1.0 Introduced on E-Series
```

ip msdp sa-limit

Configure the upper limit of SA (Source-Active) entries in SA-cache.

Syntax

```
ip msdp sa-limit number
```

To return to the default, use the `no ip msdp sa-limit number` command.

Parameters

- **number**: Enter the maximum number of SA entries in SA-cache. Range 0 to 40000

Defaults

Default 50000

Command Modes

CONFIGURATION

Command History

```
Version 7.5.1.0 Introduced
```

Usage Information

Dell Networking OS counts the SA messages originated by itself and those received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking). If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in Dell Networking OS will continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp sa-cache` command.
ip msdp shutdown

Administratively shut down a configured MSDP peer.

Syntax

`ip msdp shutdown {peer address}`

Parameters

- `peer address`: Enter the peer address in a dotted decimal format (A.B.C.D.)

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 6.2.1.1 Introduced

ip multicast-msdp

Enable MSDP.

Syntax

`ip multicast-msdp`

To exit MSDP, use the `no ip multicast-msdp` command.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 6.2.1.1 Introduced

show ip msdp

Display the MSDP peer status, SA cache, or peer summary.

Syntax

`show ip msdp {peer peer address | sa-cache | summary}`

Parameters

- `peer peer address`: Enter the keyword `peer` followed by the peer address in a dotted decimal format (A.B.C.D.)
- `sa-cache`: Enter the keyword `sa-cache` to display the Source-Active cache.
- `summary`: Enter the keyword `summary` to display a MSDP peer summary.

Defaults

Not configured
show ip msdp sa-cache rejected-sa

Display the rejected SAs in the SA cache.

Syntax

show ip msdp sa-cache rejected-sa

Defaults

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.4.1.0 Introduced
### Figure 33-4. show ip msdp sa-cache rejected-sa Command Example

FTOS#sh ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache  200 rejected SAs received, cache-size 1000

<table>
<thead>
<tr>
<th>UpTime</th>
<th>GroupAddr</th>
<th>SourceAddr</th>
<th>RPAddr</th>
<th>LearnedFrom</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:13</td>
<td>225.1.2.1</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.2</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.3</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.4</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.5</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.6</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.7</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.8</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.9</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.10</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.11</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.12</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.13</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.14</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.15</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.16</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.17</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.18</td>
<td>10.1.1.4</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
<tr>
<td>00:00:13</td>
<td>225.1.2.19</td>
<td>10.1.1.3</td>
<td>110.1.1.1</td>
<td>13.1.1.2</td>
<td>Rpf-Fail</td>
</tr>
</tbody>
</table>

FTOS#
Multiple Spanning Tree Protocol (MSTP)

Overview

Multiple Spanning Tree Protocol (MSTP), as implemented by Dell Networking OS, conforms to IEEE 802.1s. MSTP is supported by Dell Networking OS on all Dell Networking systems (C-Series, E-Series, and S-Series), as indicated by the characters that appear below each command heading:

- C-Series: C
- E-Series: E
- S-Series: S

Commands

The following commands configure and monitor MSTP:

- debug spanning-tree mstp
- disable
- forward-delay
- 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 Multiple Spanning Tree Protocol and view information on the protocol.

**Syntax**

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

To disable debugging, enter `no debug spanning-tree mstp`.

**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 Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
  Optional, 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 8.4.6.0 Added support for the keyword `fortyGigE`.
- Version 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

**Example**

```
Figure 34-1. debug spanning-tree mstp bpdu Command Example

FTOS#debug spanning-tree mstp bpdu gigabitethernet 2/0 ?
in Receive (in)  out Transmit (out)
```
description

- Enter a description of the Multiple Spanning Tree

**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**

No default behavior or values

**Command Modes**

SPANNING TREE (The prompt is “config-mstp”.)

**Command History**

- Introduced

**Related Commands**

- `protocol spanning-tree mstp` Enter Multiple SPANNING TREE mode on the switch.

disable

- Globally disable Multiple Spanning Tree Protocol on the switch.

**Syntax**

```
disable
```

To enable Multiple Spanning Tree Protocol, enter `no disable`.

**Defaults**

Multiple Spanning Tree Protocol is disabled

**Command Modes**

MULTIPLE SPANNING TREE

**Command History**

- Version 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- Introduced

**Related Commands**

- `protocol spanning-tree mstp` Enter MULTIPLE SPANNING TREE mode.
forward-delay

Syntax

forward-delay seconds

Parameters

seconds Enter the number of seconds the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
Range: 4 to 30
Default: 15 seconds.

Defaults

15 seconds

Command Modes

MULTIPLE SPANNING TREE

Command History

Version 7.6.1.0 Added support for S-Series
Version 7.5.1.0 Added support for C-Series
Version 6.5.1.0 Introduced

Related Commands

max-age Change the wait time before MSTP refreshes protocol configuration information.
hello-time Change the time interval between BPDUs.

hello-time

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 7.6.1.0 Added support for S-Series
Version 7.5.1.0 Added support for C-Series
Version 6.5.1.0 Introduced
max-age

Set the time interval for the Multiple Spanning Tree bridge to maintain configuration information before refreshing that information.

Syntax

```
max-age seconds
```

To return to the default values, enter **no max-age**.

Parameters

```
max-age
```

Enter a number of seconds the FTOS waits before refreshing configuration information.

- **Range:** 6 to 40
- **Default:** 20 seconds.

Defaults

20 seconds

Command Modes

MULTIPLE SPANNING TREE

Command History

- **Version 7.6.1.0** Added support for S-Series
- **Version 7.5.1.0** Added support for C-Series
- **Version 6.5.1.0** Introduced

Related Commands

- **forward-delay** The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
- **hello-time** Change the time interval between BPDUs.
### max-hops

Configure the maximum hop count.

**Syntax**

```
max-hops number
```

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

**Parameters**

- `range`
  - Enter a number for the maximum hop count.
  - Range: 1 to 40
  - Default: 20

**Defaults**

20 hops

**Command Modes**

MULTIPLE SPANNING TREE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced</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 `no msti instance {vlan range | bridge-priority priority}`

**Parameters**

- `msti instance`
  - Enter the Multiple Spanning Tree Protocol Instance
  - Range: zero (0) to 63

- `vlan range`
  - Enter the keyword `vlan` followed by the identifier range value.
  - Range: 1 to 4094

- `bridge-priority priority`
  - Enter the keyword `bridge-priority` followed by a value in increments of 4096 as the bridge priority.
  - Range: zero (0) to 61440
  - Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

**Defaults**

default bridge-priority is 32768

**Command Modes**

INTERFACE
By default, all VLANs are mapped to MST instance zero (0) unless you use the `vlan range` command to map it to a non-zero instance.

### name

The name you assign to the Multiple Spanning Tree region.

**Syntax**

```
name region-name
```

To remove the region name, enter `no name`

**Parameters**

- `region-name` (required)
  
  Enter the MST region name.
  
  Range: 32 character limit

**Defaults**

```
no default name
```

**Command Modes**

MULTIPLE SPANNING TREE

**Command History**

- **Version 7.6.1.0 Added support for S-Series**
- **Version 7.5.1.0 Added support for C-Series**
- **Version 6.5.1.0 Introduced**

**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` Map the VLAN(s) to an MST instance
- `revision` Assign revision number to the MST configuration.
**protocol spanning-tree mstp**

Enter the 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, enter `no protocol spanning-tree mstp` command.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.6.1.0  Added support for S-Series
- Version 7.5.1.0  Added support for C-Series
- pre-Version 6.2.1.1  Introduced on E-Series

**Example**

```
FTOS(conf)#protocol spanning-tree mstp
FTOS(config-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.

Refer to the *FTOS Configuration Guide* for more information on Multiple Spanning Tree Protocol.

**Related Commands**

- `disable`  Disable Multiple Spanning Tree.

**Defaults**

Disable.

**Command Modes**

MULTIPLE SPANNING TREE

**Usage Information**

Refer to the *FTOS Configuration Guide* for more information on Multiple Spanning Tree Protocol.
**revision**

The revision number for the Multiple Spanning Tree configuration

**Syntax**  
revision range

To return to the default values, enter no revision.

**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 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- Version 6.5.1.0 Introduced

**Usage Information**

For two MSTP switches to be within the same MST region, the switches must share the same revision number.

**Related Commands**

- msti Map the VLAN(s) to an MST instance
- name Assign 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

**Command History**

- Version 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- Version 6.5.1.0 Introduced on E-Series

**Example**

Figure 34-3. show config Command for MULTIPLE SPANNING TREE Mode

```
FTOS(conf-mstp)#show config
!
protocol spanning-tree mstp
no disable
name CustomerSvc
revision 2
MSTI 10 VLAN 101-105
max-hops 5
FTOS(conf-mstp)#
```
show spanning-tree mst configuration

View the Multiple Spanning Tree configuration.

Syntax  show spanning-tree mst configuration

Command Modes  EXEC

  EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Example  Figure 34-4.  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 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 Multiple Spanning Tree Protocol prior to using this command.

Command History

- Version 8.5.1.0 Support for the optional `guard` keyword was added on the E-Series ExaScale.
- Version 8.4.2.1 Support for the optional `guard` keyword was added on the C-Series, S-Series, and E-Series TeraScale.
- Version 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- Version 6.4.1.0 Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency (see Figure 34-6)

Example

```
Figure 34-5. show spanning-tree msti [instance-number] Command Example

FTOS#show spanning-tree msti 10
MSTI 10 VLANs mapped 101-105
Bridge Identifier has priority 32768, Address 0001.e802.3506
Configured hello time 2, max age 20, forward delay 15, max hops 5
Current root has priority 16384, Address 0001.e800.0a5c
Number of topology changes 0, last change occurred 3058087

Port 82 (GigabitEthernet 2/0) is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.82
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 32768, address 0001.e802.35:06
Designated port id is 128.82, designated path cost
Number of transitions to forwarding state 1
BPDU (Mrecords): sent 1109, received 0
The port is not in the portfast mode

Port 88 (GigabitEthernet 2/6) is root Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.88
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.88, designated path cost
Number of transitions to forwarding state 4
BPDU (Mrecords): sent 19, received 1103
The port is not in the portfast mode

Port 89 (GigabitEthernet 2/7) is alternate Discarding
Port path cost 0, Port priority 128, Port Identifier 128.89
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.89, designated path cost
Number of transitions to forwarding state 3
BPDU (Mrecords): sent 7, received 1103
The port is not in the portfast mode
```
### Example 2  
**Figure 34-6. show spanning-tree msti 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

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts</th>
<th>Bridge ID</th>
<th>PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 0/0</td>
<td>128.257</td>
<td>128</td>
<td>20000</td>
<td>EDS</td>
<td>32768</td>
<td>0001.e801.6aa8 128.257</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Role</th>
<th>PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts</th>
<th>Bridge ID</th>
<th>PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 0/0</td>
<td>ErrDis</td>
<td>128.257</td>
<td>128</td>
<td>20000</td>
<td>EDS</td>
<td>32768</td>
<td>0001.e801.6aa8 128.257</td>
</tr>
</tbody>
</table>

FTOS#show spanning-tree msti 0
MSTI 0 VLANs mapped 1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occurred 00:00:15 ago on Gi 0/0

Port 257 (GigabitEthernet 0/0) is LBK_INC Discarding
Loopback BPDU Inconsistency (LBK_INC)
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode

### Example 3  
**Figure 34-7. show spanning-tree msti guard Command Example**

FTOS#show spanning-tree msti 5 guard

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Instance</th>
<th>Sts</th>
<th>Guard Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>GL 0/1</td>
<td>5</td>
<td>INCON(Root)</td>
<td>Rootguard</td>
</tr>
<tr>
<td>GL 0/2</td>
<td>5</td>
<td>FWD</td>
<td>Loopguard</td>
</tr>
<tr>
<td>GL 0/3</td>
<td>5</td>
<td>EDS(Shut)</td>
<td>Bpduguard</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>MSTP interface</td>
</tr>
<tr>
<td>Instance</td>
<td>MSTP instance</td>
</tr>
<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>
spanning-tree

Enable Multiple Spanning Tree Protocol on the interface.

Syntax

spanning-tree

To disable the Multiple Spanning Tree Protocol on the interface, use no spanning-tree

Parameters

spanning-tree Enter the keyword spanning-tree to enable the MSTP on the interface. Default: Enable

Defaults

Enable

Command Modes

INTERFACE

Command History

- Version 7.6.1.0 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- pre-Version 6.2.1.0 Introduced on E-Series

spanning-tree msti

Configure Multiple Spanning Tree instance cost and priority for an interface.

Syntax

spanning-tree msti instance {cost cost | priority priority}

Parameters

msti instance Enter the keyword msti and the MST Instance number.
Range: zero (0) to 63

cost cost (OPTIONAL) Enter the keyword cost followed by the port cost value.
Range: 1 to 200000
Defaults:
- 100 Mb/s Ethernet interface = 200000
- 1-Gigabit Ethernet interface = 20000
- 10-Gigabit Ethernet interface = 2000
- Port Channel interface with one 100 Mb/s Ethernet = 200000
- Port Channel interface with one 1-Gigabit Ethernet = 20000
- Port Channel interface with one 10-Gigabit Ethernet = 2000
- Port Channel with two 1-Gigabit Ethernet = 18000
- Port Channel with two 10-Gigabit Ethernet = 1800
- Port Channel with two 100-Mbps Ethernet = 180000

priority priority Enter keyword priority followed by a value in increments of 16 as the priority.
Range: 0 to 240.
Default: 128

Defaults

cost = depends on the interface type; priority = 128

Command Modes

INTERFACE
spanning-tree mstp

Configures a Layer 2 MSTP interface as an edge port with (optionally) a Bridge Protocol Data Unit (BPDU) guard, or enables the root guard or loop guard feature on the interface.

Syntax

spanning-tree mstp {edge-port [bpduguard [shutdown-on-violation]] | loopguard | 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 *portfast* to enable Portfast 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.
- **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.
- **loopguard**: Enter the keyword *loopguard* to enable STP loop guard on an MSTP port or port-channel interface.
- **rootguard**: Enter the keyword *rootguard* to enable root guard on an MSTP port or port-channel interface.

Command Modes

**INTERFACE**

Command History

- **Version 8.5.1.0**: Introduced the *loopguard* and *rootguard* options on the E-Series ExaScale.
- **Version 8.4.2.1**: Introduced the *loopguard* and *rootguard* options on the E-Series TeraScale, C-Series, and S-Series.
- **Version 8.2.1.0**: Introduced hardware shutdown-on-violation option
- **Version 7.6.1.0**: Added support for S-Series
- **Version 7.5.1.0**: Added support for C-Series
- **Version 6.1.1.0**: Support for BPDU guard added

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.

If *shutdown-on-violation* is not enabled, BPDUs will still be sent to the RPM CPU.

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 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Added support for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

By default Dell Networking OS 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, this *knob* command can be turned on to enable flushing MAC addresses upon receiving every topology change notification.
Multicast

Overview

The platforms on which a command is supported is indicated by the character — E for the E-Series, C for the C-Series, and S for the S-Series — that appears below each command heading.

This chapter contains the following sections:

- IPv4 Multicast Commands
- IPv6 Multicast Commands

IPv4 Multicast Commands

The IPv4 Multicast commands are:

- clear ip mroute
- clear ip mroute snooping
- ip mroute
- ip multicast-lag-hashing
- ip multicast-mode l2
- ip multicast-routing
- ip multicast-limit
- mac-address-table static
- mac-flood-list
- mtrace
- queue backplane multicast
- restrict-flooding
- show ip mroute
- show ip rpf
- show mac-address-table static multicast
- show queue backplane multicast
clear ip mroute

Clear learned multicast routes on the multicast forwarding table. To clear the PIM tree information base, use `clear ip pim tib` command.

**Syntax**
```
clear ip mroute {group-address [source-address] | *}
```

**Parameters**
- `group-address` Enter multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
- `source-address` (OPTIONAL) Enter source address.
- `*` Enter * to clear all multicast routes.

**Command Modes**
EXEC Privilege

**Command History**
- Version 7.8.1.0 Introduced on C-Series
- E-Series legacy command

**Related Commands**
- `show ip pim tib` Show the PIM Tree Information Base.

---

clear ip mroute snooping

Clear the multicast routes learned through PIM-SM snooping from the IPv4 multicast snooping table. To clear tree information learned through PIM-SM snooping from the PIM tree information base, use `clear ip pim snooping tib` command.

**Syntax**
```
clear ip mroute snooping {vlan vlan-id [group-address [source-address] | *]}
```

**Parameters**
- `vlan vlan-id` Enter a VLAN ID to clear information learned through PIM-SM snooping about a specified VLAN. Valid VLAN IDs: 1 to 4094.
- `group-address` (OPTIONAL) Enter a group address and, optionally, a source address in dotted decimal format, to clear information learned through PIM-SM snooping about a specified multicast group and source.
- `source-address` (OPTIONAL) Enter source address.
- `*` Enter * to clear all multicast routes learned through PIM-SM snooping.

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.4.1.1 Introduced on E-Series ExaScale

**Related Commands**
- `show ip pim snooping tib` Display the information from the PIM tree information base learned through PIM snooping.
### ip mroute

Assign a static mroute.

**Syntax**

```
ip mroute destination mask {ip-address | null 0 | {bgp | ospf | isis | rip | static} {ip-address | tag | null 0}} [distance]
```

To delete a specific static mroute, use the command `ip mroute destination mask {ip-address | null 0 | {bgp | ospf | isis | rip | static} {ip-address | tag | null 0}} [distance].`

To delete all mroutes matching a certain mroute, use the `no ip mroute destination mask` command.

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination</strong></td>
<td>Enter the IP address in dotted decimal format of the destination device.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>Enter the mask in slash prefix formation (/x) or in dotted decimal format.</td>
</tr>
<tr>
<td><strong>null 0</strong></td>
<td>(OPTIONAL) Enter the null followed by zero (0).</td>
</tr>
<tr>
<td>**[protocol [process-id</td>
<td>tag] ip-address]**</td>
</tr>
<tr>
<td></td>
<td>- Enter the BGP as-number followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.</td>
</tr>
<tr>
<td></td>
<td>- Range: 1-65535</td>
</tr>
<tr>
<td></td>
<td>- Enter the OSPF process identification number followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.</td>
</tr>
<tr>
<td></td>
<td>- Range: 1-65535</td>
</tr>
<tr>
<td></td>
<td>- Enter the IS-IS alphanumeric tag string followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.</td>
</tr>
<tr>
<td></td>
<td>- Enter the RIP IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.</td>
</tr>
<tr>
<td><strong>static ip-address</strong></td>
<td>(OPTIONAL) Enter the Static IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.</td>
</tr>
<tr>
<td><strong>ip-address</strong></td>
<td>(OPTIONAL) Enter the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.</td>
</tr>
<tr>
<td><strong>distance</strong></td>
<td>(OPTIONAL) Enter a number as the distance metric assigned to the mroute.</td>
</tr>
<tr>
<td></td>
<td>- Range: 0 to 255</td>
</tr>
</tbody>
</table>

#### Defaults

Not configured.

#### Command Modes

- **CONFIGURATION**

#### Command History

E-Series legacy command

#### Related Commands

- `show ip mroute` View the E-Series routing table.
ip multicast-lag-hashing

Distribute multicast traffic among Port Channel members in a round-robin fashion.

Syntax

ip multicast-lag-hashing

To revert to the default, enter no ip multicast-lag-hashing.

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

Version 6.3.1.0 Introduced for E-Series

Usage Information

By default, one Port Channel member is chosen to forward multicast traffic. With this feature turned on, multicast traffic will be distributed among the Port Channel members in a round-robin fashion. This feature applies to the routed multicast traffic. If IGMP Snooping is turned on, this feature also applies to switched multicast traffic.

Related Commands

ip multicast-routing Enable IP multicast forwarding.
**ip multicast-limit**

Use this feature to limit the number of multicast entries on the system.

**Syntax**

```
ip multicast-limit limit
```

**Parameters**

- `limit` Enter the desired maximum number of multicast entries on the system.
  
  - **E-Series Range:** 1 to 50000
  - **E-Series Default:** 15000
  - **C-Series Range:** 1 to 10000
  - **C-Series Default:** 4000
  - **S-Series Range:** 1 to 2000
  - **S-Series Default:** 400

**Defaults**

As above

**Command Modes**

CONFIGURATION

**Command History**

- **Version 7.8.1.0** Introduced on C-Series
- **Version 7.6.1.0** Introduced on E-Series

**Usage Information**

This feature allows the user to limit the number of multicast entries on the system. This number is the sum total of all the multicast entries on all line cards in the system. On each line card, the multicast module will only install the maximum possible number of entries, depending on the configured CAM profile.

The IN-L3-McastFib CAM partition is used to store multicast routes and is a separate hardware limit that exists per port-pipe. Any software-configured limit might be superseded by this hardware space limitation. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the ip multicast-limit is reached.

**Related Commands**

- `show ip igmp groups`
**ip multicast-mode l2**

Enable Layer 2 multicast switching.

**Syntax**

```
ip multicast-mode l2
```

To return to the default Layer 3 multicast forwarding on the router, enter the `no ip multicast-mode l2` command after you remove the static multicast MAC address (`no mac-address-table static multicast-multicast-mac-address` command).

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

Version 8.4.2.5 Introduced on C-Series.

**Usage Information**

When a multicast source and multicast receivers are in the same VLAN, you can configure a router so that multicast traffic is switched only to the ports assigned to a VLAN that is associated with a static multicast MAC address. However, before you can configure a static MAC address and associate it with a VLAN used to switch Layer 2 multicast traffic, you must enable the router for Layer 2 multicast switching with the `ip multicast-mode l2` command.

**Related Commands**

- `mac-address-table static` - Configure a static multicast MAC address, associate the multicast MAC address with the Layer 2 VLAN used to switch multicast traffic, and add output ports.

---

**ip multicast-routing**

Enable IP multicast forwarding.

**Syntax**

```
ip multicast-routing
```

To disable multicast forwarding, enter `no ip multicast-routing`.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

- E-Series legacy command

**Usage Information**

You must enter this command to enable multicast on the E-Series.

After you enable multicast, you can enable IGMP and PIM on an interface. In the INTERFACE mode, enter the `ip pim sparse-mode` command to enable IGMP and PIM on the interface.

**Related Commands**

- `ip pim sparse-mode` - Enable IGMP and PIM on an interface.
mac-address-table static

Configure a static multicast MAC address, associate the multicast MAC address with the VLAN used to switch Layer 2 multicast traffic, and add output ports that will receive multicast streams on the VLAN.

To delete a configured static multicast MAC address from the MAC address table on the router, enter the no mac-address-table static multicast-mac-address command.

Syntax

mac-address-table static multicast-mac-address multicast vlan vlan-id range-output {single-interface | interface-list | interface-range}

To return to the default Layer 3 multicast forwarding on the router, enter the no ip multicast-mode l2 command after you remove the static multicast MAC address (no mac-address-table static multicast vlan output-range command).

Parameters

mac-address-table static multicast-mac-address Enter a 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format for the static MAC address to be used to switch multicast traffic.

multicast vlan vlan-id Enter the VLAN ID of the VLAN used to switch Layer 2 multicast traffic. VLAN ID range: 1 to 4094.

range-output {single-interface | interface-list | interface-range} Specify the output ports to be added to the multicast VLAN used to switch multicast traffic as follows:

range-output single-interface: Enter one of the following port types:
- 1-Gigabit Ethernet: Enter gigabitethernet slot/port.
- 10-Gigabit Ethernet: Enter tengigabitethernet slot/port.
- Port channel: Enter port-channel {1-128}.

range-output interface-list: Enter multiple ports separated by a space, comma, and space; for example:
tengigabitethernet 0/1, gigabitethernet 0/3, ...

range-output interface-range: Enter a port range in the format:
interface-type slot/first_port - last_port; for example:
tengigabitethernet 0/1 - 3

Defaults

Unconfigured

Command Modes

CONFIGURATION

Command History

Version 8.4.2.5 Introduced on C-Series.

Usage Information

When a multicast source and multicast receivers are in the same VLAN, you can configure a router so that multicast traffic is switched only to the ports assigned to a VLAN that is associated with a static multicast MAC address. However, before you can configure a static MAC address and associate it with a VLAN used to switch Layer 2 multicast traffic, you must first enable the router for Layer 2 multicast switching with the ip multicast-mode l2 command.

Related Commands

ip multicast-mode l2 Enable Layer 2 multicast switching.
mac-flood-list

This command provides an exception to the restrict-flood configuration so that multicast frames within a specified MAC address range to be flooded on all ports in a VLAN.

Syntax

```
mac-flood-list mac-address mask vlan vlan-list [min-speed speed]
```

Parameters

- **mac-address**: Enter a multicast MAC address in hexadecimal format.
- **mac-mask**: Enter the MAC Address mask.
- **vlan vlan-list**: Enter the VLAN(s) in which flooding will be restricted. Separate values by commas—no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3).
  
  Range: 1 to 4094
- **min-speed min-speed**: (OPTIONAL) Enter the minimum link speed that ports must have to receive the specified flooded multicast traffic.

Defaults

None

Command Modes

- **CONFIGURATION**

Command History

- **Version 7.7.1.0**: Introduced on E-Series

Usage Information

When the `mac-flood-list` with the `min-speed` option is used in combination with the restrict-flood command, `mac-flood-list` command has higher priority than the `restrict-flood` command.

Therefore, all multicast frames matching the mac-address range specified using the `mac-flood-list` command are flooded according to the `mac-flood-list` command. Only the multicast frames not matching the mac-address range specified using the `mac-flood-list` command are flooded according to the `restrict-flood` command.

Related Commands

- `restrict-flooding`: Prevent Layer 2 multicast traffic from being forwarded on ports below a specified speed.
mtrace

Trace a multicast route from the source to the receiver.

Syntax

mtrace {source-address/hostname} {destination-address/hostname} {group-address}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-address/</td>
<td>Enter the source IP address in dotted decimal format (A.B.C.D).</td>
</tr>
<tr>
<td>hostname</td>
<td></td>
</tr>
<tr>
<td>destination-address/</td>
<td>Enter the destination (receiver) IP address in dotted decimal format (A.B.C.D).</td>
</tr>
<tr>
<td>hostname</td>
<td></td>
</tr>
<tr>
<td>group-address</td>
<td>Enter the multicast group address in dotted decimal format (A.B.C.D).</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Expanded to support originator</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Expanded to support intermediate (transit) router</td>
</tr>
<tr>
<td>E-Series</td>
<td>E-Series legacy command</td>
</tr>
</tbody>
</table>

Usage Information

Mtrace is an IGMP protocol based on the Multicast trace route facility and implemented according to the IETF draft “A trace route facility for IP Multicast” (draft-fenner-traceroute-ipm-01.txt). Dell Networking OS supports the Mtrace client and transmit functionality.

As an Mtrace client, Dell Networking OS transmits Mtrace queries, receives, parses and prints out the details in the response packet received.

As an Mtrace transit or intermediate router, Dell Networking OS returns the response to Mtrace queries. Upon receiving the Mtrace request, Dell Networking OS computes the RPF neighbor for the source, fills in the request and forwards the request to the RPF neighbor. While computing the RPF neighbor, the static mroute and mBGP route is preferred over the unicast route.
queue backplane multicast

Reallocation the amount of bandwidth dedicated to multicast traffic.

Syntax

```
queue backplane multicast bandwidth-percentage percentage
```

Parameters

- `percentage` Enter the percentage of backplane bandwidth to be dedicated to multicast traffic.
  Range: 5-95

Defaults

80% of the scheduler weight is for unicast traffic and 20% is for multicast traffic by default.

Command Modes

CONFIGURATION

Command History

- **Version 7.7.1.0** Introduced on E-Series

Example

```
Figure 35-1.  queue backplane multicast Command Example

FTOS(conf)#queue backplane multicast bandwidth-percent 30
FTOS(conf)#exit
FTOS#00:14:04: %RPM0-P:CP %SYS-5-CONFIG_I: Configured from console by console
show run | grep bandwidth
queue backplane multicast bandwidth-percent 30
FTOS#
```

Related Commands

- `show queue backplane multicast` Display the backplane bandwidth configuration about how much bandwidth is dedicated to multicast versus unicast.
restrict-flooding

Prevent Layer 2 multicast traffic from being flooded on ports below a specified link speed.

Syntax

```
restrict-flooding multicast min-speed speed
```

Parameters

- **min-speed**  
  - Enter the minimum link speed that a port must have to receive flooded multicast traffic.  
  - Range: 1000

Defaults

None

Command Modes

INTERFACE VLAN

Command History

Version 7.7.1.0  
Introduced on E-Series TeraScale

Usage Information

This command restricts flooding for all unknown multicast traffic on ports below a certain speed. If you want some multicast traffic to be flooded on slower ports, use the command `mac-flood-list` without the `min-speed` option, in combination with `restrict-flooding`. With `mac-flood-list` you specify the traffic you want to be flooded using a MAC address range.

You may not use unicast MAC addresses when specifying MAC address ranges, and do not overlap MAC addresses ranges, when creating multiple `mac-flood-list` entries for the same VLAN. Restricted Layer 2 Flooding is not compatible with MAC accounting or VLANs.

Related Commands

- `mac-flood-list`  
  - Flood multicast frames with specified MAC addresses to all ports in a VLAN.
**show ip mroute**

View the Multicast Routing Table.

**Syntax**

```
show ip mroute [static | group-address [source-address] | active [rate] | count | snooping [vlan vlan-id] [group-address [source-address]] | summary]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static</strong></td>
<td>(OPTIONAL) Enter the keyword <code>static</code> to view static multicast routes.</td>
</tr>
<tr>
<td><strong>group-address</strong></td>
<td>(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.</td>
</tr>
<tr>
<td><strong>active [rate]</strong></td>
<td>(OPTIONAL) Enter the keyword <code>active</code> to view only active multicast routes. Enter a rate to view active routes over the specified rate. Range: 0 to 1000000</td>
</tr>
<tr>
<td><strong>count</strong></td>
<td>(OPTIONAL) Enter the keyword <code>count</code> to view the number of multicast routes and packets on the E-Series.</td>
</tr>
<tr>
<td><strong>snooping [vlan vlan-id] [group-address [source-address]]</strong></td>
<td>(OPTIONAL) E-Series ExaScale only: Enter the keyword <code>snooping</code> to display information on the multicast routes discovered by PIM-SM snooping. Enter a VLAN ID to limit the information displayed to the multicast routes discovered by PIM-SM snooping on a specified VLAN. Valid VLAN IDs: 1 to 4094. Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes discovered by PIM-SM snooping for a specified multicast group and source.</td>
</tr>
<tr>
<td><strong>summary</strong></td>
<td>(OPTIONAL) Enter the keyword <code>summary</code> to view routes in a tabular format.</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- **Version 8.4.1.1** Support for the `snooping` keyword and optional `vlan vlan-id, group-address, and source-address` parameters were added on E-Series ExaScale.
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series

**Example 1**

**Figure 35-2. show ip mroute static Command Example**

```
FTOS#show ip mroute static
Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change: 00:00:23
```
Example 2  

**Figure 35-3. show ip mroute snooping Command Example**

```
FTOS#show ip mroute snooping
IPv4 Multicast Snooping Table
(*, 224.0.0.0), uptime 17:46:23
    Incoming vlan: Vlan 2
    Outgoing interface list:
        GigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
    Incoming vlan: Vlan 2
    Outgoing interface list:
        GigabitEthernet 4/11
        GigabitEthernet 4/13

{165.87.1.7, 225.1.2.1}, uptime 00:03:17
    Incoming vlan: Vlan 2
    Outgoing interface list:
        GigabitEthernet 4/11
        GigabitEthernet 4/13
        GigabitEthernet 4/20
```

Example 3  

**Figure 35-4. show ip mroute Command Example**

```
FTOS#show ip mroute
IP Multicast Routing Table
(*, 224.10.10.1), uptime 00:05:12
    Incoming interface: GigabitEthernet 3/12
    Outgoing interface list:
        GigabitEthernet 3/13

{1.13.1.100, 224.10.10.1), uptime 00:04:03
    Incoming interface: GigabitEthernet 3/4
    Outgoing interface list:
        GigabitEthernet 3/12
        GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
    Incoming interface: GigabitEthernet 3/12
    Outgoing interface list:
        GigabitEthernet 3/4
```

Table 35-1. show ip mroute Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S,G)</td>
<td>Displays the forwarding entry in the multicast route table.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the multicast forwarding</td>
</tr>
<tr>
<td></td>
<td>table.</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) information towards the</td>
</tr>
<tr>
<td></td>
<td>source for (S,G) entries and the RP for (*,G) entries.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Lists the interfaces that meet one of the following:</td>
</tr>
<tr>
<td></td>
<td>• a directly connected member of the Group</td>
</tr>
<tr>
<td></td>
<td>• statically configured member of the Group</td>
</tr>
<tr>
<td></td>
<td>• received a (*,G) or (S,G) Join message</td>
</tr>
</tbody>
</table>
show ip rpf

View reverse path forwarding.

**Syntax**

`show ip rpf`

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

E-Series legacy command

**Usage Information**

Static mroutes are used by network administrators to control the reachability of the multicast sources. If a PIM registered multicast source is reachable via static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one the PIM selects for reachability.

**Note:** The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

**Example**

**Figure 35-5. show ip rpf Command Example**

```
FTOS#show ip rpf
RPF information for 10.10.10.9
  RPF interface: Gi 3/4
  RPF neighbor: 165.87.31.4
  RPF route/mask: 10.10.10.9/255.255.255.255
  RPF type: unicast
```
show mac-address-table static multicast

Display information on the current configuration of Layer 2 multicast switching on a router.

Syntax

```
show mac-address-table static multicast [multicast-mac-address [vlan vlan-id] | vlan vlan-id | count [vlan vlan-id]]
```

Parameters

- `multicast-mac-address [vlan vlan-id]`: Enter the static multicast MAC address in nn:nn:nn:nn:nn:nn format and (optionally) the VLAN ID of a VLAN used to switch Layer 2 multicast traffic on the router. VLAN ID range: 1 to 4094.
- `vlan vlan-id`: Enter the VLAN ID of a VLAN used to switch Layer 2 multicast traffic on the router. VLAN ID range: 1 to 4094.
- `count [vlan vlan-id]`: Enter the keyword `count` and (optionally) the VLAN ID of a VLAN used to switch Layer 2 multicast traffic to display the number of static multicast MAC addresses in use for all or a specified VLAN.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.4.2.5 Introduced on C-Series.

Usage Information

Use the `show mac-address-table static multicast` command to display the currently configured static multicast MAC addresses, associated VLAN, and assigned output ports used to switch Layer 2 multicast traffic on a router.

Example

```
FTOS# show mac-address-table static multicast
```

```
VlanId   Mac Address       Type  State   L2MCIndex  Interfaces
10       01:00:5e:01:01:01 static Active 0  Gi 1/2, Gi 2/47
11       01:00:5e:01:01:02 static Active 1  Po 10
12       01:00:5e:01:01:01 static Inactive 0
```

Table 35-2. show mac-address-table static multicast Information

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanId</td>
<td>Displays the VLAN ID number of the VLAN used for Layer 2 multicast forwarding.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>Displays the static MAC address in nn:nn:nn:nn:nn:nn format that is configured for Layer 2 multicast forwarding.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays <code>static</code> for a manually configured MAC address.</td>
</tr>
<tr>
<td>State</td>
<td>Displays whether the multicast MAC address is in use (Active) or not in use (Inactive). The state of a multicast MAC address is inactive if an associated VLAN has not been configured.</td>
</tr>
</tbody>
</table>
Table 35-2. show mac-address-table static multicast Information

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2MCIndex</td>
<td>Displays the Layer 2 multicast index used to represent a group of outbound interfaces. The L2 multicast index is a hardware-specific index that is used as an internal command and useful for debugging purposes. Range: 0 - 1023.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Displays the interface type and slot/port of output ports assigned to the VLAN used for Layer 2 multicast forwarding, where the following abbreviations are used for output port types: • gi—Gigabit Ethernet slot/port. • po—Port Channel number • te—10-Gigabit Ethernet slot/port</td>
</tr>
</tbody>
</table>

Figure 35-7. show mac-address-table static multicast count Command Output

```
FTOS#show mac-address-table static multicast count
Static Multicast MAC Entries for all vlans :  3
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip multicast-mode l2</td>
<td>Enable Layer 2 multicast switching.</td>
</tr>
<tr>
<td>mac-address-table static</td>
<td>Configure a static multicast MAC address, associate the multicast MAC address with the Layer 2 VLAN used to switch multicast traffic, and add output ports.</td>
</tr>
</tbody>
</table>
show queue backplane multicast

Display the backplane bandwidth configuration about how much bandwidth is dedicated to multicast versus unicast.

**Syntax**

```
show queue backplane multicast bandwidth-percentage
```

**Defaults**

None

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 7.7.1.0  Introduced on E-Series

**Example**

```
Figure 35-8.  show queue backplane multicast Command Example

FTOS#show queue backplane multicast bandwidth-percent
Configured multicast bandwidth percentage is 80
```

**Related Commands**

- `queue backplane multicast`  
  Reallocate the amount of bandwidth dedicated to multicast traffic.
IPv6 Multicast Commands

IPv6 Multicast commands are:

- clear ipv6 mroute
- ipv6 multicast-limit
- ip multicast-routing
- show ipv6 mroute
- show ipv6 mroute mld
- show ipv6 mroute summary

**clear ipv6 mroute**

Clear learned multicast routes on the multicast forwarding table. To clear the PIM tib, use clear ip pim tib command.

**Syntax**
```
clear ipv6 mroute {group-address [source-address] | *}
```

**Parameters**
- `group-address [source-address]`
  - Enter multicast group address and source address (if desired) to clear information on a specific group. Enter the addresses in the `X:X:X:X::X` format.
  - The `::` notation specifies successive hexadecimal fields of zero.
- `*`
  - Enter `*` to clear all multicast routes.

**Defaults**
No default behavior or values

**Command Modes**
EXEC Privilege

**Command History**
Version 7.4.1.0 Introduced

**Related Commands**
- show ipv6 pim tib Display the IPv6 PIM Tree Information Base.
**ipv6 multicast-limit**

Limit the number of multicast entries on the system.

**Syntax**

```
ipv6 multicast-limit limit
```

**Parameters**

- `limit` Enter the desired maximum number of multicast entries on the system.
  - Range: 1 to 50000
  - Default: 15000

**Defaults**

15000 routes

**Command Modes**

CONFIGURATION

**Command History**

Version 8.3.1.0 Introduced

**Usage Information**

The maximum number of multicast entries allowed on each line card is determined by the CAM profile. Multicast routes are stored in the IN-V6-McastFib CAM region, which has a fixed number of entries. Any limit configured via the CLI is superseded by this hardware limit. The opposite is also true; the CAM might not be exhausted at the time the CLI-configured route limit is reached.

---

**ipv6 multicast-routing**

Enable IPv6 multicast forwarding.

**Syntax**

```
ipv6 multicast-routing
```

To disable multicast forwarding, enter `no ipv6 multicast-routing`.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

E-Series legacy command

**Related Commands**

- ipv6 pim sparse-mode
**show ipv6 mroute**

View IPv6 multicast routes.

**Syntax**

```plaintext
show ipv6 mroute [group-address [source-address]] [active rate] [count group-address [source source-address]]
```

**Parameters**

- `group-address` (OPTIONAL) Enter the IPv6 multicast group-address to view only routes associated with that group. Optionally, enter the IPv6 source-address to view routes with that group-address and source-address.
- `active [rate]` (OPTIONAL) Enter the keyword `active` to view active multicast sources. Enter a rate to view active routes over the specified rate. Range: 0 to 10000000 packets/second
- `count [group-address [source source-address]]` (OPTIONAL) Enter the keyword `count` to view the number of IPv6 multicast routes and packets on the E-Series. Optionally, enter the IPv6 source-address count information.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 7.4.1.0 Introduced

**Example**

```plaintext
FTOS#show ipv6 mroute
IP Multicast Routing Table
(165:87:32::30, ff05:100::1), uptime 00:01:11
   Incoming interface: Vlan 200
   Outgoing interface list:  
      GigabitEthernet 2/14

(165:87:37::30, ff05:200::1), uptime 00:01:04
   Incoming interface: Port-channel 200
   Outgoing interface list:  
      Vlan 200

(165:87:31::30, ff05:300::1), uptime 00:01:19
   Incoming interface: GigabitEthernet 2/14
   Outgoing interface list:  
      Port-channel 200

(165:87:32::30, ff05:1100::1), uptime 00:01:05
   Incoming interface: Vlan 200
   Outgoing interface list:  
      GigabitEthernet 2/14

(165:87:37::30, ff05:2200::1), uptime 00:01:01
   Incoming interface: Port-channel 200
   Outgoing interface list:  
      Vlan 200

FTOS#
```
Example Figure 35-10. show ipv6 mroute active Command Example

FTOS#show ipv6 mroute active 10
Active Multicast Sources - sending >= 10 pps
Group: ff05:300::1
  Source: 165:87:31::30
  Rate: 100 pps
Group: ff05:3300::1
  Source: 165:87:31::30
  Rate: 100 pps
Group: ff3e:300::4000:1
  Source: 165:87:31::20
  Rate: 100 pps
Group: ff3e:3300::4000:1
  Source: 165:87:31::20
  Rate: 100 pps
FTOS#

Example Figure 35-11. show ipv6 mroute count group Command Examples

FTOS#show ipv6 mroute count group ff05:3300::1
IP Multicast Statistics
1 routes using 648 bytes of memory
1 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second
Group: ff05:3300::1, Source count: 1
  Source: 165:87:31::30, Forwarding: 3997/0
FTOS#

Example Figure 35-12. show ipv6 mroute count source Command Examples

FTOS#show ipv6 mroute count source 165:87:31::30
IP Multicast Statistics
2 routes using 1296 bytes of memory
2 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second
Group: ff05:300::1, Source count: 1
  Source: 165:87:31::30, Forwarding: 3993/0
Group: ff05:3300::1, Source count: 1
  Source: 165:87:31::30, Forwarding: 3997/0
FTOS#
show ipv6 mroute mld

Display the Multicast MLD information.

Syntax

```
show ipv6 mroute  [mld  [group-address | all | vlan vlan-id]]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mld</td>
<td>(OPTIONAL) Enter the keyword mld to display Multicast MLD information.</td>
</tr>
<tr>
<td>group-address</td>
<td>(OPTIONAL) Enter the multicast group address in the : notation specifies successive hexadecimal fields of zero.</td>
</tr>
<tr>
<td>all</td>
<td>(OPTIONAL) Enter the keyword all to view all the MLD information.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(OPTIONAL) Enter the keyword vlan followed by the VLAN ID to view MLD VLAN information.</td>
</tr>
</tbody>
</table>

Defaults

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.4.1.0 Introduced

Example

```
FTOS#show ipv6 mroute mld all
MLD SNOOPING MRTM Table
    (*, ff05:100::1), uptime 00:04:21
      Incoming vlan: Vlan 200
      Outgoing interface list:
        GigabitEthernet 2/15
        GigabitEthernet 2/16
    (*, ff05:200::1), uptime 00:04:15
      Incoming vlan: Vlan 200
      Outgoing interface list:
        GigabitEthernet 2/15
        GigabitEthernet 2/16
    (*, ff05:1100::1), uptime 00:04:18
      Incoming vlan: Vlan 200
      Outgoing interface list:
        GigabitEthernet 2/15
        GigabitEthernet 2/16
FTOS#
```
show ipv6 mroute summary

Display a summary of the Multicast routing table.

Syntax  show ipv6 mroute summary

Defaults No default values or behavior

Command Modes EXEC
EXEC Privilege

Command History

Example Figure 35-14.  show ipv6 mroute summary Command Example

FTOS#show ipv6 mroute summary

IP Multicast Routing Table
12 groups, 12 routes

(165:87:32::30, ff05:100::1), 00:00:24
(165:87:37::30, ff05:200::1), 00:00:24
(165:87:31::30, ff05:300::1), 00:00:24
(165:87:32::30, ff05:1100::1), 00:00:21
(165:87:37::30, ff05:2200::1), 00:00:21
(165:87:31::30, ff05:3300::1), 00:00:21
(165:87:32::20, ff3e:100::4000:1), 00:00:41
FTOS#
Neighbor Discovery Protocol (NDP)

Overview

Neighbor Discovery Protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. It defines mechanisms for solving the following problems:

- Router discovery: Hosts can locate routers residing on a link.
- Prefix discovery: Hosts can discover address prefixes for the link.
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor Unreachability Detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate Address Detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

NDP makes use of the following five ICMPv6 packet types in its implementation:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

Commands

The Neighbor Discovery Protocol (NDP) commands in this chapter are:

- clear ipv6 neighbors
- ipv6 nd managed-config-flag
- ipv6 nd max-ra-interval
- ipv6 nd mtu
- ipv6 nd other-config-flag
- ipv6 nd prefix
- ipv6 nd ra-lifetime
- ipv6 nd reachable-time
Neighbor Discovery Protocol (NDP)

- ipv6 nd suppress-ra
- ipv6 neighbor
- show ipv6 neighbors

**clear ipv6 neighbors**

Delete all entries in the IPv6 neighbor discovery cache, or neighbors of a specific interface. Static entries will not be removed using this command.

**Syntax**

```
clear ipv6 neighbors [ipv6-address] [interface]
```

**Parameters**

- `ipv6-address`
  - Enter the IPv6 address of the neighbor in the X::X::X::X format to remove a specific IPv6 neighbor.
  - The :: notation specifies successive hexadecimal fields of zero.
- `interface interface`
  - To remove all neighbor entries learned on a specific interface, enter the keyword `interface` followed by the interface type and slot/port or number information of the interface:
    - For a Fast Ethernet interface, enter the keyword `fastEthernet` followed by the slot/port information.
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - 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.

**Command Modes**

- EXEC
- EXEC Privilege

**ipv6 nd managed-config-flag**

Set the managed address configuration flag in the IPv6 router advertisement. The description of this flag from RFC 2461 (http://tools.ietf.org/html/rfc2461) is:

- **M**: 1-bit “Managed address configuration” flag. When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration. The use of this flag is described in:


**Syntax**

```
ipv6 nd managed-config-flag
```

To clear the flag from the IPv6 router advertisements, use the `no ipv6 nd managed-config-flag` command.

**Defaults**

The default flag is 0.

**Command Modes**

- INTERFACE
ipv6 nd max-ra-interval

Configure the interval between the IPv6 router advertisement (RA) transmissions on an interface.

**Syntax**

```
ipv6 nd max-ra-interval {interval} min-ra-interval {interval}
```

To restore the default interval, use the `no ipv6 nd max-ra-interval` command.

**Parameters**

- **max-ra-interval** `{interval}`
  - Enter the keyword `max-ra-interval` followed by the interval in seconds.
  - Range: 4 to 1800 seconds

- **min-ra-interval** `{interval}`
  - Enter the keyword `min-ra-interval` followed by the interval in seconds.
  - Range: 3 to 1350 seconds

**Defaults**

Max RA interval: 600 seconds, Min RA interval: 200 seconds

**Command Modes**

INTERFACE

---

ipv6 nd mtu

Configure an IPv6 neighbor discovery.

**Syntax**

```
ipv6 nd mtu number
```

**Parameters**

- **mtu** `number`
  - Set the MTU advertisement value in Routing Prefix Advertisement packets. Range: 1280 to 9234

**Defaults**

No default values or behavior

**Command Modes**

INTERFACE

**Command History**

- **Version 8.3.1.0**  Introduced

**Usage Information**

The `ip nd mtu` command sets the value advertised to routers. It does not set the actual MTU rate. For example, if `ip nd mtu` is set to 1280, the interface will still pass 1500-byte packets.

The `mtu` command sets the actual frame size passed, and can be larger than the advertised MTU. If the mtu setting is larger than the ip nd mtu, an error message is sent, but the configuration is accepted.

```
% Error: nd ra mtu is greater than link mtu, link mtu will be used.
```

**Related Commands**

- `mtu`  Set the maximum link MTU (frame size) for an Ethernet interface.
ipv6 nd other-config-flag

Set the other stateful configuration flag in the IPv6 router advertisement. The description of this flag from RFC 2461 (http://tools.ietf.org/html/rfc2461) is:

O: 1-bit “Other stateful configuration” flag. When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information. The use of this flag is described in:


Syntax

ipv6 nd other-config-flag

To clear the flag from the IPv6 router advertisements, use the no ipv6 nd other-config-flag command.

Defaults

The default flag is 0.

Command Modes

INTERFACE

ipv6 nd prefix

Configure how IPv6 prefixes are advertised in the IPv6 router advertisements. The description of an IPv6 prefix from RFC 2461(http://tools.ietf.org/html/rfc2461) is a bit string that consists of some number of initial bits of an address.

Syntax

ipv6 nd prefix {ipv6-address prefix-length | default} [no-advertise] | [no-autoconfig | no-rtr-address | off-link]

Parameters

| ipv6-address prefix-length | Enter the IPv6 address in the x:x:x:x: format followed by the prefix length in the /x format. Range: /0 to /128
| default | (OPTIONAL) Enter the keyword default to specify the prefix default parameters.
| no-advertise | (OPTIONAL) Enter the keyword no-advertise to not advertise prefixes.
| no-autoconfig | (OPTIONAL) Enter the keyword no-autoconfig to not use prefixes for auto-configuration.
| no-rtr-address | (OPTIONAL) Enter the keyword no-rtr-address to not send full router addresses in prefix advertisement.
| off-link | (OPTIONAL) Enter the keyword off-link to not use prefixes for on-link determination.

Defaults

Not configured

Command Modes

INTERFACE
ipv6 nd ra-lifetime

Configure the router lifetime value in the IPv6 router advertisements on an interface. The description of router lifetime from RFC 2461(http://tools.ietf.org/html/rfc2461) is:

**Router Lifetime**: 16-bit unsigned integer. The lifetime associated with the default router in units of seconds. The maximum value corresponds to 18.2 hours. A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the default router list. The Router Lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options. Options that need time limits for their information include their own lifetime fields.

**Syntax**

```
ipv6 nd ra-lifetime seconds
```

To restore the default values, use the **no ipv6 nd ra-lifetime** command.

**Parameters**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Enter the lifetime value in seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range: 0 to 9000</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

9000 seconds

**Command Modes**

INTERFACE

ipv6 nd reachable-time

Configure the amount of time that a remote IPv6 node is considered available after a reachability confirmation event has occurred. The description of reachable time from RFC 2461(http://tools.ietf.org/html/rfc2461) is:

**Reachable Time**: 32-bit unsigned integer. The time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. Used by the Neighbor Unreachability Detection algorithm. A value of zero means unspecified (by this router).

**Syntax**

```
ipv6 nd reachable-time {milliseconds}
```

To restore the default time, use the **no ipv6 nd reachable-time** command.

**Parameters**

<table>
<thead>
<tr>
<th>milliseconds</th>
<th>Enter the leachability time in milliseconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range: 0 to 3600000</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

3600000 milliseconds

**Command Modes**

INTERFACE

ipv6 nd suppress-ra

Suppress the IPv6 router advertisement transmissions on an interface.

**Syntax**

```
ipv6 nd suppress-ra
```

To enable the sending of IPv6 router advertisement transmissions on an interface, use the **no ipv6 nd suppress-ra** command.
ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

**Syntax**

```
ipv6 neighbor {ipv6-address} {interface interface} {hardware_address}
```

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the **no ipv6 neighbor {ipv6-address} {interface interface}** command.

**Parameters**

- **ipv6-address**: Enter the IPv6 address of the neighbor in the `x:X:x:X:X::X` format. The `::` notation specifies successive hexadecimal fields of zero.

- **interface interface**: Enter the keyword **interface** followed by the interface type and slot/port or number information:
  - For a Fast Ethernet interface, enter the keyword **fastEthernet** followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

- **hardware_address**: Enter a 48-bit hardware MAC address in `nn:nn:nn:nn:nn:nn` format.

**Defaults**

- No default behavior or values

**Command Modes**

- **CONFIGURATION**

---

show ipv6 neighbors

Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the CP (control processor).

**Syntax**

```
show ipv6 neighbors [ipv6-address] [cpu {rp1 [ipv6-address] | rp2 [ipv6-address]}] [interface interface]
```

**Parameters**

- **ipv6-address**: Enter the IPv6 address of the neighbor in the `x:X:x:X:X::X` format. The `::` notation specifies successive hexadecimal fields of zero.
**CPU**
Enter the keyword **cpu** followed by either **rp1** or **rp2** (Route Processor 1 or 2), optionally followed by an IPv6 address to display the IPv6 neighbor entries stored on the designated RP.

**Interface interface**
- For a Fast Ethernet interface, enter the keyword **fastEthernet** followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
- For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255.
- 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.

**Defaults**
No default behavior or values

**Command Modes**
EXEC

EXEC Privilege

**Example**

**Figure 36-1. show ipv6 neighbors Command Example**

```
FTOS#show ipv6 neighbors
IPv6 Address   Expires(min)   Hardware Address   State   Interface  VLAN   CPU
------------------------------------------------------------------------------
fe80::201:e8ff:fe17:5bc6   1439       00:01:e8:17:5b:c6  STALE   Gi 1/9        -   CP
fe80::201:e8ff:fe17:5bc7   1439       00:01:e8:17:5b:c7  STALE   Gi 1/10       -   CP
fe80::201:e8ff:fe17:5bc8   1439       00:01:e8:17:5b:c8  STALE   Gi 1/11       -   CP
fe80::201:e8ff:fe17:5caf  0.3        00:01:e8:17:5c:af  REACH   Po 1          -   CP
fe80::201:e8ff:fe17:5cb0   1439       00:01:e8:17:5c:b0  STALE   Po 32         -   CP
fe80::201:e8ff:fe17:5cb1   1439       00:01:e8:17:5c:b1  STA LEE   Po 255        -   CP
fe80::201:e8ff:fe17:5cae   1439       00:01:e8:17:5c:ae  STALE   Gi 1/3     Vl 100 CP
fe80::201:e8ff:fe17:5cae   1439       00:01:e8:17:5c:ae  STALE   Gi 1/5     Vl 1000 CP
fe80::201:e8ff:fe17:5cae   1439       00:01:e8:17:5c:ae  STALE   Gi 1/7     Vl 2000 CP
FTOS#
```
Object Tracking

Object Tracking supports IPv4 and IPv6, and is available on platforms: C E S

Overview

Object tracking allows you to define objects of interest, monitor their state, and report to a client when a change in an object’s state occurs. The following tracked objects are supported:

- Link status of Layer 2 interfaces
- Routing status of Layer 3 interfaces (IPv4 and IPv6)
- Reachability of IPv4 and IPv6 routes
- Metric thresholds of IPv4 and IPv6 routes

You can configure client applications, such VRRP, to receive a notification when the state of a tracked object changes.

This chapter has the following sections:

- IPv4 Object Tracking Commands on page 993
- IPv6 Object Tracking Commands on page 1007

IPv4 Object Tracking Commands

The IPv4 VRRP commands are:

- debug track
- delay
- description
- show running-config track
- show track
- threshold metric
- track interface ip routing
- track interface line-protocol
- track ip route metric threshold
- track ip route reachability
- track resolution ip route
**debug track**

Enables debugging for tracked objects.

**Syntax**

```plaintext
debug track [all | notifications | object-id]
```

**Parameters**

- `all`: Enables debugging on the state and notifications of all tracked objects.
- `notifications`: Enables debugging on the notifications of all tracked objects.
- `object-id`: Enables debugging on the state and notifications of the specified tracked object. Range: 1 to 65535.

**Defaults**

Enable debugging on the state and notifications of all tracked objects (`debug track all`).

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Introduced in Version 8.4.1.0

**Example**

Command Example: `debug track all`

```
FTOS#debug track all
04:35:04: %RPM0-P:RP2 %OTM-5-STATE: track 6 - Interface GigabitEthernet 0/2 line-protocol DOWN
04:35:04: %RPM0-P:RP2 %OTM-5-NOTIF: VRRP notification: resource ID 6 DOWN
```
Configure the time delay used before communicating a change in the status of a tracked object to clients.

**Syntax**

```
delay {{up seconds} [down seconds]}
```

To return to the default setting, enter `no delay`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Enter the number of seconds the object tracker waits before sending a notification about the change in the UP and/or DOWN state of a tracked object to clients. Range: 0 to 180. Default: 0 seconds.</td>
</tr>
</tbody>
</table>

**Defaults**

0 seconds

**Command Modes**

OBJECT TRACKING (conf_track_object-id)

**Version 8.4.1.0** Introduced

**Related Commands**

- **track interface ip routing**
  - Configure object tracking on the routing status of an IPv4 Layer 3 interface.
- **track interface line-protocol**
  - Configure object tracking on the line-protocol state of a Layer 2 interface.
- **track ip route metric threshold**
  - Configure object tracking on the threshold of an IPv4 route metric.
- **track ip route reachability**
  - Configure object tracking on the reachability of an IPv4 route.

**Usage Information**

You can configure an UP and/or DOWN timer for each tracked object to set the time delay before a change in the state of a tracked object is communicated to clients. The configured time delay starts when the state changes from UP to DOWN or vice-versa.

If the state of an object changes back to its former UP/DOWN state before the timer expires, the timer is cancelled and the client is not notified. For example, if the DOWN timer is running when an interface goes down and comes back up, the DOWN timer is cancelled and the client is not notified of the event.

If the timer expires and an object’s state has changed, a notification is sent to the client. If no delay is configured, a notification is sent immediately as soon as a change in the state of a tracked object is detected. The time delay in communicating a state change is specified in seconds.
**description**

Enter a description of a tracked object.

**Syntax**

```
description {text}
```

To remove the description, enter the `no description {text}` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>text</code></td>
<td>Enter a description to identify a tracked object (80 characters maximum).</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

OBJECT TRACKING (conf_track_object-id)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>track interface ip routing</code></td>
<td>Configure object tracking on the routing status of an IPv4 Layer 3 interface.</td>
</tr>
<tr>
<td><code>track interface line-protocol</code></td>
<td>Configure object tracking on the line-protocol state of a Layer 2 interface.</td>
</tr>
<tr>
<td><code>track ip route metric threshold</code></td>
<td>Configure object tracking on the threshold of an IPv4 route metric.</td>
</tr>
<tr>
<td><code>track ip route reachability</code></td>
<td>Configure object tracking on the reachability of an IPv4 route.</td>
</tr>
</tbody>
</table>
show running-config track

Display the current configuration of tracked objects.

Syntax

show running-config track [object-id]

Parameters

object-id (OPTIONAL) Display information on the specified tracked object. Range: 1 to 65535.

Command Modes

EXEC Privilege

Command History

Version 8.4.1.0 Introduced

Related Commands

show track Display information about tracked objects, including configuration, current state, and clients which track the object.

track interface ip routing Configure object tracking on the routing status of an IPv4 Layer 3 interface.

track interface line-protocol Configure object tracking on the line-protocol state of a Layer 2 interface.

track ip route metric threshold Configure object tracking on the threshold of an IPv4 route metric.

track ip route reachability Configure object tracking on the reachability of an IPv4 route.

Example

Command Example: show running-config track

FTOS#show running-config track
track 1 ip route 23.0.0.0/8 reachability
track 2 ipv6 route 2040::/64 metric threshold
delay down 3
delay up 5
threshold metric up 200
track 3 ipv6 route 2050::/64 reachability
track 4 interface GigabitEthernet 13/4 ip routing
track 5 ip route 192.168.0.0/24 reachability vrf red
track resolution ip route isis 20
track resolution ip route ospf 10

Command Example: show running-config track object-id

FTOS#show running-config track 300
track 300 ip route 10.0.0.0/8 metric threshold
delay down 3
delay up 5
threshold metric up 100
show track

Display information about tracked objects, including configuration, current tracked state (UP or DOWN), and the clients which are tracking an object.

Syntax

show track [object-id [brief] | interface [brief] [vrf vrf-name] | ip route [brief] [vrf vrf-name] | resolution | vrf vrf-name [brief] | brief]

Parameters

object-id (OPTIONAL) Display information on the specified tracked object. Range: 1 to 65535.

interface (OPTIONAL) Display information on all tracked interfaces (Layer 2 and IPv4 Layer 3). Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a Port Channel interface, enter the keyword port-channel followed by a number:
  C-Series Range: 1-128
  E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- 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 the VLAN ID. The VLAN ID range is from 1 to 4094.

ip route (OPTIONAL) Display information on all tracked IPv4 routes.

resolution (OPTIONAL) Display information on the configured resolution values used to scale protocol-specific route metrics to the range 0 to 255.

brief (OPTIONAL) Display a single line summary of the tracking information for a specified object, object type, or all tracked objects.

vrf vrf-name (OPTIONAL) E-Series only: Display information on only the tracked objects that are members of the specified VRF instance. Maximum: 32 characters. If you do not enter a VRF name, information on the tracked objects from all VRF is displayed.

Command Modes

EXEC Privilege

Command History

Version 8.4.6.0 Added support for the keyword fortyGigE.

Version 8.4.1.0 Introduced

Related Commands

show running-config track Display configuration information about tracked objects.

track interface ip routing Configure object tracking on the routing status of an IPv4 Layer 3 interface.

track interface line-protocol Configure object tracking on the line-protocol state of a Layer 2 interface.

track ip route metric threshold Configure object tracking on the threshold of an IPv4 route metric.

track ip route reachability Configure object tracking on the reachability of an IPv4 route.
Figure 37-1. Command Example: show track

```
FTOS#show track

Track 1
IP route 23.0.0.0/8 reachability
Reachability is Down (route not in route table)
  2 changes, last change 00:16:08
Tracked by:

Track 2
IPV6 route 2040::/64 metric threshold
Metric threshold is Up (STATIC/0/0)
  5 changes, last change 00:02:16
Metric threshold down 255 up 254
First-hop interface is GigabitEthernet 13/2
Tracked by:
  VRRP GigabitEthernet 7/30 IPv6 VRID 1

Track 3
IPV6 route 2050::/64 reachability
Reachability is Up (STATIC)
  5 changes, last change 00:02:16
First-hop interface is GigabitEthernet 13/2
Tracked by:
  VRRP GigabitEthernet 7/30 IPv6 VRID 1
```
To configure the metric threshold used to determine the UP and/or DOWN state of a tracked IPv4 or IPv6 route, use the `threshold metric` command.

```
threshold metric
```

Syntax:
```
threshold metric {up number | down number}
```

To return to the default setting, enter `no threshold metric {up number | down number}`.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object-id</td>
<td>Enter the ID number of the tracked object. Range: 1 to 65535.</td>
</tr>
<tr>
<td>up number</td>
<td>Enter a number for the UP threshold to be applied to the scaled metric of an IPv4 or IPv6 route. Default UP threshold: 254. The routing state is UP if the scaled route metric is less than or equal to the UP threshold.</td>
</tr>
<tr>
<td>down number</td>
<td>Enter a number for the DOWN threshold to be applied to the scaled metric of an IPv4 or IPv6 route. Default DOWN threshold: 255. The routing state is DOWN if the scaled route metric is greater than or equal to the DOWN threshold.</td>
</tr>
</tbody>
</table>

### Defaults

None

### Command Modes

OBJECT TRACKING (conf_track_object-id)

### Command History

- **Version 8.4.1.0** Introduced

### Related Commands

- `track ip route metric threshold` Configure object tracking on the threshold of an IPv4 route metric.
- `track resolution ip route` Configure the protocol-specific resolution value used to scale an IPv4 route metric.

### Usage Information

Use this command to configure the UP and/or DOWN threshold for the scaled metric of a tracked IPv4 or IPv6 route.

The UP/DOWN state of a tracked route is determined by the threshold for the current value of the route metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible. The scaled metric value communicated to a client always considers a lower value to have priority over a higher value.

The resulting scaled value is compared against the configured threshold values to determine the state of a tracked route as follows:
• If the scaled metric for a route entry is less than or equal to the UP threshold, the state of a route is UP.
• If the scaled metric for a route is greater than or equal to the DOWN threshold or the route is not entered in the routing table, the state of a route is DOWN.

You configure the UP and DOWN thresholds for each tracked route with the `threshold metric` command. The default UP threshold is 254; the default DOWN threshold is 255. The notification of a change in the state of a tracked object is sent when a metric value crosses a configured threshold.

The tracking process uses a protocol-specific resolution value to convert the actual metric in the routing table to a scaled metric in the range 0 to 255. You can configure the resolution value used to scale route metrics for supported protocols with the `track resolution ip route` and `track resolution ipv6 route` commands.

### track

**Enter Object Tracking command mode to modify the configuration of a tracked object.**

**Syntax**

```
track object-id
```

**Parameters**

- `object-id` Enter the ID number of the tracked object. Range: 1 to 65535.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

Version 8.4.1.0 Introduced

**Related Commands**

- `show track` Display information about tracked objects, including configuration, current state, and clients which track the object.

**Usage Information**

Use this command to enter the Object Tracking mode to edit an existing configuration of a tracked object. For example, after you enter the `track object-id` command, you can modify or add a delay timer (`delay` command) or a metric threshold (`threshold metric` command) for the UP or DOWN state of the tracked object.

### track ip route metric threshold

**Configure object tracking on the threshold of an IPv4 route metric.**

**Syntax**

```
track object-id ip route ip-address/prefix-len metric threshold [vrf vrf-name]
```

To return to the default setting, enter `no track object-id`.

**Parameters**

- `object-id` Enter the ID number of the tracked object. Range: 1 to 65535.
Use this command to create an object that tracks the UP and/or DOWN threshold of an IPv4 route metric. In order for a route’s metric to be tracked, the route must appear as an entry in the routing table.

A tracked IPv4 route is considered to match an entry in the routing table only if the exact IPv4 address and prefix length match a table entry. For example, when configured as a tracked route, 10.0.0.0/24 does not match the routing table entry 10.0.0.0/8. If no route-table entry has the exact IPv4 address and prefix length, the status of the tracked route is considered to be DOWN.

When you configure the threshold of an IPv4 route metric as a tracked object, the UP/DOWN state of the tracked route is also determined by the current metric for the route in the routing table.

To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible. The scaled metric value communicated to a client always considers a lower value to have priority over a higher value. The resulting scaled value is compared against the configured threshold values to determine the state of a tracked route as follows:

- If the scaled metric for a route entry is less than or equal to the UP threshold, the state of a route is UP.
- If the scaled metric for a route is greater than or equal to the DOWN threshold or the route is not entered in the routing table, the state of a route is DOWN.

You configure the UP and DOWN thresholds for each tracked route by using the `threshold metric` command. The default UP threshold is 254; the default DOWN threshold is 255. The notification of a change in the state of a tracked object is sent when a metric value crosses a configured threshold.

### Examples

To configure object tracking on the reachability of an IPv4 route:

```
track ip route reachability
```

**Command Syntax**

```
track object-id ip route ip-address/prefix-len reachability [vrf vrf-name]
```

**To return to the default setting, enter**

```
no track object-id
```

### Related Commands

- `show track` Display information about tracked objects, including configuration, current state, and clients which track the object.
- `threshold metric` Configure the metric threshold used to determine the UP and/or DOWN state of a tracked route.
- `track resolution ip route` Configure the protocol-specific resolution value used to scale an IPv4 route metric.
Use this command to create an object that tracks the reachability of an IPv4 route. In order for a route’s reachability to be tracked, the route must appear as an entry in the routing table.

A tracked IPv4 route is considered to match an entry in the routing table only if the exact IPv4 address and prefix length match a table entry. For example, when configured as a tracked route, 10.0.0.0/24 does not match the routing table entry 10.0.0.0/8. If no route-table entry has the exact IPv4 address and prefix length, the status of the tracked route is considered to be DOWN.

When you configure IPv4 route reachability as a tracked object, the UP/DOWN state of the tracked route is also determined by the entry of the next-hop address in the ARP cache. A tracked route is considered to be reachable if there is an ARP cache entry for the route's next-hop address.

If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to regenerate the ARP cache entry to see if the next-hop address appears before considering the route DOWN.

**Parameters**

- **object-id**
  - Enter the ID number of the tracked object. Range: 1 to 65535.

- **ip-address/prefix-len**
  - Enter an IPv4 address in dotted decimal format. Valid IPv4 prefix lengths are from /0 to /32.

- **vrf vrf-name**
  - (Optional) E-Series only: You can configure a VPN routing and forwarding (VRF) instance to specify the virtual routing table to which the tracked route belongs.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

Version 8.4.1.0 Introduced

**Related Commands**

- **show track**
  - Display information about tracked objects, including configuration, current state, and clients which track the object.

- **track ip route metric threshold**
  - Configure object tracking on the threshold of an IPv4 route metric.
track interface ip routing

Configure object tracking on the routing status of an IPv4 Layer 3 interface.

Syntax

```
track object-id interface interface ip routing
```

To return to the default setting, enter `no track object-id`.

Parameters

- `object-id` Enter the ID number of the tracked object. Range: 1 to 65535.
- `interface` Enter one of the following values:
  - For a 1-Gigabit Ethernet interface, enter `gigabitethernet slot-number/port-number`.
  - For a Loopback interface, enter `loopback number`, where `number` is from 0 to 16383.
  - For a Port Channel interface, enter `port-channel number`, where the valid values are:
    - C-Series and S-Series: 1 to 128
    - E-Series: 1 to 32 for EtherScale; 1 to 255 for TeraScale; 1 to 512 for ExaScale.
  - For SONET interfaces, enter the `sonet slot-number/port-number`.
  - For a 10-Gigabit Ethernet interface, enter `tengigabitethernet slot-number/port-number`.
  - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
  - For a VLAN interface, enter `vlan number`, where `number` is from 1 to 4094.

Defaults

None

Command Modes

CONFIGURATION

Command History

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.4.1.0** Introduced

Related Commands

- `show track` Display information about tracked objects, including configuration, current state, and clients which track the object.
- `track interface line-protocol` Configure object tracking on the line-protocol state of a Layer 2 interface.

Usage Information

Use this command to create an object that tracks the routing state of an IPv4 Layer 2 interface:

- The status of the IPv4 interface is UP only if the Layer 2 status of the interface is UP and the interface has a valid IP address.
- The Layer 3 status of an IPv4 interface goes DOWN when its Layer 2 status goes down (for a Layer 3 VLAN, all VLAN ports must be down) or the IP address is removed from the routing table.
track interface line-protocol

Configure object tracking on the line-protocol state of a Layer 2 interface.

Syntax

```
track object-id interface interface line-protocol
```

To return to the default setting, enter `no track object-id`.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object-id</td>
<td>Enter the ID number of the tracked object. Range: 1 to 65535.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter <code>gigabitethernet slot-number/port-number</code>.</td>
</tr>
<tr>
<td></td>
<td>• For a Loopback interface, enter <code>loopback number</code>, where <code>number</code> is from 0 to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter <code>port-channel number</code>, where the valid values are:</td>
</tr>
<tr>
<td></td>
<td>C-Series and S-Series: 1 to 128</td>
</tr>
<tr>
<td></td>
<td>E-Series: 1 to 32 for EtherScale; 1 to 255 for TeraScale; 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For SONET interfaces, enter the <code>sonet slot-number/port-number</code>.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet slot-number/port-number</code>.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN interface, enter <code>vlan number</code>, where <code>number</code> is from 1 to 4094.</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>Version 8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>Version 8.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show track</td>
<td>Display information about tracked objects, including configuration, current state, and clients which track the object.</td>
</tr>
<tr>
<td>track interface ip routing</td>
<td>Configure object tracking on the routing status of an IPv4 Layer 3 interface.</td>
</tr>
</tbody>
</table>

Usage Information

Use this command to create an object that tracks the line-protocol state of a Layer 2 interface by monitoring its operational status (UP or DOWN).

When the link-level status goes down, the tracked object status is considered to be DOWN; if the link-level status is up, the tracked object status is considered to be UP.
track resolution ip route

Configure the protocol-specific resolution value used to scale an IPv4 route metric.

Syntax

track resolution ip route {isis resolution-value | ospf resolution-value}

To return to the default setting, enter no track object-id.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object-id</td>
<td>Enter the ID number of the tracked object. Range: 1 to 65535.</td>
</tr>
<tr>
<td>isis resolution-value</td>
<td>Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.</td>
</tr>
<tr>
<td>ospf resolution-value</td>
<td>Enter the resolution used to convert the metric in the routing table for OSPF routes to a scaled metric.</td>
</tr>
</tbody>
</table>

Defaults

None

Command Modes

CONFIGURATION

Command History

Version 8.4.1.0 Introduced

Related Commands

threshold metric Configure the metric threshold used to determine the UP and/or DOWN state of a tracked route.
track ip route metric threshold Configure object tracking on the threshold of an IPv4 route metric.

Usage Information

Use this command to configure the protocol-specific resolution value that converts the actual metric of an IPv4 route in the routing table to a scaled metric in the range 0 to 255.

The UP/DOWN state of a tracked IPv4 route is determined by a user-configurable threshold (threshold metric command) for the route’s metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible.

The protocol-specific resolution value calculates the scaled metric by dividing a route's cost by the resolution value set for the route protocol:

- For ISIS, you can set the resolution in the range 1 to 1000, where the default is 10.
- For OSPF, you can set the resolution in the range 1 to 1592, where the default is 1.
- The resolution value used to map static routes is not configurable. By default, Dell Networking OS assigns a metric of 0 to static routes.
- The resolution value used to map RIP routes is not configurable. The RIP hop-count is automatically multiplied by 16 to scale it. For example, a RIP metric of 16 (unreachable) scales to 256, which considers the route to be DOWN.
IPv6 Object Tracking Commands

The IPv6 object tracking commands are:

- `show track ipv6 route`
- `track interface ipv6 routing`
- `track ipv6 route metric threshold`
- `track ipv6 route reachability`
- `track resolution ipv6 route`

The following object tracking commands apply to IPv4 and IPv6:

- `debug track`
- `delay`
- `description`
- `show running-config track`
- `threshold metric`
- `track interface line-protocol`

**show track ipv6 route**

Display information about all tracked IPv6 routes, including configuration, current tracked state (UP or DOWN), and the clients which are tracking an object.

**Syntax**

`show track ipv6 route [brief]`

**Parameters**

- `brief` (OPTIONAL) Display a single line summary of information for tracked IPv6 routes.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 8.4.1.0 Introduced

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config track</code></td>
<td>Display configuration information about tracked objects.</td>
</tr>
<tr>
<td><code>show track</code></td>
<td>Display information about tracked objects, including configuration, current state, and clients which track the object.</td>
</tr>
<tr>
<td><code>track interface ipv6 routing</code></td>
<td>Configure object tracking on the routing status of an IPv6 Layer 3 interface.</td>
</tr>
<tr>
<td><code>track ipv6 route metric threshold</code></td>
<td>Configure object tracking on the threshold of an IPv6 route metric.</td>
</tr>
<tr>
<td><code>track ipv6 route reachability</code></td>
<td>Configure object tracking on the reachability of an IPv6 route.</td>
</tr>
</tbody>
</table>
Figure 37-3. Command Example: show track ipv6 route

FTOS#show track ipv6 route

Track 2
IPv6 route 2040::/64 metric threshold
Metric threshold is Up (STATIC/0/0)
5 changes, last change 00:02:30
Metric threshold down 255 up 254
First-hop interface is GigabitEthernet 13/2
Tracked by:
VRRP GigabitEthernet 7/30 IPv6 VRID 1

Track 3
IPv6 route 2050::/64 reachability
Reachability is Up (STATIC)
5 changes, last change 00:02:30
First-hop interface is GigabitEthernet 13/2
Tracked by:
VRRP GigabitEthernet 7/30 IPv6 VRID 1

Table 37-3. Command Example Description: show track ipv6 route

<table>
<thead>
<tr>
<th>show track ipv6 route</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track object-id</td>
<td>Displays the number of the tracked object.</td>
</tr>
<tr>
<td>Interface type slot/port IP route ip-address IPv6 route ipv6-address</td>
<td>Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.</td>
</tr>
<tr>
<td>object is Up/Down</td>
<td>Up/Down state of tracked object; for example, IPv4 interface, reachability or metric threshold of an IP route.</td>
</tr>
<tr>
<td>number changes, last change time</td>
<td>Number of times that the state of the tracked object has changed and the time since the last change in hours:minutes:seconds</td>
</tr>
<tr>
<td>First hop interface</td>
<td>Displays the type and slot/port number of the first-hop interface of the tracked route.</td>
</tr>
<tr>
<td>Tracked by</td>
<td>Client that is tracking an object's state; for example, VRRP.</td>
</tr>
</tbody>
</table>

Figure 37-4. Command Example: show track ipv6 route brief

FTOS#show track ipv6 route brief

<table>
<thead>
<tr>
<th>ResID</th>
<th>Resource</th>
<th>Parameter</th>
<th>State</th>
<th>LastChange</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>IPv6 route metric threshold</td>
<td>2040::/64</td>
<td>Up</td>
<td>00:02:36</td>
</tr>
<tr>
<td>3</td>
<td>IPv6 route reachability</td>
<td>2050::/64</td>
<td>Up</td>
<td>00:02:36</td>
</tr>
</tbody>
</table>

Table 37-4. Command Example Description: show track ipv6 route brief

<table>
<thead>
<tr>
<th>show track ipv6 route brief Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResID</td>
<td>Number of the tracked object</td>
</tr>
<tr>
<td>Resource</td>
<td>Type of tracked object</td>
</tr>
<tr>
<td>Parameter</td>
<td>Detailed description of the tracked object</td>
</tr>
<tr>
<td>State</td>
<td>Up or Down state of the tracked object</td>
</tr>
<tr>
<td>Last Change</td>
<td>Time since the last change in the state of the tracked object</td>
</tr>
</tbody>
</table>
track interface ipv6 routing

Configure object tracking on the routing status of an IPv6 Layer 3 interface.

Syntax

track object-id interface interface ipv6 routing

To return to the default setting, enter no track object-id.

Parameters

- **object-id**: Enter the ID number of the tracked object. Range: 1 to 65535.
- **interface**: Enter one of the following values:
  - For a 1-Gigabit Ethernet interface, enter `gigabitethernet slot-number/port-number`.
  - For a Loopback interface, enter `loopback number`, where `number` is from 0 to 16383.
  - For a Port Channel interface, enter `port-channel number`, where the valid values are:
    - C-Series and S-Series: 1 to 128
    - E-Series: 1 to 32 for EtherScale; 1 to 255 for TeraScale; 1 to 512 for ExaScale.
  - For SONET interfaces, enter the `sonet slot-number/port-number`.
  - For a 10-Gigabit Ethernet interface, enter `tengigabitethernet slot-number/port-number`.
  - For a 40-Gigabit Ethernet interface, enter `fortyGigE slot-number/port-number`.
  - For a VLAN interface, enter `vlan number`, where `number` is from 1 to 4094.

Defaults

None

Command Modes

CONFIGURATION

Command History

- Version 8.4.1.0 Introduced

Related Commands

- **show track ipv6 route**: Display information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- **track interface ip routing**: Configure object tracking on the routing status of an IPv4 Layer 3 interface.

Usage Information

Use this command to create an object that tracks the routing state of an IPv6 Layer 3 interface:

- The status of the IPv6 interface is UP only if the Layer 2 status of the interface is UP and the interface has a valid IP address.
- The Layer 3 status of an IPv6 interface goes DOWN when its Layer 2 status goes down (for a Layer 3 VLAN, all VLAN ports must be down) or the IP address is removed from the routing table.
**track ipv6 route metric threshold**

Configure object tracking on the threshold of an IPv4 route metric.

### Syntax

```
track object-id ipv6 route ipv6-address/prefix-len metric threshold
```

To return to the default setting, enter `no track object-id`.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object-id</td>
<td>Enter the ID number of the tracked object. Range: 1 to 65535.</td>
</tr>
<tr>
<td>ipv6-address/prefix-len</td>
<td>Enter an IPv6 address in X:X::X format. Valid IPv6 prefix lengths are from /0 to /128.</td>
</tr>
</tbody>
</table>

### Defaults

None

### Command Modes

CONFIGURATION

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### Related Commands

- `show track ipv6 route` Display information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- `threshold metric` Configure the metric threshold used to determine the UP and/or DOWN state of a tracked route.
- `track resolution ipv6 route` Configure the protocol-specific resolution value used to scale an IPv6 route metric.

### Usage Information

Use this command to create an object that tracks the UP and/or DOWN threshold of an IPv6 route metric. In order for a route’s metric to be tracked, the route must appear as an entry in the routing table.

A tracked IPv6 route is considered to match an entry in the routing table only if the exact IPv6 address and prefix length match a table entry. For example, when configured as a tracked route, 3333:100:200:300::/80 does not match routing table entry 3333:100:200:300::/64. If no route-table entry has the exact IPv6 address and prefix length, the status of the tracked route is considered to be DOWN.

When you configure the threshold of an IPv6 route metric as a tracked object, the UP/DOWN state of the tracked route is also determined by the current metric for the route in the routing table.

To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible. The scaled metric value communicated to a client always considers a lower value to have priority over a higher value. The resulting scaled value is compared against the configured threshold values to determine the state of a tracked route as follows:

- If the scaled metric for a route entry is less than or equal to the UP threshold, the state of a route is UP.
- If the scaled metric for a route is greater than or equal to the DOWN threshold or the route is not entered in the routing table, the state of a route is DOWN.

You configure the UP and DOWN thresholds for each tracked IPv6 route by using the `threshold metric` command. The default UP threshold is 254; the default DOWN threshold is 255. The notification of a change in the state of a tracked object is sent when a metric value crosses a configured threshold.
track ipv6 route reachability

Configure object tracking on the reachability of an IPv6 route.

Syntax

```
track object-id ipv6 route ip-address/prefix-len reachability
```

To return to the default setting, enter `no track object-id`.

Parameters

- **object-id**: Enter the ID number of the tracked object. Range: 1 to 65535.
- **ipv6-address/prefix-len**: Enter an IPv6 address in X:X:: format. Valid IPv6 prefix lengths are from /0 to /128.

Defaults

None

Command Modes

CONFIGURATION

Command History

- **Version 8.4.1.0**: Introduced

Related Commands

- `show track ipv6 route`: Display information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- `track ip route reachability`: Configure object tracking on the reachability of an IPv4 route.

Usage Information

Use this command to create an object that tracks the reachability of an IPv6 route. In order for a route’s reachability to be tracked, the route must appear as an entry in the routing table.

A tracked route is considered to match an entry in the routing table only if the exact IPv6 address and prefix length match a table entry. For example, when configured as a tracked route, 3333:100:200:400::/80 does not match routing table entry 3333:100:200::/64. If no route-table entry has the exact IPv6 address and prefix length, the tracked route is considered to be DOWN.

When you configure IPv6 route reachability as a tracked object, the UP/DOWN state of the tracked route is also determined by the entry of the next-hop address in the ARP cache. A tracked route is considered to be reachable if there is an ARP cache entry for the route's next-hop address.

If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to regenerate the ARP cache entry to see if the next-hop address appears before considering the route DOWN.
track resolution ipv6 route

Configure the protocol-specific resolution value used to scale an IPv6 route metric.

Syntax

track resolution ipv6 route {isis resolution-value | ospf resolution-value}

To return to the default setting, enter no track object-id.

Parameters

object-id Enter the ID number of the tracked object. Range: 1 to 65535.

isis resolution-value Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.

ospf resolution-value Enter the resolution used to convert the metric in the routing table for OSPF routes to a scaled metric.

Defaults

None

Command Modes

CONFIGURATION

Command History

Version 8.4.1.0 Introduced

Related Commands

threshold metric Configure the metric threshold used to determine the UP and/or DOWN state of a tracked route.

track ipv6 route metric threshold Configure object tracking on the threshold of an IPv6 route metric.

Usage Information

Use this command to configure the protocol-specific resolution value that converts the actual metric of an IPv6 route in the routing table to a scaled metric in the range 0 to 255.

The UP/DOWN state of a tracked IPv6 route is determined by the user-configurable threshold (threshold metric command) for a route’s metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible.

The protocol-specific resolution value calculates the scaled metric by dividing a route's cost by the resolution value set for the route protocol:

- For ISIS, you can set the resolution in the range 1 to 1000, where the default is 10.
- For OSPF, you can set the resolution in the range 1 to 1592, where the default is 1.
- The resolution value used to map static routes is not configurable. By default, Dell Networking OS assigns a metric of 0 to static routes.
- The resolution value used to map RIP routes is not configurable. The RIP hop-count is automatically multiplied by 16 to scale it. For example, a RIP metric of 16 (unreachable) scales to 256, which considers the route to be DOWN.
Open Shortest Path First (OSPFv2 and OSPFv3)

Overview

Open Shortest Path First version 2 for IPv4 is supported on platforms C E S

Open Shortest Path First version 3 (OSPFv3) for IPv6 is supported on platforms C E

Note: The C-Series supports OSPFv3 with Dell Networking OS version 7.8.1.0 and later.

OSPF is an Interior Gateway Protocol (IGP), which means that it distributes routing information between routers in a single Autonomous System (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, etc.) are the same for OSPFv2 and OSPFv3. OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis.

This chapter is divided into 2 sections. There is no overlap between the two sets of commands. You cannot use an OSPFv2 command in the IPv6 OSPFv3 mode.

- OSPFv2 Commands
- OSPFv3 Commands

Note: Dell Networking OS version 7.8.1.0 introduces Multi-Process OSPF on IPv4 (OSPFv2) only. It is not supported on OSPFv3 (IPv6).

Note that the CLI now requires that the Process ID be included when entering the ROUTER-OSPF mode. Each command entered applies to the specified OSPFv2 process only.

OSPFv2 Commands

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

- area default-cost
- area nssa
- area range
- area stub
- area virtual-link
- 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
• enable inverse mask
• fast-convergence
• flood-2328
• graceful-restart grace-period
• graceful-restart helper-reject
• graceful-restart mode
• graceful-restart role
• 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
• max-metric router-lsa
• maximum-paths
• mib-binding
• network area
• passive-interface
• redistribute
• redistribute bgp
• redistribute isis
• 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
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

<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>cost</td>
<td>Specifies the stub area’s advertised external route metric. Range: 0 to 65535.</td>
</tr>
</tbody>
</table>

Defaults

cost = 1; no areas are configured.

Command Modes

ROUTER OSPF

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Changed Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

In FTOS, cost is defined as reference bandwidth/bandwidth.

Related Commands
da

Create 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, enter no area area-id nssa.

Parameters

area-id
Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from 0 and 65535.

no-redistribution (OPTIONAL) Specify that the redistribute command should not distribute routes into the NSSA. You should only use this command in a NSSA Area Border Router (ABR).

default-information-originate (OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.

no-summary (OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

Defaults
Not configured

Command Mode
ROUTER OSPF

Command History

Version 7.8.1.0 Introduced support for Multi-Process OSPF.
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
pre-Version 6.1.1.1 Introduced on E-Series

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

area-id
Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from zero (0) to 65535.

ip-address
Specify an IP address in dotted decimal format.

mask
Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).

not-advertise (OPTIONAL) Enter the keyword not-advertise to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)

Defaults
No range is configured.

Command Modes
ROUTER OSPF

Command History

Version 7.8.1.0 Introduced support for Multi-Process OSPF.
Version 7.6.1.0 Introduced on S-Series
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area stub</td>
<td>Create a stub area.</td>
</tr>
<tr>
<td>area virtual-link</td>
<td>Set a virtual link and its parameters.</td>
</tr>
</tbody>
</table>

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, enter `no area area-id stub`.

Parameters

- **area-id**: Specify the stub area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
- **no-summary**: (OPTIONAL) Enter the keyword `no-summary` to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.

Defaults

Disabled

Command Modes

ROUTER OSPF

Command History

- Version 7.8.1.0: Introduced support for Multi-Process OSPF.
- Version 7.6.1.0: Introduced on S-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.1: Introduced on E-Series

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>Enter the ROUTER OSPF mode to configure an OSPF instance.</td>
</tr>
</tbody>
</table>
To delete a parameter of a virtual link, use the no area area-id virtual-link router-id
[[authentication-key [encryption-type] key] | [message-digest-key keyid md5
[encryption-type] key]] [dead-interval seconds] [hello-interval seconds]
[retransmit-interval seconds] [transmit-delay seconds] command syntax.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>Specify the transit area for the virtual link in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.</td>
</tr>
<tr>
<td>router-id</td>
<td>Specify an ID (IP address in dotted decimal format) associated with a virtual link neighbor.</td>
</tr>
<tr>
<td>authentication-key</td>
<td>(OPTIONAL) Choose between two authentication methods:</td>
</tr>
<tr>
<td>[encryption-type] key]</td>
<td>- Enter the keyword authentication-key to enable simple authentication followed by an alphanumeric string up to 8 characters long. Optionally, for the encryption-type variable, enter the number 7 before entering the key string to indicate that an encrypted password will follow.</td>
</tr>
<tr>
<td>message-digest-key</td>
<td>- Enter the keyword message-digest-key followed by a number from 1 to 255 as the keyid. After the keyid, enter the keyword md5 followed by the key. The key is an alphanumeric string up to 16 characters long. Optionally, for the encryption-type variable, enter the number 7 before entering the key string to indicate that an encrypted password will follow.</td>
</tr>
<tr>
<td>keyid</td>
<td></td>
</tr>
<tr>
<td>md5</td>
<td></td>
</tr>
<tr>
<td>[encryption-type] key]</td>
<td></td>
</tr>
<tr>
<td>dead-interval seconds</td>
<td>(OPTIONAL) Enter the keyword dead-interval followed by a number as the number of seconds for the interval. Range: 1 to 8192. Default: 40 seconds.</td>
</tr>
<tr>
<td>hello-interval seconds</td>
<td>(OPTIONAL) Enter the keyword hello-interval followed by the number of seconds for the interval. Range: 1 to 8192. Default: 10 seconds.</td>
</tr>
<tr>
<td>retransmit-interval</td>
<td>(OPTIONAL) Enter the keyword retransmit-interval followed by the number of seconds for the interval. Range: 1 to 8192. Default: 5 seconds.</td>
</tr>
<tr>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td>transmit-delay seconds</td>
<td>(OPTIONAL) Enter the keyword transmit-delay followed by the number of seconds for the interval. Range: 1 to 8192. Default: 1 second.</td>
</tr>
</tbody>
</table>

| Defaults                | dead-interval seconds = 40 seconds; hello-interval seconds = 10 seconds; retransmit-interval
|                        | seconds = 5 seconds; transmit-delay seconds = 1 second                                               |

| Command Modes           | ROUTER OSPF                                                                                          |

| Command History         | Version 7.8.1.0 Introduced support for Multi-Process OSPF.                                            |
|                        | Version 7.6.1.0 Introduced on S-Series                                                                |
|                        | Version 7.5.1.0 Introduced on C-Series                                                                |
|                        | pre-Version 6.1.1.1 Introduced on E-Series                                                           |

| Usage Information       | All OSPF areas must be connected to a backbone area (usually Area 0). Virtual links connect broken or
discontiguous areas. |
You cannot enable both authentication options. Choose either the `authentication-key` or `message-digest-key` option.

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**clear ip ospf**

Clear all OSPF routing tables.

**Syntax**

```
clear ip ospf process-id [vrf vrf-name] [process]
```

- `process-id` Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- `process` (OPTIONAL) Enter the keyword `process` to reset the OSPF process.

**Command Modes**

- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
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 a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **C-Series** and **S-Series**: Range: 1-128
    - **E-Series**: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

- **neighbor router-id**
  - (OPTIONAL) Enter the keyword `neighbor` followed by the neighbor’s router-id in dotted decimal format (A.B.C.D.).

**Defaults**

No defaults values or behavior

**Command Modes**

EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 7.8.1.0** Introduced support for Multi-Process OSPF.
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **Version 7.4.1.0** Introduced on E-Series

**Related Commands**

- `show ip ospf statistics` — Display the OSPF statistics

---

display ip ospf

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

**Syntax**

```
display ip ospf [process-id] [vrf vrf-name] [bfd | event | packet | spf]
```

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.

- **vrf**
  - **vrf-name**: (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.

- **bfd**: (OPTIONAL) Enter the keyword `bfd` to debug only OSPF BFD information.

- **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.

### Command Modes

- **EXEC Privilege**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

### Example

**Figure 38-1. Command example: debug ip ospf process-id packet**

```
FTOS#debug ip ospf 1 packet
OSPF process 90, packet debugging is on
FTOS#
08:14:24 : OSPF(100:00): Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
      aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Gi 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 38-1. Output Descriptions for debug ip ospf process-id packet

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:14</td>
<td>Displays the time stamp.</td>
</tr>
<tr>
<td>OSPF</td>
<td>Displays the OSPF process ID: instance ID.</td>
</tr>
<tr>
<td>v:</td>
<td>Displays the OSPF version. FTOS supports version 2 only.</td>
</tr>
<tr>
<td>t:</td>
<td>Displays the type of packet sent:</td>
</tr>
<tr>
<td></td>
<td>• 1 - Hello packet</td>
</tr>
<tr>
<td></td>
<td>• 2 - database description</td>
</tr>
<tr>
<td></td>
<td>• 3 - link state request</td>
</tr>
<tr>
<td></td>
<td>• 4 - link state update</td>
</tr>
<tr>
<td></td>
<td>• 5 - link state acknowledgement</td>
</tr>
<tr>
<td>l:</td>
<td>Displays the packet length.</td>
</tr>
<tr>
<td>rid:</td>
<td>Displays the OSPF router ID.</td>
</tr>
<tr>
<td>aid:</td>
<td>Displays the Autonomous System ID.</td>
</tr>
<tr>
<td>chk:</td>
<td>Displays the OSPF checksum.</td>
</tr>
</tbody>
</table>
To 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, enter `no default-information originate`.

**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 7.8.1.0 Introduced support for Multi-Process OSPF.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

**Related Commands**

- redistribute Redistribute 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, enter `no default-metric [number]`.

**Parameters**

- `number` Enter a number as the metric.
  - Range: 1 to 16777214.

**Defaults**

Disabled.

**Command Modes**

ROUTER OSPF

**Command History**

- Version 7.8.1.0 Introduced support for Multi-Process OSPF.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

**Related Commands**

- redistribute Redistribute routes from other routing protocols into OSPF.

---

**description**

Add a description about the selected OSPF configuration.

**Syntax**

```
description description
```

**Defaults**

No default description.
To remove the OSPF description, use the **no description** command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>description</strong></td>
<td>Enter a text string description to identify the OSPF configuration (80 characters maximum).</td>
<td>No default behavior or values</td>
</tr>
</tbody>
</table>

| Command Modes       | ROUTER OSPF                                                                 |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Version 7.8.1.0 Introduced support for Multi-Process OSPF.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Version 7.6.1.0 Introduced on S-Series</td>
</tr>
<tr>
<td></td>
<td>Version 7.5.1.0 Introduced on C-Series</td>
</tr>
<tr>
<td></td>
<td>pre-Version 6.1.1.1 Introduced on E-Series</td>
</tr>
</tbody>
</table>

| Related Commands    | show ip ospf asbr Display 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.

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

| Command Modes       | ROUTER OSPF                                                                 |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Version 7.8.1.0 Introduced support for Multi-Process OSPF.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Increased name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td></td>
<td>Version 7.6.1.0 Introduced on S-Series</td>
</tr>
<tr>
<td></td>
<td>Version 7.5.1.0 Introduced on C-Series</td>
</tr>
<tr>
<td></td>
<td>pre-Version 6.1.1.1 Introduced on E-Series</td>
</tr>
</tbody>
</table>
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, enter no distance ospf.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>external dist3</td>
<td>(OPTIONAL) Enter the keyword external followed by a number to specify a</td>
</tr>
<tr>
<td></td>
<td>distance for external type 5 and 7 routes.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 255</td>
</tr>
<tr>
<td></td>
<td>Default: 110.</td>
</tr>
<tr>
<td>inter-area dist2</td>
<td>(OPTIONAL) Enter the keyword inter-area followed by a number to specify a</td>
</tr>
<tr>
<td></td>
<td>distance metric for routes between areas.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 255</td>
</tr>
<tr>
<td></td>
<td>Default: 110.</td>
</tr>
<tr>
<td>intra-area dist1</td>
<td>(OPTIONAL) Enter the keyword intra-area followed by a number to specify a</td>
</tr>
<tr>
<td></td>
<td>distance metric for all routes within an area.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 255</td>
</tr>
<tr>
<td></td>
<td>Default: 110.</td>
</tr>
</tbody>
</table>

Defaults

external dist3 = 110; inter-area dist2 = 110; intra-area dist1 = 110.

Command Modes

ROUTER OSPF

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

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.
### 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 [bgp | connected | isis | rip | static]
```

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

**Parameters**

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

* BGP and ISIS routes are not available on the C-Series.
BGP, ISIS, and RIP routes are not available on the S-Series.
Defaults
Not configured.

Command Modes
ROUTER OSPF

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

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.

enable inverse mask
Dell Networking OS, by default, permits the user to input OSPF `network` command with a net-mask. This command provides a choice between inverse-mask or net-mask (the default).

Syntax
`enable inverse mask`

To return to the default net-mask, enter `no enable inverse mask`.

Defaults
net-mask

Command Modes
CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

fast-convergence
This command sets the minimum LSA origination and arrival times to zero (0), allowing more rapid route computation so that convergence takes less time.

Syntax
`fast-convergence {number}`

To cancel fast-convergence, enter `no fast convergence`.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the convergence level desired. The higher this parameter is set, the</td>
</tr>
<tr>
<td></td>
<td>faster OSPF converge takes place.</td>
</tr>
<tr>
<td></td>
<td>Range: 1-4</td>
</tr>
</tbody>
</table>

Defaults
None.

Command Modes
ROUTER OSPF

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on all platforms.</td>
</tr>
</tbody>
</table>
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 Networking technical support.

**flood-2328**

Enable RFC-2328 flooding behavior.

**Syntax**

`flood-2328`

To disable, use the **no flood-2328** command.

**Defaults**

Disabled

**Command Modes**

ROUTER OSPF

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series and E-Series</td>
</tr>
</tbody>
</table>

**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, Dell Networking OS 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 Dell Networking OS to flood LSAs on all interfaces.

**graceful-restart grace-period**

Specifies the time duration, in seconds, that the router’s neighbors will continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

**Syntax**

`graceful-restart grace-period seconds`

To disable the grace period, enter **no graceful-restart grace-period**.

**Parameters**

- `seconds` Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process.
  Range: 40 to 3000 seconds

**Defaults**

Not Configured
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 7.8.1.0: Introduced support for Multi-Process OSPF.
- Restart role enabled on S-Series (Both Helper and Restart roles now supported on S-Series).
- Version 7.7.1.0: Helper-Role supported on S-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.1: Introduced on E-Series

graceful-restart mode

Enable the graceful restart mode.

Syntax

```
graceful-restart mode [planned-only | unplanned-only]
```

To disable graceful restart mode, enter `no graceful-restart mode`.

Parameters

- `planned-only`: (OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only.
- `unplanned-only`: (OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only.

Defaults

Support for both planned and unplanned failures.

Command Modes

ROUTER OSPF

Command History

- Version 7.8.1.0: Introduced on S-Series
graceful-restart role

Specify the role for your OSPF router during graceful restart.

Syntax

```
graceful-restart role [helper-only | restart-only]
```

To disable graceful restart role, enter `no graceful-restart role`.

Parameters

- **role helper-only** (OPTIONAL) Enter the keywords `helper-only` to specify the OSPF router as a helper only during graceful restart.
- **role restart-only** (OPTIONAL) Enter the keywords `restart-only` to specify the OSPF router as a restart only during graceful-restart.

Defaults

OSPF routers are, by default, both helper and restart routers during a graceful restart.

Command Modes

- ROUTER OSPF

Command History

- Version 7.8.1.0 Introduced support for Multi-Process OSPF.
- Restart and helper roles supported on S-Series
- Version 7.7.1 Helper-Role supported on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

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, enter `no ip ospf auth-change-wait-time`.

Parameters

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

Defaults

zero (0) seconds

Command Modes

- INTERFACE

Command History

- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series
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, enter `no ip ospf authentication-key`.

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 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

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, enter `no ip ospf cost`.

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 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

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` Control 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, enter `no ip ospf dead-interval`.

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 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

Usage Information

By default, the dead interval is four times the default hello-interval.

Related Commands

- `ip ospf hello-interval` Set 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, enter `no ip ospf hello-interval`.

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 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

Usage Information

The time interval between hello packets must be the same for routers in a network.

Related Commands

- `ip ospf dead-interval` Set 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**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 Networking recommends keeping only one key per interface.

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

---

**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, enter `no ip ospf mtu-ignore`.

**Defaults**

Enabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
ip ospf network

Set the network type for the interface.

Syntax

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

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

ROUTER OSPF

Command History

- Version 7.8.1.0 Introduced support for Multi-Process OSPF.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

ip ospf priority

Set the priority of the interface to determine the Designated Router for the OSPF network.

Syntax

```
 ip ospf priority number
```

Parameters

- **number**: Enter a number as the priority.
  - Range: 0 to 255.
  - The default is 1.

Defaults

1

Command Modes

INTERFACE

Command History

- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

Usage Information

Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.
### ip ospf retransmit-interval

Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

**Syntax**

```plaintext
ip ospf retransmit-interval seconds
```

To return to the default values, enter `no ip ospf retransmit-interval`.

**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 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

**Usage Information**

Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval should be larger for interfaces connected to virtual links.

### ip ospf transmit-delay

Set the estimated time elapsed to send a link state update packet on the interface.

**Syntax**

```plaintext
ip ospf transmit-delay seconds
```

To return to the default value, enter `no ip ospf transmit-delay`.

**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 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series
**log-adjacency-changes**

Generate a Syslog message for OSPF adjacency state changes. When enabled, changes are logged for both IPv4 and IPv6 adjacencies.

**Syntax**

```
log-adjacency-changes
```

**Defaults**

Disabled.

**Command Mode**

ROUTER OSPF

**Command History**

+-----------------+---------------------------------------------------------------------+
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced for IPv6.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**max-metric router-lsa**

Configure the maximum cost of 65535 on a new router so that it functions as a stub router in the network and OSPF traffic destined to other networks is not forwarded on a path through the router.

**Syntax**

```
max-metric router-lsa [on-startup {announce-time | wait-for-bgp [wait-time]}]
```

To remove the maximum metric assignment from an OSPF router and send LSAs with the currently configured cost, enter `no max-metric router-lsa [on-startup {announce-time | wait-for-bgp [wait-time]}].`

**Parameters**

- **on-startup announce-time**
  - Enter the time (in seconds) following boot-up during which the maximum cost (65535) for transmitting OSPF traffic on router interfaces is announced in LSAs and the router functions as a stub router.
  - Range: 5 to 86400 seconds.

- **on-startup wait-for-bgp [wait-time]**
  - Enable the router to announce the maximum metric in OSPF LSAs until the BGP routing table converges with updated routes.
  - Default: 600 seconds.
  - You can also specify the time (in seconds) that the router waits for the BGP routing table to converge before it stops advertising the maximum cost in LSAs and advertises the router’s currently configured OSPF cost. Range: 5 to 86400 seconds.

**Defaults**

Not Configured

**Command Modes**

- ROUTER OSPF

**Command History**

+-----------------+---------------------------------------------------------------------+
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.5</td>
<td>Introduced on C-Series and E-Series TeraScale.</td>
</tr>
<tr>
<td>8.4.1.3</td>
<td>Introduced on E-Series ExaScale.</td>
</tr>
</tbody>
</table>
When you bring a new router onto an OSPF network, you can configure the router to function as a stub router by globally reconfiguring the OSPF link cost so that other routers do not use a path that forwards traffic destined to other networks through the new router for a specified time until the router’s switching and routing functions are up and running, and the routing tables in network routers have converged.

By using the **max-metric router-lsa** command, you force the link cost of all OSPF non-stub links to the maximum link cost (65535). The advertisement of this maximum metric causes other routers to assign a cost to the new router that is higher than the cost of using an alternate path. Because of the high cost assigned to paths that pass through the new router, other routers will not use a path through the router as a transit path to forward traffic to other networks.

Use the **max-metric router-lsa** command to gracefully shut down or reload a router without dropping packets destined for other networks.

**Note:** If you enter the **max-metric router-lsa** command without an option (**on-startup announce-time** or **on-startup wait-for-bgp** [**wait-time**]), the maximum metric of 65535 is always announced in LSAs sent by the router.

### Example

**Figure 38-2. Command Example: max-metric router-lsa**

```plaintext
FTOS(conf)#router ospf 10
FTOS(conf-router_ospf)#log-adjacency-changes
FTOS(conf-router_ospf)#network 4.1.1.0/24 area 0
FTOS(conf-router_ospf)#network 1.1.1.0/24 area 1
FTOS(conf-router_ospf)#max-metric router-lsa on-startup wait-for-bgp
FTOS(conf-router_ospf)#exit

FTOS(conf)#show ip ospf
Routing Process ospf 10 with ID 100.1.1.1 Virtual router default-vrf
Supports only single TOS (TOS0) routes
It is an Area Border Router
Originating router lsas with maximum metric
Time remaining 00:07:07
Condition : On-Startup while BGP is converging for 600 secs. State : Active
SPF schedule delay 5 secs, Hold time between two SPF s 10 secs
Convergence Level 0
Min LSA origination 5 secs, Min LSA arrival 1 secs
Number of area in this router is 2, normal 2 stub 0 nssa 0
  Area BACKBONE (0)
    Number of interface in this area is 1
    SPF algorithm executed 3 times
    Area ranges are
  Area 1
    Number of interface in this area is 1
    SPF algorithm executed 3 times
    Area ranges are

FTOS(conf)#show ip ospf database router
Exception Flag: Announcing maximum link costs
LS age: 198
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 2.1.1.1
Advertising Router: 2.1.1.1
LS Seq Number: B0000005
Checksum: 0x9F5D
Length: 48
Number of Links: 2
```
maximum-paths

Enable the software to forward packets over multiple paths.

Syntax

```
maximum-paths number
```

To disable packet forwarding over multiple paths, enter `no maximum-paths`.

Parameters

```
number
  Specify the number of paths.
  Range: 1 to 16.
  Default: 4 paths.
```

Defaults

```
4
```

Command Modes

```
ROUTER OSPF
```

Command History

```
Version 7.8.1.0    Introduced support for Multi-Process OSPF.
Version 7.6.1.0    Introduced on S-Series
Version 7.5.1.0    Introduced on C-Series
pre-Version 6.1.1.1 Introduced on E-Series
```

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, enter `no mib-binding`.

Defaults

```
None.
```

Command Modes

```
ROUTER OSPF
```

Command History

```
Version 7.8.1.0    Introduced to all platforms.
```

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>Enter a network mask in /prefix format. (/x)</td>
</tr>
<tr>
<td><strong>area-id</strong></td>
<td>Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range: 0 to 65535. IP address format: dotted decimal format A.B.C.D.  <strong>Note:</strong> If the area ID is smaller than 65535, it will be converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it will be converted to 1.</td>
</tr>
</tbody>
</table>

### Command Modes

**ROUTER OSPF**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

To enable OSPF on an interface, the **network area** command must include, in its range of addresses, the primary IP address of an interface.

**Note:** An interface can be attached only to a single OSPF area.

If you delete all the **network area** commands for Area 0, the **show ip ospf** command output will not list Area 0.

#### passive-interface

**C E S**

Suppress both receiving and sending routing updates on an interface.

**Syntax**

```
passive-interface {default | interface}
```

To enable both the receiving and sending routing, enter the **no passive-interface interface** command.

To return all OSPF interfaces (current and future) to active, enter the **no passive-interface default** command.
**default**
Enter the keyword `default` to make all OSPF interfaces (current and future) passive.

**interface**
Enter the following keywords and slot/port or number information:
- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - **C-Series** and **S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

---

**Command Modes**

- **ROUTER OSPF**

---

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Modified to include the <code>default</code> keyword.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**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

**Syntax**

```
redistribute {connected | rip | static} [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]
```

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

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>Enter the keyword <code>connected</code> to specify that information from active routes on interfaces is redistributed.</td>
</tr>
<tr>
<td>rip</td>
<td>Enter the keyword <code>rip</code> to specify that RIP routing information is redistributed.</td>
</tr>
<tr>
<td>static</td>
<td>Enter the keyword <code>static</code> to specify that information from static routes is redistributed.</td>
</tr>
<tr>
<td>metric metric-value</td>
<td>(OPTIONAL) Enter the keyword <code>metric</code> followed by a number. Range: 0 (zero) to 16777214.</td>
</tr>
</tbody>
</table>
| metric-type type-value | (OPTIONAL) Enter the 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 7.8.1.0 Introduced support for Multi-Process OSPF.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

**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><code>default-information originate</code></td>
<td>Generate a default route into the OSPF routing domain.</td>
</tr>
</tbody>
</table>
**redistribute bgp**

Redistribute BGP routing information throughout the OSPF instance.

**Syntax**

```
redistribute bgp as number [metric metric-value] | [metric-type type-value] | [tag tag-value]
```

To disable redistribution, use the `no redistribute bgp as number [metric metric-value] | [metric-type type-value] | [route-map map-name] | [tag tag-value]` command.

**Parameters**

- **as number**
  
  Enter the autonomous system number.
  
  Range: 1 to 65535

- **metric metric-value**
  
  (OPTIONAL) Enter the keyword `metric` followed by the metric-value number.
  
  Range: 0 to 16777214

- **metric-type type-value**
  
  (OPTIONAL) Enter the keyword `metric-type` followed by one of the following:
  
  - 1 = for OSPF External type 1
  - 2 = for 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` to set the tag for routes redistributed into OSPF.
  
  Range: 0 to 4294967295

**Defaults**

No default behavior or values

**Command Modes**

ROUTER OSPF

**Command History**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.3</td>
<td>Introduced Route Map for BGP Redistribution to OSPF</td>
</tr>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>Version 7.4.1.0</td>
<td>Modified to include the <code>default</code> keyword.</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**redistribute isis**

Redistribute IS-IS routing information throughout the OSPF instance.

**Syntax**

```
redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]
```

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]` command.

**Parameters**

- **tag**
  
  (OPTIONAL) Enter the name of the IS-IS routing process.

- **level-1**
  
  (OPTIONAL) Enter the keyword `level-1` to redistribute only IS-IS Level-1 routes.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>level-1-2</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>level-1-2</strong> to redistribute both IS-IS Level-1 and Level-2 routes.</td>
</tr>
<tr>
<td><strong>level-2</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>level-2</strong> to redistribute only IS-IS Level-2 routes.</td>
</tr>
<tr>
<td><strong>metric metric-value</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>metric</strong> followed by a number. Range: 0 (zero) to 4294967295.</td>
</tr>
</tbody>
</table>
| **metric-type type-value** | (OPTIONAL) Enter the keyword **metric-type** followed by one of the following:  
  - 1 = for OSPF External type 1  
  - 2 = for 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**
IS-IS is not supported on S-Series platforms.

---

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the router ID in the IP address format</td>
</tr>
</tbody>
</table>

**Defaults**
This command has no default behavior or values.

**Command Modes**
ROUTER OSPF

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
Example

**Figure 38-3. Command Example: router-id**

FTOS(conf)#router ospf 100
FTOS(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/n]:

FTOS(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
FTOS(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/n]:
FTOS#

Usage Information

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If 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**

```plaintext
C E S
```

Enter the ROUTER OSPF mode to configure an OSPF instance.

**Syntax**

```plaintext
router ospf process-id [vrf {vrf name}]
```

To clear an OSPF instance, enter `no router ospf process-id`.

**Parameters**

- `process-id` Enter a number for the OSPF instance.
  - Range: 1 to 65535.
- `vrf name` (Optional) **E-Series Only**: Enter the VRF process identifier to tie the OSPF instance to the VRF. All network commands under this OSPF instance are subsequently tied to the VRF instance.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

- **Version 7.9.1.0** Introduced VRF
- **Version 7.8.1.0** Introduced support of Multi-Process OSPF.
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **pre-Version 6.1.1.1** Introduced on E-Series

**Example**

**Figure 38-4. Command Example: router ospf**

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.

Once the OSPF process and the VRF are tied together, the OSPF Process ID cannot be used again in the system.
show config

Display the non-default values in the current OSPF configuration.

**Syntax**

`show config`

**Command Modes**

ROUTER OSPF

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 38-5. Command Example: show config**

```
FTOS(conf-router_ospf)#show config
!
router ospf 3
  passive-interface FastEthernet 0/1
FTOS(conf-router_ospf)#
```

show ip ospf

Display information on the OSPF process configured on the switch.

**Syntax**

`show ip ospf process-id [vrf vrf name]`

**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.
- `vrf name`: 
  - E-Series Only: Show only the OSPF information tied to the VRF process.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced <code>process-id</code> option, in support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

If you delete all the network area commands for Area 0, the `show ip ospf` command output will not list Area 0.
Example

Figure 38-6. Command Example: show ip ospf process-id

FTOS>show ip ospf 1
Routing Process ospf 1 with ID 11.1.2.1
Supports only single TOS (TOS0) routes
It is an autonomous system boundary router
SPF schedule delay 0 secs, Hold time between two SPFs 5 secs
Number of area in this router is 1, normal 1 stub 0 nssa 0
Area BACKBONE (0.0.0.0)
  Number of interface in this area is 2
  SPF algorithm executed 4 times
  Area ranges are

FTOS>

Table 38-2. Command Output Descriptions: show ip ospf process-id

<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>“Number of...”</td>
<td>Displays the number and type of areas configured for this process ID.</td>
</tr>
</tbody>
</table>

show ip ospf asbr

Syntax

show ip ospf process-id asbr

Parameters

process-id Enter the OSPF Process ID to show a specific process.

Defaults

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.8.1.0 Introduced support of Multi-Process OSPF.

Version 7.8.1.0 Introduced process-id option, in support of Multi-Process OSPF.

Version 7.6.1.0 Introduced on S-Series

Version 7.5.1.0 Introduced on C-Series and E-Series

Usage Information

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.
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 38-7. Command Example: show ip ospf process-id asbr**

```
FTOS#show ip ospf 1 asbr

RouterID         Flags    Cost   Nexthop         Interface    Area
3.3.3.3          -/-/-/   2      10.0.0.2        Gi 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 [vrf vrf-name] database [database-summary]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.</td>
</tr>
<tr>
<td>database-summary</td>
<td>(OPTIONAL) Enter the keywords database-summary to the display summary of the information stored in the OSPFv2 database of the router, including the number of LSAs received from OSPFv2 neighbor routers.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

**Example**

**Figure 38-8. Command Example: show ip ospf process-id database database-summary**

FTOS#show ip ospf database database-summary

OSPF Router with ID (200.1.1.1) (Process ID 1)

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Router Net</th>
<th>S-Net</th>
<th>S-ASBR</th>
<th>Type7</th>
<th>Type9</th>
<th>Type10</th>
<th>Total</th>
<th>ChSum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4</td>
<td>3</td>
<td>3000</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3008</td>
</tr>
</tbody>
</table>

**Example**

**Figure 38-9. Command Example: show ip ospf process-id database**

FTOS>show ip ospf 1 database

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

<table>
<thead>
<tr>
<th>Router (Area 0.0.0.0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
</tr>
<tr>
<td>11.1.2.1</td>
</tr>
<tr>
<td>13.1.1.1</td>
</tr>
<tr>
<td>192.68.135.2</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>12.2.3.0</td>
<td>11.1.2.1</td>
<td>718</td>
<td>0x80000002</td>
<td>0x792f</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>0x792f</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>0x792f</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>0x792f</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>0x45de</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>0x831e</td>
<td>0</td>
</tr>
<tr>
<td>12.1.1.0</td>
<td>11.1.1.1</td>
<td>1192</td>
<td>0x80000066</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>0x80000066</td>
<td>0x1c22</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>0xd8d6</td>
<td>0</td>
</tr>
</tbody>
</table>

**Table 38-3. Command Output Description: show ip ospf process-id database**

<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</td>
</tr>
<tr>
<td></td>
<td>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]

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 7.8.1.0 Introduced support of Multi-Process OSPF.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

Usage Information
If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

Example

```
Figure 38-10. Command Example: show ip ospf database asbr-summary (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: 0x800000010
Checksum: 0x4198
Length: 28
--More--
```
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 7.8.1.0: Introduced support of Multi-Process OSPF.
- Version 7.6.1.0: Introduced on S-Series

---

### Table 38-4. Command Output Descriptions: show ip ospf database asbr-summary

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA’s age.</td>
</tr>
</tbody>
</table>
| Options       | Displays the optional capabilities available on router. The following options can be found in this item:  
  - TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.  
  - DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.  
  - E or No E is displayed on whether the originating router can accept AS External LSAs. |
| LS Type       | Displays the LSA’s type.                                                   |
| Link State ID | Displays the Link State ID.                                                |
| Advertising Router | Identifies the advertising router’s ID.                              |
| Checksum     | Displays the Fletcher checksum of the an LSA's complete contents.         |
| Length        | Displays the length in bytes of the LSA.                                  |
| Network Mask  | Displays the network mask implemented on the area.                        |
| TOS           | Displays the Type of Service (TOS) options. Option 0 is the only option.  |
| Metric        | Displays the LSA metric.                                                  |

**Related Commands**

- `show ip ospf database`: Displays OSPF database information.
If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

**Example**

**Figure 38-11. Command Example: show ip ospf database external**

```
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
        Metric 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
        Metric Type: 2
        TOS: 0
        Metrics: 1
        Forward Address: 0.0.0.0
        External Route Tag: 701

FTOS#
```

**Table 38-5. Command Example Descriptions: show ip ospf process-id database external**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
</tbody>
</table>
| Options               | Displays the optional capabilities available on router. The following options can be found in this item:  
                        | • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.  
                        | • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.  
                        | • E or No E is displayed on whether the originating router can accept AS External LSAs. |
| LS Type               | Displays the LSA's type.                                                  |
| Link State ID         | Displays the Link State ID.                                               |
| Advertising Router    | Identifies the router ID of the LSA's originating router.                 |
Table 38-5. Command Example Descriptions: show ip ospf process-id database external

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Seq Number</td>
<td>Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA's complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Displays the network mask implemented on the area.</td>
</tr>
<tr>
<td>Metrics Type</td>
<td>Displays the external type.</td>
</tr>
<tr>
<td>TOS</td>
<td>Displays the TOS options. Option 0 is the only option.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Displays the LSA metric.</td>
</tr>
<tr>
<td>Forward Address</td>
<td>Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.</td>
</tr>
<tr>
<td>External Route Tag</td>
<td>Displays the 32-bit field attached to each external route. This field is not used by the OSPF protocol, but can be used for external route management.</td>
</tr>
</tbody>
</table>

**Related Commands**

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

**show ip ospf database network**

Display the network (type 2) LSA information.

**Syntax**

`show ip ospf process-id database network [link-state-id] [adv-router ip-address]`

**Parameters**

- `process-id` Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- `link-state-id` (OPTIONAL) Specify 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

**Example**

**Figure 38-12. Command Example: show ip ospf process-id database network**

```
FTOS#show ip ospf 1 data network

OSPF Router with ID (20.20.20.5) (Process ID 1)

Network (Area 0.0.0.0)
  LS age: 1372
  Options: (No TOS-capability, DC, E)
  LS type: Network
  Link State ID: 202.10.10.2
  Advertising Router: 20.20.20.8
  LS Seq Number: 0x80000006
  Checksum: 0xa35
  Length: 36
  Network Mask: /24
  Attached Router: 20.20.20.8
  Attached Router: 20.20.20.9
  Attached Router: 20.20.20.7

Network (Area 0.0.0.1)
  LS age: 252
  Options: (TOS-capability, No DC, E)
  LS type: Network
  Link State ID: 192.10.10.2
  Advertising Router: 192.10.10.2
  LS Seq Number: 0x80000007
  Checksum: 0x4309
  Length: 36
  Network Mask: /24
  Attached Router: 192.10.10.2
  Attached Router: 20.20.20.1
  Attached Router: 20.20.20.5
```

**Table 38-6. Command Example Descriptions: show ip ospf process-id database network**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>• E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA’s type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the router ID of the LSA’s originating router.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the Fletcher checksum of an LSA’s complete contents.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Attached Router</td>
<td>Identifies the IP address of routers attached to the network.</td>
</tr>
</tbody>
</table>
show ip ospf database nssa-external

Display NSSA-External (type 7) LSA information.

Syntax

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

Parameters

- `link-state-id` (OPTIONAL) Specify 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 7.8.1.0 Introduced support of Multi-Process OSPF.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

Usage Information

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

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

```
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 7.8.1.0: Introduced support of Multi-Process OSPF.
- Version 7.6.1.0: Introduced on S-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.1: Introduced on E-Series

Usage Information

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

Example

**Figure 38-13. Command Example: show ip ospf process-id database opaque-area (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)
    LS type: Type-10 Opaque Link Area
    Link State ID: 1.0.0.1
    Advertising Router: 10.16.1.160
    LS Seq Number: 0x80000416
    Checksum: 0x376
    Length: 28
    Opaque Type: 1
    Opaque ID: 1
    Unable to display opaque data

    LS age: 833
    Options: (No TOS-capability, No DC, E)
    LS type: Type-10 Opaque Link Area
    Link State ID: 1.0.0.2
    Advertising Router: 10.16.1.160
    LS Seq Number: 0x80000002
    Checksum: 0x19c2
    --More--
```

<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>
</tbody>
</table>
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 7.8.1.0: Introduced support of Multi-Process OSPF.
- Version 7.6.1.0: Introduced on S-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.1: Introduced on E-Series

Usage Information

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

Related Commands

- `show ip ospf database`: Displays OSPF database information.
- `show ip ospf database opaque-area`: 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]
```

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**

- `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` 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td></td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td></td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td></td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1</td>
<td></td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

**Related Commands**

- `show ip ospf database`  
  Displays OSPF database information.
If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

**Figure 38-14. Command Example: show ip ospf process-id database router (Partial)**

```
FTOS#show ip ospf 100 database router

OSPF Router with ID (1.1.1.10) (Process ID 100)

    Router (Area 0)

    LS age: 967
    Options: (No TOS-capability, No DC, E)
    LS type: Router
    Link State ID: 1.1.1.10
    Advertising Router: 1.1.1.10
    LS Seq Number: 0x8000012f
    Checksum: 0x3357
    Length: 144
    AS Boundary Router
    Area Border Router
    Number of Links: 10

    Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.129.1
    (Link Data) Router Interface address: 192.68.129.1
    Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.130.1
    (Link Data) Router Interface address: 192.68.130.1
    Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.142.2
    (Link Data) Router Interface address: 192.68.142.2
    Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.141.2
    (Link Data) Router Interface address: 192.68.141.2
    Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.140.2
    (Link Data) Router Interface address: 192.68.140.2
    Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Stub Network
    (Link ID) Network/subnet number: 11.1.5.0

--More--
Table 38-8. Command Example Descriptions: `show ip ospf process-id database router`

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
</tbody>
</table>
| Options         | Displays the optional capabilities available on router. The following options can be found in this item:  
|                 | • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.  
|                 | • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.  
|                 | • E or No E is displayed on whether the originating router can accept AS External LSAs. |
| LS Type         | Displays the LSA type.                                                       |
| Link State ID   | Displays the Link State ID.                                                  |
| Advertising Router | Identifies the router ID of the LSA’s originating router.                  |
| LS Seq Number   | Displays the link state sequence number. This number detects duplicate or old LSAs. |
| Checksum        | Displays the Fletcher checksum of an LSA’s complete contents.               |
| Length          | Displays the length in bytes of the LSA.                                    |
| Number of Links | Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line. |
| Link connected to: | Identifies the type of network to which the router is connected.         |
| (Link ID)       | Identifies the link type and address.                                        |
| (Link Data)     | Identifies the router interface address.                                     |
| Number of TOS Metric | Lists the number of TOS metrics.            |
| TOS 0 Metric    | Lists the number of TOS 0 metrics.                                          |

**Related Commands**

`show ip ospf database`  
Displays OSPF database information.

**Syntax**

`show ip ospf process-id database summary [link-state-id] [adv-router ip-address]`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>process-id</code></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`   | (OPTIONAL) Enter the keywords `adv-router` ip-address to display only the LSA information about that router. |
| `ip-address`   |                                                                             |
**Command Modes**

EXEC

**EXEC Privilege**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

**Example**

```
Figure 38-15. Command Example: show ip ospf process-id database summary

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)
    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)
    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)
    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
```
### Table 38-9. Command Example Descriptions: show ip ospf process-id database summary

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
</tbody>
</table>
| Options        | Displays the optional capabilities available on router. The following options can be found in this item:
|                | • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. |
|                | • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. |
|                | • E or No E is displayed on whether the originating router can accept AS External LSAs.                |
| LS Type        | Displays the LSA's type.                                                   |
| Link State ID  | Displays the Link State ID.                                                |
| Advertising Router | Identifies the router ID of the LSA's originating router.                  |
| LS Seq Number  | Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs. |
| Checksum       | Displays the Fletcher checksum of an LSA's complete contents.              |
| Length         | Displays the length in bytes of the LSA.                                  |
| Network Mask   | Displays the network mask implemented on the area.                        |
| TOS            | Displays the TOS options. Option 0 is the only option.                     |
| Metric         | Displays the LSA metrics.                                                 |

**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 a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port 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 a Port Channel interface, enter the keyword **port-channel** followed by a number:  
    - **C-Series** and **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword **sonet** followed by the 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.
  - For a VLAN, enter the keyword **vlan** followed by the VLAN ID. The range is from 1 to 4094.

**Command Modes**

- **EXEC**

**EXEC Privilege**

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced <strong>process-id</strong> option, in support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.
Example

Figure 38-16. Command Example: show ip ospf process-id interface

FTOS>show ip ospf int

GigabitEthernet 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)

GigabitEthernet 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 BROTHER, 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.

Table 38-10. Command Example Descriptions: show ip ospf process-id interface

<table>
<thead>
<tr>
<th>Line beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet...</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 configured.

Syntax show ip ospf process-id neighbor
**show ip ospf routes**

Display routes as calculated by OSPF and stored in OSPF RIB.

**Syntax**

```
show ip ospf process-id routes
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>process-id</code></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>

**Defaults**

No default values or behavior

**Command Modes**

EXEC
show ip ospf

Display OSPF statistics.

Syntax

show ip ospf process-id statistics global | [interface name {neighbor router-id}]

Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.</td>
</tr>
<tr>
<td>global</td>
<td>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.</td>
</tr>
</tbody>
</table>
### interface name

(OPTIONAL) Enter the keyword `interface` followed by one of the following interface keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - **C-Series and S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword `sonet` followed by the 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.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

### neighbor router-id

(OPTIONAL) Enter the keyword `neighbor` followed by the neighbor’s router-id in dotted decimal format (A.B.C.D.).

### Defaults

No default behavior or values

### Command Modes

EXEC

EXEC Privilege

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code></td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.
Example

Figure 38-19. Command Example: show ip ospf process-id statistics global

FTOS#show ip ospf 1 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>
<th>LSAck</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX</td>
<td>10</td>
<td>0</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</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>0</td>
<td>2</td>
</tr>
<tr>
<td>LSR-Q</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other-Q</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error packets (Only for RX)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf-Down</td>
<td>0</td>
<td>Non-Dr</td>
<td>0</td>
<td>Self-Org</td>
</tr>
<tr>
<td>Wrong-Len</td>
<td>0</td>
<td>Invld-Nbr</td>
<td>0</td>
<td>Nbr-State</td>
</tr>
<tr>
<td>Auth-Err</td>
<td>0</td>
<td>MD5-Err</td>
<td>0</td>
<td>Chksum</td>
</tr>
<tr>
<td>Version</td>
<td>0</td>
<td>AreaMis</td>
<td>0</td>
<td>Conf-Issues</td>
</tr>
<tr>
<td>No-Buffer</td>
<td>0</td>
<td>Seq-No</td>
<td>0</td>
<td>Socket</td>
</tr>
<tr>
<td>Q-Overflow</td>
<td>0</td>
<td>Unknown-Pkt</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error packets (Only for TX)</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Socket Errors</td>
<td>0</td>
<td></td>
<td></td>
<td>FTOS#</td>
</tr>
</tbody>
</table>

Table 38-12. Command Example Descriptions: show ip ospf statistics process-id global

<table>
<thead>
<tr>
<th>Row Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Displays the total number of packets received/transmitted by the OSPF process</td>
</tr>
<tr>
<td>Error</td>
<td>Displays the error count while receiving and transmitting packets by the OSPF process</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of OSPF Hello packets</td>
</tr>
<tr>
<td>DDiscr</td>
<td>Number of database description packets</td>
</tr>
<tr>
<td>LSReq</td>
<td>Number of link state request packets</td>
</tr>
<tr>
<td>LSUpd</td>
<td>Number of link state update packets</td>
</tr>
<tr>
<td>LSAck</td>
<td>Number of link state acknowledgement packets</td>
</tr>
<tr>
<td>TxQ-Len</td>
<td>The transmission queue length</td>
</tr>
<tr>
<td>RxQ-Len</td>
<td>The reception queue length</td>
</tr>
<tr>
<td>Tx-Mark</td>
<td>The highest number mark in the transmission queue</td>
</tr>
<tr>
<td>Rx-Mark</td>
<td>The highest number mark in the reception queue</td>
</tr>
<tr>
<td>Hello-Q</td>
<td>The queue, for transmission or reception, for the hello packets</td>
</tr>
<tr>
<td>LSR-Q</td>
<td>The queue, for transmission or reception, for the link state request packets.</td>
</tr>
<tr>
<td>Other-Q</td>
<td>The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.</td>
</tr>
</tbody>
</table>

Table 38-13. Error Definitions: show ip ospf statistics process-id global

<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>
</tbody>
</table>
Table 38-13. Error Definitions: show ip ospf statistics *process-id* global

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</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
Example

Figure 38-20. Command Example: show ip ospf process-id statistics

FTOS#show ip ospf 100 statistics

Interface GigabitEthernet 0/8

Hello-Timer 9, Wait-Timer 0, Grace-Timer 0
Error packets (Only for RX)

Intf-Down 0 Non-Dr 0 Self-Org 0
Wrong-Len 0 Invl-Nbr 0 Nbr-State 0
Auth-Error 0 MD5-Error 0 Cksum-Err 0
Version 0 AreaMisMatch 0 Conf-Issue 0
SeqNo-Err 0 Unknown-Pkt 0

Neighbor ID 9.1.1.2

<table>
<thead>
<tr>
<th>Hello</th>
<th>DDiscr</th>
<th>LSReq</th>
<th>LSUpd</th>
<th>LSAck</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX 59</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>TX 62</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Dead-Timer 37, Transmit-Timer 0
LSU-Q-Len 0, LSU-Q-Wmark 0
LSR-Q-Len 0, LSR-Q-Wmark 1

Related Commands

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

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

No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.8.1.0 Introduced support of Multi-Process OSPF.
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series and E-Series

Usage Information

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

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.
show ip ospf virtual-links

Display the OSPF virtual links configured and is useful for debugging OSPF routing operations. If no OSPF virtual-links are enabled on the switch, no output is generated.

Syntax

```
show ip ospf process-id virtual-links
```

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 7.8.1.0: Introduced support of Multi-Process OSPF.
- Version 7.6.1.0: Introduced on S-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.1: Introduced on E-Series

Usage Information

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

Example

```
Figure 38-22. Command Example: show ip ospf process-id virtual-links

FTOS#show ip ospf 1 virt

Virtual Link to router 192.168.253.5 is up
  Run as demand circuit
  Transit area 0.0.0.1, via interface GigabitEthernet 13/16, Cost of using 2
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 18, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02
```

Table 38-14. Command Example Descriptions: show ip ospf process-id virtual-links

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Virtual Link...”</td>
<td>This line specifies the OSPF neighbor to which the virtual link was created</td>
</tr>
<tr>
<td></td>
<td>and the link’s status.</td>
</tr>
<tr>
<td>“Run as...”</td>
<td>This line states the nature of the virtual link.</td>
</tr>
<tr>
<td>“Transmit area...”</td>
<td>This line identifies the area through which the virtual link was created,</td>
</tr>
<tr>
<td></td>
<td>the interface used, and the cost assigned to that link.</td>
</tr>
<tr>
<td>“Transmit Delay...”</td>
<td>This line displays the transmit delay assigned to the link and the State of</td>
</tr>
<tr>
<td></td>
<td>the OSPF neighbor.</td>
</tr>
</tbody>
</table>
**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

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If you are using Multi-Process OSPF, you must enter the Process ID to view information regarding a specific OSPF process. If you do not enter the Process ID, only the first configured process is listed.

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
```

To return to the default, enter `no timers spf`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delay</code></td>
<td>Enter a number as the delay.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>Default: 5 seconds</td>
</tr>
<tr>
<td><code>holdtime</code></td>
<td>Enter a number as the hold time.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>Default: 10 seconds</td>
</tr>
</tbody>
</table>

**Defaults**

delay = 5 seconds; holdtime = 10 seconds

**Command Modes**

ROUTER OSPF

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**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.
OSPFv3 Commands

Open Shortest Path First version 3 (OSPFv3) for IPv6 is supported on the C and E platforms.

Note: The C-Series supports OSPFv3 with Dell Networking OS version 7.8.1.0 and later.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, etc.) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Dell Networking implementation of OSPFv3 is based on IETF RFC 2740. The following commands allow you to configure and enable OSPFv3.

- area authentication
- area encryption
- clear ipv6 ospf process
- debug ipv6 ospf packet
- default-information originate
- graceful-restart grace-period
- graceful-restart mode
- ipv6 ospf area
- ipv6 ospf authentication
- ipv6 ospf cost
- ipv6 ospf dead-interval
- ipv6 ospf encryption
- ipv6 ospf graceful-restart helper-reject
- ipv6 ospf hello-interval
- ipv6 ospf priority
- ipv6 router ospf
- passive-interface
- redistribute
- router-id
- show crypto ipsec policy
- show crypto ipsec sa ipv6
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbor
area authentication

Configure an IPsec authentication policy for OSPFv3 packets in an OSPFv3 area.

Syntax

```
area area-id authentication ipsec spi number {MD5 | SHA1} [key-encryption-type] key
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area area-id</td>
<td>Area for which OSPFv3 traffic is to be authenticated. For area-id, you can enter a number or an IPv6 prefix.</td>
</tr>
<tr>
<td>ipsec spi number</td>
<td>Security Policy index (SPI) value that identifies an IPsec security policy. Range: 256 to 4294967295.</td>
</tr>
<tr>
<td>MD5</td>
<td>SHA1</td>
</tr>
<tr>
<td>key-encryption-type</td>
<td>(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).</td>
</tr>
<tr>
<td>key</td>
<td>Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).</td>
</tr>
</tbody>
</table>

Default

Not configured.

Command Modes

ROUTER OSPFv3

Command History

Version 8.4.2.0 Introduced

Usage Information

Before you enable IPsec authentication on an OSPFv3 area, you must first enable OSPFv3 globally on the router. You must configure the same authentication policy (same SPI and key) on each interface in an OSPFv3 link.

An SPI number must be unique to one IPsec security policy (authentication or encryption) on the router.

If you have enabled IPsec encryption in an OSPFv3 area with the area encryption command, you cannot use the area authentication command in the area at the same time.

The configuration of IPsec authentication on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area authentication policy that has been configured is applied to the interface.

To remove an IPsec authentication policy from an OSPFv3 area, enter the no area area-id authentication spi number command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 ospf authentication</td>
<td>Configure an IPsec authentication policy on an OSPFv3 interface.</td>
</tr>
<tr>
<td>show crypto ipsec policy</td>
<td>Display the configuration of IPsec authentication policies.</td>
</tr>
</tbody>
</table>
area encryption

Configure an IPsec encryption policy for OSPFv3 packets in an OSPFv3 area.

Syntax

```
area area-id encryption ipsec spi number esp encryption-algorithm [key-encryption-type] key
authentication-algorithm [key-encryption-type] key
```

Parameters

- **area area-id**
  - Area for which OSPFv3 traffic is to be encrypted. For `area-id`, you can enter a number or an IPv6 prefix.

- **ipsec spi number**
  - Security Policy index (SPI) value that identifies an IPsec security policy.
  - Range: 256 to 4294967295.

- **esp encryption-algorithm**
  - Encryption algorithm used with ESP.
  - Valid values are: 3DES, DES, AES-CBC, and NULL.
  - For AES-CBC, only the AES-128 and AES-192 ciphers are supported.

- **key-encryption-type**
  - (OPTIONAL) Specifies if the key is encrypted.
  - Valid values: 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  - Text string used in encryption.
  - The required lengths of a non-encrypted or encrypted key are:
    - 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.

- **authentication-algorithm**
  - Specifies the authentication algorithm to use for encryption.
  - Valid values are `MD5` or `SHA1`.

- **key-encryption-type**
  - (OPTIONAL) Specifies if the authentication key is encrypted.
  - Valid values: 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  - Text string used in authentication.
  - For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).
  - For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

- **null**
  - Causes an encryption policy configured for the area to not be inherited on the interface.

Default

Not configured.

Command Modes

- ROUTER OSPFv3

Command History

- Version 8.4.2.0 Introduced

Usage Information

Before you enable IPsec encryption on an OSPFv3 interface, you must first enable OSPFv3 globally on the router. You must configure the same encryption policy (same SPI and keys) on each interface in an OSPFv3 link.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router.

Note that when you configure encryption for an OSPFv3 area with the `area encryption` command, you enable both IPsec encryption and authentication. However, when you enable authentication on an area with the `area authentication` command, you do not enable encryption at the same time.

If you have enabled IPsec authentication in an OSPFv3 area with the `area authentication` command, you cannot use the `area encryption` command in the area at the same time.
The configuration of IPsec encryption on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area encryption policy that has been configured is applied to the interface.

To remove an IPsec encryption policy from an interface, enter the `no area area-id encryption spi number` command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 ospf encryption</td>
<td>Configure an IPsec encryption policy on an OSPFv3 interface.</td>
</tr>
<tr>
<td>show crypto ipsec policy</td>
<td>Display the configuration of IPsec encryption policies.</td>
</tr>
</tbody>
</table>

### clear ipv6 ospf process

Reset an OSPFv3 router process without removing or re-configuring the process.

**Syntax**
```
clear ipv6 ospf process [process-id]
```

**Parameters**
- `process-id` (OPTIONAL) Enter the process identification number.

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
- Version 7.8.1.0 Added support for C-Series
- Version 7.4.1.0 Introduced

### debug ipv6 ospf packet

Display debug information on OSPF IPv6 packets.

**Syntax**
```
download ipv6 ospf packet [interface]
```

To cancel the debug, use the `no debug ipv6 ospf packet [interface]` command.
Parameters

interface  (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a Port Channel interface, enter the keyword port-channel followed by a number:
  C-Series Range: 1-128
  E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For a SONET interface, enter the keyword sonet followed by the 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.
- For a VLAN, enter the keyword vlan followed by a number from 1 to 4094

Command Modes

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example

Figure 38-23. debug ipv6 ospf packet Command Example

```plaintext
FTOS#debug ipv6 ospf packet
OSPFv3 packet related debugging is on for all interfaces
05:21:01 : OSPFv3: Sending, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.254, Area ID:0, Inst:0, on Po 255
05:21:03 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.255, Area ID:0, Chksum:a177, Inst:0, from Vl 100
05:20:25 : OSPFv3: Sending, Ver:3, Type:4(LS Update), Len:580, Router ID:223.255.255.254, Area ID:0, Inst:0, on Vl 1000
FTOS#
```

Table 38-15. debug ip ospf Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3...</td>
<td>Debugging is on for all OSPFv3 packets and all interfaces</td>
</tr>
<tr>
<td>05:21:01</td>
<td>Displays the time stamp.</td>
</tr>
<tr>
<td>Sending Ver:3</td>
<td>Sending OSPF3 version.</td>
</tr>
<tr>
<td>Type:</td>
<td>Displays the type of packet sent:</td>
</tr>
<tr>
<td>• 1 - Hello packet</td>
<td></td>
</tr>
<tr>
<td>• 2 - database description</td>
<td></td>
</tr>
<tr>
<td>• 3 - link state request</td>
<td></td>
</tr>
<tr>
<td>• 4 - link state update</td>
<td></td>
</tr>
<tr>
<td>• 5 - link state acknowledgement</td>
<td></td>
</tr>
<tr>
<td>Length:</td>
<td>Displays the packet length.</td>
</tr>
</tbody>
</table>
default-information originate

Configure Dell Networking OS to generate a default external route into the OSPFv3 routing domain.

**Syntax**

```plaintext
default-information originate [always [metric metric-value] [metric-type type-value]] [route-map map-name]
```

To return to the default, use the `no default-information originate` command.

**Parameters**

- **always**  (OPTIONAL) Enter the keyword `always` to indicate that default route information must always be advertised.
- **metric metric-value**  (OPTIONAL) Enter the keyword `metric` followed by the 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 the OSPFv3 link state type of 1 or 2 for default routes. The values are:
  - 1 = Type 1 external route
  - 2 = Type 2 external route
  - Default: 2
- **route-map map-name**  (OPTIONAL) Enter the keyword `route-map` followed by the name of an established route map.

**Defaults**

Disabled

**Command Modes**

ROUTER OSPFv3

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Related Commands**

- `redistribute`  Redistribute routes from other routing protocols into OSPFv3.

graceful-restart grace-period

Enable OSPFv3 graceful restart globally by setting the grace period (in seconds) that an OSPFv3 router’s neighbors will continue to advertise the router as adjacent during a graceful restart.

**Syntax**

```
graceful-restart grace-period seconds
```

To disable OSPFv3 graceful restart, enter `no graceful-restart grace-period`.
OSPFv3 graceful restart is disabled and functions in a helper-only role.

To enable OSPFv3 graceful restart, you must enter the `ipv6 router ospf` command to enter OSPFv3 configuration mode and then configure a grace period using the `graceful-restart grace-period` command. The grace period is the length of time that OSPFv3 neighbors continue to advertise the restarting router as though it is fully adjacent. When graceful restart is enabled (restarting role), an OSPFv3 restarting expects its OSPFv3 neighbors to help when it restarts by not advertising the broken link.

When you enable the helper-reject role on an interface with the `ipv6 ospf graceful-restart helper-reject` command, you reconfigure OSPFv3 graceful restart to function in a “restarting-only” role. In a “restarting-only” role, OSPFv3 does not participate in the graceful restart of a neighbor.

```plaintext
graceful-restart mode
```

Specify the type of events that trigger an OSPFv3 graceful restart.

**Syntax**
```
graceful-restart mode [planned-only | unplanned-only]
```

To disable the configured graceful-restart mode, enter `no graceful-restart mode`.

**Parameters**

| planned-only  | (OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only. |
| unplanned-only | (OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only. |

**Defaults**

OSPFv3 graceful restart supports both planned and unplanned failures.

**Command Modes**

ROUTER OSPFv3

**Command History**

Version 8.4.2.2 Introduced on E-Series TeraScale.

OSPFv3 graceful restart supports planned-only and/or unplanned-only restarts. The default is support for both planned and unplanned restarts.

- A planned restart occurs when you enter the `redundancy force-failover rpm` command to force the primary RPM to switch to the backup RPM. During a planned restart, OSPF sends out a Type-11 Grace LSA before the system switches over to the backup RPM.
An unplanned restart occurs when an unplanned event causes the active RPM to switch to the backup RPM, such as when an active process crashes, the active RPM is removed, or a power failure happens. During an unplanned restart, OSPF sends out a Grace LSA when the backup RPM comes online.

By default, both planned and unplanned restarts trigger an OSPFv3 graceful restart. Selecting one or the other mode restricts OSPFv3 to the single selected mode.

**ipv6 ospf area**

Enable IPv6 OSPF on an interface.

**Syntax**

```
ipv6 ospf process-id area area-id
```

To disable OSPFv6 routing for an interface, use the `no ipv6 ospf process-id area area-id` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Enter the process identification number.</td>
</tr>
<tr>
<td>area area-id</td>
<td>Specify the OSPF area.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 65535</td>
</tr>
</tbody>
</table>

**Defaults**

No default values or behavior

**Command Modes**

INTERFACE

**Command History**

Version 7.4.1.0 Introduced

**ipv6 ospf authentication**

Configure an IPsec authentication policy for OSPFv3 packets on an IPv6 interface.

**Syntax**

```
ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1} [key-encryption-type] key}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>Causes an authentication policy configured for the area to not be inherited on the interface.</td>
</tr>
<tr>
<td>ipsec spi number</td>
<td>Security Policy index (SPI) value that identifies an IPsec security policy. Range: 256 to 4294967295.</td>
</tr>
<tr>
<td>MD5</td>
<td>Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).</td>
</tr>
<tr>
<td>SHA1</td>
<td>Authentication type: Secure Hash Algorithm 1 (SHA-1).</td>
</tr>
<tr>
<td>key-encryption-type</td>
<td>(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).</td>
</tr>
<tr>
<td>key</td>
<td>Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).</td>
</tr>
</tbody>
</table>

**Default**

Not configured.
Before you enable IPsec authentication on an OSPFv3 interface, you must first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. You must configure the same authentication policy (same SPI and key) on each OSPFv3 interface in a link.

To remove an IPsec authentication policy from an interface, enter the `no ipv6 ospf authentication spi number` command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf authentication null` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area authentication</code></td>
<td>Configure an IPsec authentication policy for an OSPFv3 area.</td>
</tr>
<tr>
<td><code>show crypto ipsec policy</code></td>
<td>Display the configuration of IPsec authentication policies.</td>
</tr>
<tr>
<td><code>show crypto ipsec sa ipv6</code></td>
<td>Display the security associations set up for OSPFv3 interfaces in authentication policies.</td>
</tr>
</tbody>
</table>

### ipv6 ospf encryption

Configure an IPsec encryption policy for OSPFv3 packets on an IPv6 interface.

**Syntax**

```
ipv6 ospf encryption {null | ipsec spi number esp encryption-algorithm [key-encryption-type] key} authentication-algorithm [key-encryption-type] key
```

**Parameters**

- **null**: Causes an encryption policy configured for the area to not be inherited on the interface.
- **ipsec spi number**: Security Policy index (SPI) value that identifies an IPsec security policy. Range: 256 to 4294967295.
- **esp encryption-algorithm**: Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.
- **key-encryption-type**: (OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
- **key**: Text string used in encryption. The required lengths of a non-encrypted or encrypted key are: 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and AES-192 ciphers are supported.
- **authentication-algorithm**: Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.
Before you enable IPsec encryption on an OSPFv3 interface, you must first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. You must configure the same encryption policy (same SPI and keys) on each OSPFv3 interface in a link.

To remove an IPsec encryption policy from an interface, enter the `no ipv6 ospf encryption spi number` command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf encryption null` command.

For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).

For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

### Related Commands

- **area encryption** Configure an IPsec encryption policy for an OSPFv3 area.
- **show crypto ipsec policy** Display the configuration of IPsec encryption policies.
- **show crypto ipsec sa ipv6** Display the security associations set up for OSPFv3 interfaces in encryption policies.

### ipv6 ospf cost

Explicitly specify the cost of sending a packet on an interface.

**Syntax**

```
ipv6 ospf cost interface-cost
```

To reset the interface cost to the default value, use the `no ipv6 ospf cost interface-cost` command.

**Parameters**

- `interface-cost` Enter a unsigned integer value expressed as the link-state metric. Range: 1 to 65535

**Defaults**

Default cost based on the bandwidth

**Command Modes**

INTERFACE

**Command History**

- Version 7.8.1.0 Added support for C-Series
- Version 7.4.1.0 Introduced
In general, the path cost is calculated as:

\[ \frac{10^{8}}{\text{bandwidth}} \]

Using this formula, the default path cost are calculated as:

- GigabitEthernet—Default cost is 1
- TenGigabitEthernet—Default cost is 1
- Ethernet—Default cost is 10

**ipv6 ospf dead-interval**

Set the time interval since the last hello-packet was received from a router. After the time interval elapsed, the neighboring routers declare the router down.

**Syntax**

```
ipv6 ospf dead-interval seconds
```

To return to the default time interval, use the `no ipv6 ospf dead-interval` command.

**Parameters**

- `seconds` Enter the time interval in seconds.
  
  Range: 1 to 65535 seconds
  
  Default: 40 seconds (Ethernet)

**Defaults**

As above

**Command Modes**

INTERFACE

**Command History**

- Version 7.8.1.0 Added support for C-Series
- Version 7.4.1.0 Introduced

**Usage Information**

By default, the dead interval is four times longer than the default hello-interval.

**Related Commands**

- `ipv6 ospf hello-interval` Specify the time interval between hello packets

**ipv6 ospf graceful-restart helper-reject**

Configure an OSPFv3 interface to not act upon the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

**Syntax**

```
graceful-restart helper-reject
```

To disable the helper-reject role, enter `no ipv6 ospf graceful-restart helper-reject`.

**Defaults**

The helper-reject role is not configured.

**Command Modes**

INTERFACE

**Command History**

- Version 8.4.2.2 Introduced on E-Series TeraScale.
By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

The `graceful-restart role` command is not supported in OSPFv3. When you enable the helper-reject role on an interface, you reconfigure an OSPFv3 router to function in a “restarting-only” role.

**ipv6 ospf hello-interval**

Specify the time interval between the hello packets sent on the interface.

**Syntax**

```
ipv6 ospf hello-interval seconds
```

To return to the default value, enter `no ipv6 ospf hello-interval`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Enter a time interval in seconds as the time between hello packets. Range: 1 to 65535. Default: 10 seconds (Ethernet)</td>
</tr>
</tbody>
</table>

**Defaults**

As above

**Command Modes**

`INTERFACE`

**Command History**

- **Version 7.8.1.0** Added support for C-Series
- **Version 7.4.1.0** Introduced

**Usage Information**

The time interval between hello packets must be the same for routers in a network.

**Related Commands**

`ipv6 ospf dead-interval` Set the time interval since the last hello-packet was received from a router.

**ipv6 ospf priority**

Set the priority of the interface to determine the Designated Router for the OSPFv3 network.

**Syntax**

```
ipv6 ospf priority number
```

To return to the default value, use the `no ipv6 ospf priority` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter a number as the priority. Range: 0 to 255. Default: 1</td>
</tr>
</tbody>
</table>

**Defaults**

1

**Command Modes**

`INTERFACE`
Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

**ipv6 router ospf**

Enable OSPF for IPv6 router configuration.

**Syntax**

```
ipv6 router ospf process-id
```

To exit OSPF for IPv6, enter `no ipv6 router ospf process-id`

**Parameters**

- `process-id` Enter the process identification number.
  
  Range: 1 to 65535

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.8.1.0 Added support for C-Series
- Version 7.4.1.0 Introduced

**passive-interface**

Disable (suppress) sending routing updates on an interface.

**Syntax**

```
passive-interface interface
```

To enable sending routing updates on an interface, use the `no passive-interface interface` command.

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    
    - **C-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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

Enabled, that is sending of routing updates are enabled by default

Command Modes

ROUTER OSPFv3

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

By default, no interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.

redistribute

Redistribute into OSPFv3.

Syntax

redistribute {bgp as number} {connected | static} [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp as number</td>
<td>Enter the keyword bgp followed by the autonomous system number. Range: 1 to 65535</td>
</tr>
<tr>
<td>connected</td>
<td>Enter the keyword connected to redistribute routes from physically connected interfaces.</td>
</tr>
<tr>
<td>static</td>
<td>Enter the keyword static redistribute manually configured routes.</td>
</tr>
<tr>
<td>metric metric-value</td>
<td>Enter the keyword metric followed by the metric value. Range: 0 to 16777214 Default: 20</td>
</tr>
<tr>
<td>metric-type type-value</td>
<td>(OPTIONAL) Enter the keyword metric-type followed by the OSPFv3 link state type of 1 or 2 for default routes. The values are: 1 = Type 1 external route 2 = Type 2 external route Default: 2</td>
</tr>
<tr>
<td>route-map map-name</td>
<td>(OPTIONAL) Enter the keyword route-map followed by the name of an established route map. If the route map is not configured, the default is deny (to drop all routes).</td>
</tr>
<tr>
<td>tag tag-value</td>
<td>(OPTIONAL) Enter the keyword tag to set the tag for routes redistributed into OSPFv3. Range: 0 to 4294967295 Default: 0</td>
</tr>
</tbody>
</table>

Default

Not configured.
### router-id

**Syntax**
```
router-id ip-address
```

To return to the previous router ID, use the `no router-id ip-address` command.

**Parameters**
- `ip-address`: Enter the router ID in the dotted decimal format.

**Defaults**
The router ID is selected automatically from the set of IPv4 addresses configured on a router.

**Command Modes**
- ROUTER OSPF

**History**
- Version 7.4.1.0 Introduced
- Version 7.8.1.0 Added support for C-Series

**Usage Information**
You can configure an arbitrary value in the IP address for each router. However, each router ID must be unique.

If this command is used on an OSPFv3 process that is already active (has neighbors), all the neighbor adjacencies are brought down immediately and new sessions are initiated with the new router ID.

**Related Commands**
- `clear ipv6 ospf process`: Reset an OSPFv3 router process.
The `show crypto ipsec policy` command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.

**Version 8.4.2.0** Introduced

**Usage Information**

The `show crypto ipsec policy` command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.

**Related Commands**

- `show crypto ipsec sa ipv6` Display the IPsec security associations used on OSPFv3 interfaces.

**Example**

Figure 38-24.  show crypto ipsec policy Command

```
FTOS#show crypto ipsec policy

Crypto IPSec client security policy data
Policy name : OSPFv3-1-502
Policy refcount : 1
Inbound ESP SPI : 502 (0x1F6)
Outbound ESP SPI : 502 (0x1F6)
Inbound ESP Auth Key : 123456789a123456789b123456789c12
Outbound ESP Auth Key : 123456789a123456789b123456789c12
Inbound ESP Cipher Key : 123456789a123456789b123456789c123456789d123456789e
Outbound ESP Cipher Key : 123456789a123456789b123456789c123456789d123456789e
Transform set : esp-3des esp-md5-hmac

Crypto IPSec client security policy data
Policy name : OSPFv3-1-500
Policy refcount : 2
Inbound AH SPI : 500 (0x1F4)
Outbound AH SPI : 500 (0x1F4)
Inbound AH Key : bbdd96e6eb482e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e9f7e
Outbound AH Key : bbdd96e6eb482e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e9f7e
Transform set : ah-md5-hmac

Crypto IPSec client security policy data
Policy name : OSPFv3-0-501
Policy refcount : 1
Inbound ESP SPI : 501 (0x1F5)
Outbound ESP SPI : 501 (0x1F5)
Inbound ESP Auth Key : bbdd96e6eb482e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e9f7e
Outbound ESP Auth Key : bbdd96e6eb482e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e9f7e
Inbound ESP Cipher Key : bbdd96e6eb482e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e9f7e
Outbound ESP Cipher Key : bbdd96e6eb482e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e9f7e
Transform set : esp-128-aes esp-sha1-hmac
```

**Table 38-16.  show crypto ipsec policy Command Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Displays the name of an IPsec policy.</td>
</tr>
<tr>
<td>Policy refcount</td>
<td>Number of interfaces on the router that use the policy.</td>
</tr>
<tr>
<td>Inbound ESP SPI</td>
<td>The encapsulating security payload (ESP) security policy index (SPI) for inbound and outbound links.</td>
</tr>
<tr>
<td>Outbound ESP SPI</td>
<td></td>
</tr>
<tr>
<td>Inbound ESP Auth Key</td>
<td>The ESP authentication key for inbound and outbound links.</td>
</tr>
<tr>
<td>Outbound ESP Auth Key</td>
<td></td>
</tr>
</tbody>
</table>
show crypto ipsec sa ipv6

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.

**Syntax**
```
show crypto ipsec sa ipv6 [interface interface]
```

**Parameters**
- `interface interface` (OPTIONAL) Displays information about the SAs used on a specified OSPFv3 interface, where `interface` is one of the following values:
  - For a 1-Gigabit Ethernet interface, enter `GigabitEthernet slot/port`.
  - For a Port Channel interface, enter `port-channel number`. Valid port-channel numbers (on an E-Series TeraScale): 1 to 255.
  - For a 10-Gigabit Ethernet interface, enter `TenGigabitEthernet slot/port`.
  - For a VLAN interface, enter `vlan vlan-id`. Valid VLAN IDs: 1 to 4094.

**Defaults**
No default behavior or values

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**
- Version 8.4.2.0 Introduced

**Usage Information**
The `show crypto ipsec sa ipv6` command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.

**Related Commands**
- `show crypto ipsec policy` — Display the configuration of IPsec authentication and encryption policies.
Example

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>IPv6 interface</td>
</tr>
<tr>
<td>Link local address</td>
<td>IPv6 address of interface</td>
</tr>
<tr>
<td>IPSecv6 policy name</td>
<td>Name of the IPSec security policy applied to the interface.</td>
</tr>
<tr>
<td>inbound/outbound ah</td>
<td>Authentication policy applied to inbound or outbound traffic.</td>
</tr>
<tr>
<td>inbound/outbound esp</td>
<td>Encryption policy applied to inbound or outbound traffic.</td>
</tr>
<tr>
<td>spi</td>
<td>Security policy index number used to identify the policy.</td>
</tr>
<tr>
<td>transform</td>
<td>Security algorithm that is used to provide authentication, integrity, and confidentiality.</td>
</tr>
<tr>
<td>in use settings</td>
<td>Transform that the SA uses (only transport mode is supported).</td>
</tr>
<tr>
<td>replay detection support</td>
<td>Y: An SA has enabled the replay detection feature. N: The replay detection feature is not enabled.</td>
</tr>
<tr>
<td>STATUS</td>
<td>ACTIVE: The authentication or encryption policy is enabled on the interface.</td>
</tr>
</tbody>
</table>
show ipv6 ospf database

Display information in the OSPFv3 database, including link-state advertisements (LSAs).

**Syntax**

```
show ipv6 ospf database [database-summary | grace-lsa]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>database-summary</td>
<td>(OPTIONAL) Enter the keywords <code>database-summary</code> to view a summary of database LSA information.</td>
</tr>
<tr>
<td>grace-lsa</td>
<td>(OPTIONAL) E-Series TeraScale only: Enter the keywords <code>grace-lsa</code> to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.2</td>
<td>Added support for the display of graceful restart parameters and Type-11 Grace LSAs on E-Series TeraScale routers.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

**Figure 38-26. show ipv6 ospf database grace-lsa Command**

```
FTOS#show ipv6 ospf database grace-lsa
Type-11 Grace LSA (Area 0)
   LS Age              : 10
   Link State ID       : 6.16.192.66
   Advertising Router  : 100.1.1.1
   LS Seq Number       : 0x80000001
   Checksum            : 0x1DF1
   Length               : 36
   Associated Interface: Gi 5/3
   Restart Interval     : 180
   Restart Reason       : Switch to Redundant Processor
```
Example

**Figure 38-27. show ipv6 ospf database database-summary Command**

```
FTOS#show ipv6 ospf database database-summary

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Process 1 database summary
Type Count/Status
Oper Status 1
Admin Status 1
Area Bdr Rtr Status 1
AS Bdr Rtr Status 1
AS Scope LSA Count 0
AS Scope LSA Cksum sum 0
Origin New LSAS 50
Rx New LSAS 22
Ext LSA Count 0
Rte Max Eq Cost Paths 10
GR grace-period 180
GR mode planned and unplanned

Area 0 database summary
Type Count/Status
Brd Rtr Count 1
AS Bdr Rtr Count 1
LSA count 6
Rtr LSA Count 2
Net LSA Count 1
Inter Area Pfx LSA Count 1
Inter Area Rtr LSA Count 0
Group Mem LSA Count 0
Type-7 LSA count 0
Intra Area Pfx LSA Count 2
Intra Area TE LSA Count 2

Area 1 database summary
Type Count/Status
Brd Rtr Count 1
AS Bdr Rtr Count 1
LSA count 8
Rtr LSA Count 1
Net LSA Count 0
Inter Area Pfx LSA Count 5
Inter Area Rtr LSA Count 0
Group Mem LSA Count 0
Type-7 LSA count 0
Intra Area Pfx LSA Count 2
Intra Area TE LSA Count 2

E1200-T2C2#sh ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
63.114.8.36 1 FULL/DR 00:00:37 4 Gi 9/0
```

*show ipv6 ospf interface*

View OSPFv3 interface information.

**Syntax**

`show ipv6 ospf [interface]`
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **interface** | (OPTIONAL) Enter one of the following keywords and slot/port or number information:  
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.  
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:  
    - C-Series Range: 1-128  
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.  
  - For a SONET interface, enter the keyword `sonet` followed by the 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.  
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094 |

### Defaults

No default behavior or values

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code></td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### Example

**Figure 38-28. show ipv6 ospf interface command**

```
FTOS#show ipv6 ospf interface gigabitethernet 1/0
GigabitEthernet 1/0 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5
FTOS#
```

### Syntax

```
show ipv6 ospf neighbor
```

**Display the OSPF neighbor information on a per-interface basis.**

**Syntax**

```
show ipv6 ospf neighbor [interface]
```
Parameters

```
interface (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a Port Channel interface, enter the keyword port-channel followed by a number:
  C-Series Range: 1-128
  E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- 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 the VLAN ID. The range is from 1 to 4094.
```

Defaults
No default behavior or values

Command Modes
EXEC

EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added</td>
<td>support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added</td>
<td>support for C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
<td></td>
</tr>
</tbody>
</table>

Example

`Figure 38-29.  show ipv6 ospf neighbor Command Example`

```
FTOS#show ipv6 ospf neighbor gi 9/0
Neighbor ID      Pri State   Dead Time Interface ID Interface
63.114.8.36     1   FULL/DR 00:00:38 4       Gi 9/0
FTOS#
```
Policy-based Routing (PBR)

Overview

Policy-based Routing (PBR) enables you to apply routing policies to specific interfaces. To enable PBR, you create a redirect list and then apply it to the interface. Once the redirect list is applied to the interface, all traffic passing through the interface is subject to the rules defined in the redirect list.

PBR is supported by Dell Networking OS on the C-Series, E-Series, and S-Series platforms.

Commands

Policy-based routing includes the following commands:

- `description`
- `ip redirect-group`
- `ip redirect-list`
- `permit`
- `redirect`
- `seq`
- `show cam pbr`
- `show ip redirect-list`

PBR can be applied to physical interfaces and logical interfaces (such as LAG or VLAN). Trace lists and redirect lists do not function correctly when both are configured in the same configuration.

Note: Apply Policy-based Routing to Layer 3 interfaces only.
### description

Add a description to this redirect list.

**Syntax**

description \{description\}

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

**Parameters**

- **description**
  - Enter a description to identify the IP redirect list (80 characters maximum).

**Defaults**

No default behavior or values

**Command Modes**

REDIRECT-LIST

**Command History**

- Version 8.4.2.1 Introduced on the C-Series and S-Series
- Version 8.4.2.0 Introduced on the E-Series TeraScale
- pre-Version 7.7.1.0 Introduced on the E-Series ExaScale

### ip redirect-group

Apply a redirect list (policy-based routing) on an interface. You can apply multiple redirect lists to an interface by entering this command multiple times.

**Syntax**

ip redirect-group redirect-list-name

To remove a redirect list from an interface, use the no ip redirect-group name command.

**Parameters**

- **redirect-list-name**
  - Enter the name of a configured redirect list.

**Defaults**

No default behavior or values

**Command Modes**

INTERFACE (conf-if-vl-)

**Command History**

- Version 8.4.2.1 Introduced on the C-Series and S-Series
- Version 8.4.2.0 Introduced on the E-Series TeraScale
- Version 7.4.2.0 Added support for LAG and VLAN interfaces
- Version 6.5.3.0 Introduced on the E-Series ExaScale

**Usage Information**

Any number of redirect-groups can be applied to an interface. A redirect list can contain any number of configured rules. These rules includes the next-hop IP address where the incoming traffic is to be redirected.
If the next hop address is reachable, traffic is forwarded to the specified next hop. Otherwise the normal routing table is used to forward traffic. When a redirect-group is applied to an interface and the next-hop is reachable, the rules are added into the PBR CAM region. When incoming traffic hits an entry in the CAM, the traffic is redirected to the corresponding next-hop IP address specified in the rule.

**Note:** Apply redirect list to physical, VLAN, or LAG interfaces only.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cam pbr</code></td>
<td>Display the content of the PBR CAM.</td>
</tr>
<tr>
<td><code>show ip redirect-list</code></td>
<td>Display the redirect-list configuration.</td>
</tr>
</tbody>
</table>

**ip redirect-list**

Configure a redirect list and enter the REDIRECT-LIST mode.

**Syntax**

```
ip redirect-list redirect-list-name
```

To remove a redirect list, enter `no ip redirect-list`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redirect-list-name</code></td>
<td>Enter the name of a redirect list.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
<tr>
<td>6.5.3.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
</tbody>
</table>
permit

Configure a rule for the redirect list.

Syntax

```
permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [bit] [operators]
```

To remove the rule, use one of the following:

- If you know the filter sequence number, use the `no seq sequence-number` syntax.
- `no permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [bit] [operators]`

Parameters

- **ip-protocol-number**: Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
- **protocol-type**: Enter one of the following keywords as the protocol type:
  - `icmp` for Internet Control Message Protocol
  - `ip` for Any Internet Protocol
  - `tcp` for Transmission Control Protocol
  - `udp` for User Datagram Protocol
- **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).
- **any**: Enter the keyword `any` to specify that all traffic is 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.
- **bit** (OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags:
  - `ack` = acknowledgement
  - `fin` = finish (no more data from the user)
  - `psh` = push function
  - `rst` = reset the connection
  - `syn` = synchronize sequence number
  - `urg` = urgent field
- **operator** (OPTIONAL) For TCP and UDP parameters only. 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` command parameter.)

Defaults

No default behavior or values

Command Modes

REDIRECT-LIST

Command History

- Version 8.4.2.1 Introduced on the C-Series and S-Series
- Version 8.4.2.0 Introduced on the E-Series TeraScale
- Version 7.5.1.0 Introduced on the E-Series ExaScale
Configure a rule for the redirect list.

**Syntax**
```
redirect {ip-address | sonet slot/port} {ip-protocol-number | protocol-type [bit]} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator]
```

To remove this filter, use one of the following:
- Use the **no seq sequence-number** command syntax if you know the filter’s sequence number.
- Use the **no redirect {ip-address | sonet slot/port} {ip-protocol-number [bit] | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator]**

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the forwarding router.</td>
</tr>
<tr>
<td>sonet slot/port</td>
<td>Enter the keyword sonet followed by the slot/port information.</td>
</tr>
<tr>
<td>ip-protocol-number</td>
<td>Enter a number from 0 to 255 for the protocol identified in the IP protocol header.</td>
</tr>
<tr>
<td>protocol-type</td>
<td>Enter one of the following keywords as the protocol type:</td>
</tr>
<tr>
<td>bit</td>
<td>(OPTIONAL) For TCP protocol type only. Enter one or a combination of the following TCP flags:</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).</td>
</tr>
<tr>
<td>any</td>
<td>Enter the keyword any to specify that all traffic is 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>operator</td>
<td>(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand:</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

REDIRECT-LIST
**seq**

Configure a filter with an assigned sequence number for the redirect list.

**Syntax**

```
seq sequence-number (permit | redirect {ip-address | sonet slot/port}) {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operator]
```

To delete a filter, use the **no seq sequence-number** command.

**Parameters**

- `sequence-number`: Enter a number from 1 to 65535.
- `permit`: Enter the keyword `permit` to assign the sequence to the permit list.
- `redirect`: Enter the keyword `redirect` to assign the sequence to the redirect list.
- `ip-address`: Enter the IP address of the forwarding router.
- `sonet slot/port`: Enter the keyword `sonet` followed by the slot/port information.
- `ip-protocol-number`: Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
- `protocol-type`: Enter one of the following keywords as the protocol type:
  - `icmp` for Internet Control Message Protocol
  - `ip` for Any Internet Protocol
  - `tcp` for Transmission Control Protocol
  - `udp` for User Datagram Protocol
- `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).
- `any`: Enter the keyword `any` to specify that all traffic is 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.
### bit

(Optional) For TCP protocol type only, enter one or a combination of the following TCP flags:

- `ack` = acknowledgement
- `fin` = finish (no more data from the user)
- `psh` = push function
- `rst` = reset the connection
- `syn` = synchronize sequence number
- `urg` = urgent field

### operator

(Optional) For TCP and UDP parameters only. 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` command parameter.)

---

**Defaults**

No default behavior or values

**Command Modes**

REDIRECT-LIST

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added the bit variable and Permit and Redirect</td>
</tr>
<tr>
<td>6.5.3.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
</tbody>
</table>
**show cam pbr**

Display the PBR CAM content.

**Syntax**

```
show cam pbr { [interface interface] | linecard slot-number port-set number } [ summary ]
```

**Parameters**

- **interface interface**
  - Enter the keyword `interface` followed by the name of the interface. Enter the following keywords and slot/port or number information:
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet followed by the slot/port information.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
      - **C-Series** Range: 1-128
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - 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 the VLAN ID. The VLAN ID range is from 1 to 4094.

- **linecard slot-number**
  - Enter the keyword `linecard` followed the slot number. Range: 0 to 13 for the E1200, 0 to 6 for the E600/E600i, 0 to 5 for the E300

- **port-set number**
  - Enter the keyword `port-set` followed the port-pipe number. Range: 0 to 1

- **summary**
  - Enter the keyword `summary` to view only the total number of CAM entries.

**Defaults**

No default values or behavior

**Command Modes**

EXEC

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 7.4.1.0** Introduced

**Example**

**Figure 39-1. Command example: show cam pbr linecard 2 port-set 0**

```
FTOS#show cam pbr linecard 2 p 0
TCP Flag: Bit 5 - URG, Bit 4 - ACK, Bit 3 - PSH, Bit 2 - RST, Bit 1 - SYN, Bit 0 - FIN
Cam Port VlanID Proto Tcp   Src   Dst   SrcIp              DstIp              Next-hop          Egress Port
Index Flag  Port  Port                                        MAC               Port
------------------------------------------------------------------------------------------------------
15230 0x10 0 0 100.55.1.0/24 182.16.1.1/24 N/A N/A
FTOS#
```

**Usage Information**

The `show cam pbr` command displays the PBR CAM content. The “VlanID” column displays the corresponding VLAN ID to which the redirect-group is applied.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip redirect-group</code></td>
<td>Apply a redirect group to an interface.</td>
</tr>
<tr>
<td><code>show ip redirect-list</code></td>
<td>Display the redirect-list configuration.</td>
</tr>
<tr>
<td><code>show cam-usage</code></td>
<td>Display the CAM usage on ACL, router, or switch.</td>
</tr>
</tbody>
</table>
show ip redirect-list

View the redirect list configuration and the interfaces it is applied to.

Syntax

```
show ip redirect-list redirect-list-name
```

Parameters

- `redirect-list-name`: Enter the name of a configured Redirect list.

Command Modes

- EXEC
- EXEC Privilege

Example

```
Figure 39-2. show ip redirect-list Command Example

FTOS#show ip redirect-list test_sonet

IP redirect-list rcl0:
  Defined as:
    seq 5 permit ip any host 182.16.2.10
    seq 10 redirect 182.16.1.2 ip any any, Next-hop un-reachable, ARP un-resolved
  Applied interfaces:
    Gi 9/0
    So 8/2
    Vl 10
    Po 3

FTOS#
```
PIM-Dense Mode (PIM-DM)

Overview

PIM-DM is supported on E-Series ExaScale E in Dell Networking OS 8.1.1.0. and later.

PIM-DM is supported on E-Series TeraScale E, C-Series C, and S-Series S platforms in Dell Networking OS 8.4.2.0. and later.

For information on the commands required to configure and use PIM-Dense Mode (PIM-DM), refer to:

- IPv4 PIM Commands on page 1141
- IPv4 PIM-Dense Mode Commands

IPv4 PIM-Dense Mode Commands

The IPv4 PIM-Dense Mode (PIM-DM) commands are:

- ip pim dense-mode
**ip pim dense-mode**

Enable PIM Dense-Mode (PIM-DM) Multicast capability for the specified interface.

**Syntax**

```
ip pim dense-mode
```

To disable PIM-DM, use the **no ip pim dense-mode** command.

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series TeraScale</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

*Figure 40-1. ip pim dense-mode Command Example*

```
FTOS#conf
FTOS(conf)# interface gigabitethernet 3/27
FTOS(gigabitethernet 3/27)# ip address 10.1.1.1 /24
FTOS(gigabitethernet 3/27)# no shut
FTOS(gigabitethernet 3/27)# ip pim dense-mode
FTOS#
```

**Usage Information**

Currently, the chassis operates in either PIM Dense-Mode or PIM Sparse-Mode. The mode configuration for the first PIM enabled interface determines the mode for the entire chassis. Subsequent configurations, on other interfaces, to enable PIM is only accepted if the mode is the same as the original configuration mode. The chassis PIM mode can be changed if PIM-configuration from all interfaces are removed prior to applying a new PIM mode configuration.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip pim sparse-mode</td>
<td>Configure sparse-mode</td>
</tr>
<tr>
<td>show ip pim tib</td>
<td>Display PIM tree information.</td>
</tr>
</tbody>
</table>
PIM-Sparse Mode (PIM-SM)

Overview

The platforms on which a command is supported is indicated by the character — E for the E-Series, C for the C-Series, and S for the S-Series — that appears below each command heading.

PIM is supported on E-Series ExaScale E with Dell Networking OS 8.1.1.0. and later.

This chapter contains the following sections:

- IPv4 PIM-Sparse Mode Commands
- IPv6 PIM-Sparse Mode Commands

IPv4 PIM-Sparse Mode Commands

The IPv4 PIM-Sparse Mode (PIM-SM) commands are:

- clear ip pim rp-mapping
- clear ip pim tib
- clear ip pim snooping tib
- debug ip pim
- ip pim bsr-border
- ip pim bsr-candidate
- ip pim dr-priority
- ip pim graceful-restart
- ip pim join-filter
- ip pim ingress-interface-map
- ip pim neighbor-filter
- ip pim query-interval
- ip pim register-filter
- ip pim rp-address
- ip pim rp-candidate
- ip pim snooping
- ip pim sparse-mode
- ip pim sparse-mode sg-expiry-timer
- ip pim spt-threshold
- no ip pim snooping dr-flood
- show ip pim bsr-router
### clear ip pim rp-mapping

**Syntax**
```
clear ip pim rp-mapping rp-address
```

**Parameters**
- `rp-address` (OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D)

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.8.1.0 Introduced on S-Series

### clear ip pim tib

**Syntax**
```
clear ip pim tib [group]
```

**Parameters**
- `group` (OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D)

**Command Modes**
EXEC Privilege

**Command History**
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.8.1.0 Introduced on S-Series
clear ip pim snooping tib

Clear tree information discovered by PIM-SM snooping from the PIM database.

Syntax

```
clear ip pim snooping tib [vlan vlan-id] [group-address]
```

Parameters

- **vlan vlan-id** (OPTIONAL) Enter a VLAN ID to clear TIB information learned through PIM-SM snooping about a specified VLAN. Valid VLAN IDs: 1 to 4094.
- **group-address** (OPTIONAL) Enter a multicast group address in dotted decimal format (A.B.C.D) to clear TIB information learned through PIM-SM snooping about a specified multicast group.

Command Modes

EXEC Privilege

Command History

Version 8.4.1.1 Introduced on E-Series ExaScale

Related Commands

- **show ip pim snooping tib** Display TIB information learned through PIM-SM snooping.

---

debug ip pim

View IP PIM debugging messages.

Syntax

```
debug ip pim [bsr | events | group | packet [in | out] | register | state | timer [assert | hello | joinprune | register]]
```

To disable PIM debugging, enter **no debug ip pim**, or enter **undebug all** to disable all debugging.

Parameters

- **bsr** (OPTIONAL) Enter the keyword **bsr** to view PIM Candidate RP/BSR activities.
- **events** (OPTIONAL) Enter the keyword **events** to view PIM events.
- **group** (OPTIONAL) Enter the keyword **group** to view PIM messages for a specific group.
- **packet [in | out]** (OPTIONAL) Enter the keyword **packet** to view PIM packets. Enter one of the optional parameters:
  - in: to view incoming packets
  - out: to view outgoing packets.
- **register** (OPTIONAL) Enter the keyword **register** to view PIM register address in dotted decimal format (A.B.C.D).
- **state** (OPTIONAL) Enter the keyword **state** to view PIM state changes.
- **timer [assert | hello | joinprune | register]** (OPTIONAL) Enter the keyword **timer** to view PIM timers. Enter one of the optional parameters:
  - assert: to view the assertion timer.
  - hello: to view the PIM neighbor keepalive timer.
  - joinprune: to view the expiry timer (join/prune timer)
  - register: to view the register suppression timer.

Defaults

Disabled

Command Modes

EXEC Privilege
**ip pim bsr-border**

Configure the PIM router to join the Bootstrap election process.

**Syntax**

```
ip pim bsr-border
```

To return to the default value, enter `no ip pim bsr-border`.

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Usage Information**

This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time out. Candidate RP advertisements can be cleaned using the `clear ip pim rp-mapping` command.

**ip pim bsr-candidate**

Configure the PIM router to join the Bootstrap election process.

**Syntax**

```
ip pim bsr-candidate interface [hash-mask-length] [priority]
```

To return to the default value, enter `no ip pim bsr-candidate`.

**Parameters**

- `interface`
  Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - 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:
    - **C-Series** and **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `fortyGigE` 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 pim dr-priority

**Syntax:**
```
ip pim dr-priority priority-value
```

**Parameters:**
- `priority-value`: Enter a number. Preference is given to larger/higher number.
  - Range: 0 to 4294967294
  - Default: 0

**Defaults:**
1

**Command Modes:**
- INTERFACE

**Usage Information:**
The router with the largest value assigned to an interface becomes the Designated Router. If two interfaces contain the same DR priority value, the interface with the largest interface IP address becomes the Designated Router.

### ip pim graceful-restart

This feature permits configuration of Non-stop Forwarding (NFS or graceful restart) capability of a PIM router to its neighbors.

**Syntax:**
```
[ipv6] ip pim graceful-restart [helper-only | nsf [restart-time | stale-entry-time]]
```

**Parameters:**
- `ipv6`: Enter this keyword to enable graceful-restart for IPv6 Multicast Routes.
- `helper-only`: Enter the keyword `helper-only` to configure as a receiver (helper) only by preserving the PIM status of a graceful restart PIM neighboring router.
nsf

Enter the keyword **nsf** to configure the **Non-stop Forwarding** capability.

<table>
<thead>
<tr>
<th>restart-time</th>
<th>(OPTIONAL) Enter the keyword <strong>restart-time</strong> followed by the number of seconds estimated for the PIM speaker to restart. Range: 30 to 300 seconds Default: 180 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>stale-entry-time</td>
<td>(OPTIONAL) Enter the keyword <strong>stale-entry-time</strong> followed by the number of seconds for which entries are kept alive after restart. Range: 30 to 300 seconds Default: 60 seconds</td>
</tr>
</tbody>
</table>

**Defaults**
as above

**Command Modes**
CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale. Added the ipv6 option for E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

When an NSF-capable router comes up, it announces the graceful restart capability and restart duration as a Hello option. The receiving router notes the Hello option. Routers not NSF capable will discard the unknown Hello option and adjacency is not affected.

When an NSF-capable router goes down, neighboring PIM speaker preserves the states and continues the forwarding of multicast traffic while the neighbor router restarts.

**ip pim join-filter**

Permit or deny PIM Join/Prune messages on an interface using an extended IP access list. This command prevents the PIM SM router from creating state based on multicast source and/or group.

**Syntax**

```
ip pim join-filter ext-access-list {in | out}
```

Remove the access list using the command **no ip pim join-filter ext-access-list {in | out}**

**Parameters**

- **ext-access-list** Enter the name of an extended access list.
- **in** Enter this keyword to apply the access list to inbound traffic.
- **out** Enter this keyword to apply the access list to outbound traffic.

**Defaults**
None

**Command Modes**
INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series on port-channels and S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>
**Example**

**Figure 41-1.  ip pim join-filter Command Example**

FTOS(conf)# ip access-list extended iptv-channels
FTOS(config-ext-nacl)# permit ip 10.1.2.3/24 225.1.1.0/24
FTOS(config-ext-nacl)# permit ip any 232.1.1.0/24
FTOS(config-ext-nacl)# permit ip 100.1.1.0/16 any
FTOS(config-if-gi-1/1)# ip pim join-filter iptv-channels in
FTOS(config-if-gi-1/1)# ip pim join-filter iptv-channels out

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list extended</td>
<td>Configure an access list based on IP addresses or protocols.</td>
</tr>
</tbody>
</table>

**ip pim ingress-interface-map**

When the Dell Networking system is the RP, statically map potential incoming interfaces to (*,G) entries to create a lossless multicast forwarding environment.

**Syntax**

```
ip pim ingress-interface-map std-access-list
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>std-access-list</td>
<td>Enter the name of an standard access list that permits the</td>
</tr>
</tbody>
</table>

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

Version 8.4.1.0 Introduced

**Example**

FTOS(conf)# ip access-list extended iptv-channels
FTOS(config-ext-nacl)# permit 224.0.0.1/24
FTOS(config-ext-nacl)# exit
FTOS(config-if-gi-1/1)# ip pim ingress-interface-map map1

**ip pim neighbor-filter**

Configure this feature to prevent a router from participating in protocol independent Multicast (PIM).

**Syntax**

```
ip pim neighbor-filter {access-list}
```

To remove the restriction, use the no ip pim neighbor-filter {access-list} command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>Enter the name of a standard access list. Maximum 16 characters.</td>
</tr>
</tbody>
</table>

**Defaults**

Defaults.

**Command Modes**

CONFIGURATION.

**Command History**

Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.8.1.0 Introduced on C-Series and S-Series
Version 7.6.1.0 Introduced on the E-Series
**ip pim query-interval**

Change the frequency of PIM Router-Query messages.

**Syntax**

```
ip pim query-interval seconds
```

To return to the default value, enter `no ip pim query-interval seconds` command.

**Parameters**

- `seconds` Enter a number as the number of seconds between router query messages.
  - Default: 30 seconds
  - Range: 0 to 65535

**Defaults**

30 seconds

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version 8.1.1.0</th>
<th>Introduced on E-Series ExaScale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on C-Series on port-channels and S-Series</td>
</tr>
</tbody>
</table>

**ip pim register-filter**

Use this feature to prevent a PIM source DR from sending register packets to an RP for the specified multicast source and group.

**Syntax**

```
ip pim register-filter access-list
```

To return to the default, use the `no ip pim register-filter access-list` command.

**Parameters**

- `access-list` Enter the name of an extended access list. Maximum 16 characters.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version 7.8.1.0</th>
<th>Introduced on C-Series and S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

The access name is an extended IP access list that denies PIM register packets to RP at the source DR based on the multicast and group addresses. Do not enter this command before creating the access-list.
ip pim rp-address

Configure a static PIM Rendezvous Point (RP) address for a group or access-list.

Syntax

```
ip pim rp-address address {group-address group-address mask} override
```

To remove an RP address, use the `no ip pim rp-address address {group-address group-address mask} override` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Enter the RP address in dotted decimal format (A.B.C.D).</td>
</tr>
<tr>
<td>group-address</td>
<td>Enter the keyword <code>group-address</code> followed by a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.</td>
</tr>
<tr>
<td>group-address mask</td>
<td></td>
</tr>
<tr>
<td>override</td>
<td>Enter the keyword <code>override</code> to override the BSR updates with static RP. The override will take effect immediately during enable/disable. Note: This option is applicable to multicast group range.</td>
</tr>
</tbody>
</table>

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

- **Version 8.1.1.0**
  - Introduced on E-Series ExaScale
- **Version 7.8.1.0**
  - Introduced on S-Series
- **pre-Version 6.1.1.1**
  - Introduced on E-Series

Usage Information

This address is used by first-hop routers to send Register packets on behalf of source multicast hosts. The RP addresses are stored in the order in which they are entered. RP addresses learned via BSR take priority over static RP addresses. Without the override option, RPs advertised by the BSR updates take precedence over the statically configured RPs.
**ip pim rp-candidate**

Configure a PIM router to send out a Candidate-RP-Advertisement message to the Bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR.

**Syntax**

```
ip pim rp-candidate {interface [priority]}
```

To return to the default value, enter `no ip pim rp-candidate {interface [priority]}` command.

**Parameters**

- `interface` Enter the following keywords and slot/port or number information:
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 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:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
- `priority` (OPTIONAL) Enter the priority used in Bootstrap election process.
  Range: zero (0) to 255
  Default: 192

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.
ip pim snooping

Enable PIM-SM snooping globally on a switch or on a VLAN interface.

Syntax

```
ip pim snooping [enable]
```

To disable PIM-SM snooping enter the `no` form of the command.

Defaults

Disabled.

Command Modes

- **CONFIGURATION**: To configure PIM-SM snooping globally, enter the `ip pim snooping enable` command in global configuration mode.
- **VLAN INTERFACE**: To configure PIM-SM snooping on a VLAN interface, enter the `ip pim snooping` command in VLAN interface configuration mode.

Command History

| Version 8.4.1.1 | Introduced on E-Series ExaScale |

Usage Information

Because PIM-SM snooping is used in a Layer 2 environment, PIM-SM snooping and PIM multicast routing are mutually exclusive. PIM-SM snooping cannot be enabled on a switch/router if PIM-SM or PIM-DM is enabled.

If enabled at the global level, PIM-SM snooping is automatically enabled on all VLANs unless the `no ip pim snooping` command has been entered on a VLAN.

If enabled at the VLAN level, PIM-SM snooping requires that you also enter the `no shutdown` command to enable the interface.

PIM-SM snooping is supported with IGMP snooping, and forwards the IGMP report on the port that connects to the PIM DR. It is recommended that you do not enable IGMP snooping on a PIM-SM snooping-enabled VLAN interface unless until it is necessary for VLAN operation.

PIM-SM snooping listens to PIM hello and PIM-SM join and prune messages while maintaining the VLAN- and port-specific information in multicast packets that are snooped.

To display information about the operation of PIM-SM snooping on a switch, enter the `show ip pim summary` command.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip pim snooping tib</code></td>
<td>Display TIB information learned through PIM-SM snooping.</td>
</tr>
</tbody>
</table>
ip pim sparse-mode

Enable PIM sparse mode and IGMP on the interface.

Syntax
ip pim sparse-mode

To disable PIM sparse mode and IGMP, enter no ip pim sparse-mode.

Defaults
Disabled.

Command Modes
INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series on port-channels and S-Series</td>
</tr>
</tbody>
</table>

Usage Information
C-Series supports a maximum of 31 PIM interfaces.

The interface must be enabled (no shutdown command) and not have the switchport command configured. Multicast must also be enabled globally (using the ip multicast-lag-hashing command). PIM is supported on the port-channel interface.

Related Commands

ip multicast-lag-hashing

Enable multicast globally.

ip pim sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources, or for a specific set of (S,G) pairs defined by an access list.

Syntax
ip pim sparse-mode sg-expiry-timer seconds [access-list name]

To disable configured timers and return to default mode, enter no ip pim sparse-mode sg-expiry-timer.

Parameters

- **seconds**
  Enter the number of seconds the S, G entries will be retained.
  Range 211-86400

- **access-list name** (OPTIONAL) Enter the name of a previously configured Extended ACL to enable the expiry time to specified S,G entries

Defaults
Disabled. The default expiry timer (with no times configured) is 210 sec.

Command Modes
CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced</td>
</tr>
<tr>
<td>7.7.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information
This command configures an expiration timer for all S.G entries, unless they are assigned to an Extended ACL.
ip pim spt-threshold

Configure PIM router to switch to shortest path tree when the traffic reaches the specified threshold value.

Syntax

```
ip pim spt-threshold value | infinity
```

To return to the default value, enter `no ip pim spt-threshold`.

Parameters

- **value** (OPTIONAL) Enter the traffic value in kilobits per second. Default: 10 packets per second. A value of zero (0) will cause a switchover on the first packet.
- **infinity** (OPTIONAL) To never switch to the source-tree, enter the keyword `infinity`.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 8.4.1.1 Introduced on E-Series ExaScale

Usage Information

This is applicable to last hop routers on the shared tree towards the Rendezvous Point (RP).

no ip pim snooping dr-flood

Disable the flooding of multicast packets to the PIM designated router.

Syntax

```
o ip pim snooping dr-flood
```

To re-enable the flooding of multicast packets to the PIM designated router, enter the `ip pim snooping dr-flood` command.

Defaults

Enabled.

Command Modes

CONFIGURATION

Command History

- Version 8.4.1.1 Introduced on E-Series ExaScale

Usage Information

By default, when you enable PIM-SM snooping, a switch floods all multicast traffic to the PIM designated router (DR), including unnecessary multicast packets. To minimize the traffic sent over the network to the designated router, you can disable designated-router flooding.

When designated-router flooding is disabled, PIM-SM snooping only forwards the multicast traffic, which belongs to a multicast group for which the switch receives a join request, on the port connected towards the designated router.

If the PIM DR flood is not disabled (default setting):
- Multicast traffic is transmitted on the egress port towards the PIM DR if the port is not the incoming interface.
- Multicast traffic for an unknown group is sent on the port towards the PIM DR. When DR flooding is disabled, multicast traffic for an unknown group is dropped.
**show ip pim bsr-router**

**Syntax**
show ip pim bsr-router

**Command Modes**
EXEC
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

**Example**

Figure 41-2. show ip pim bsr-router Command Example

```
E600-7-rpm0#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  Uptime: 16:59:06, BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:08

This system is a candidate BSR
  Candidate BSR address: 7.7.7.7, priority: 0, hash mask length: 30
```

**show ip pim interface**

**Syntax**
show ip pim interface

**Command Modes**
EXEC
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

**Example**

Figure 41-3. show ip pim interface Command Example

```
E600-7-rpm0#show ip pim interface
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  Uptime: 16:59:06, BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:08

This system is a candidate BSR
  Candidate BSR address: 7.7.7.7, priority: 0, hash mask length: 30
```
show ip pim neighbor

View PIM neighbors.

Syntax
show ip pim neighbor

Command Modes
EXEC
EXEC Privilege

Command History
Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.8.1.0 Introduced on S-Series

Example
Figure 41-4. show ip pim neighbor Command Example

FTOS#show ip pim neighbor
Neighbor Address    Interface      Uptime/Expires Ver DR
127.87.3.4          Gi 7/16        09:44:58/00:01:24 v2 1  / S
FTOS#

Table 41-2. show ip pim neighbor Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor address</td>
<td>Displays the IP address of the PIM neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.</td>
</tr>
<tr>
<td>Uptime/expires</td>
<td>Displays the amount of time the neighbor has been up followed by the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).</td>
</tr>
</tbody>
</table>
**show ip pim rp**

View all multicast groups-to-RP mappings.

**Syntax**

```
show ip pim rp [mapping | group-address]
```

**Parameters**

- **mapping** (OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.

- **group-address** (OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

**Example 1**

```
FTOS#sh ip pim rp
Group            RP
224.2.197.115    165.87.20.4
224.2.217.146    165.87.20.4
224.3.3.3        165.87.20.4
225.1.2.1        165.87.20.4
225.1.2.2        165.87.20.4
229.1.2.1        165.87.20.4
229.1.2.2        165.87.20.4
FTOS#
```

**Example 2**

```
FTOS#sh ip pim rp mapping
Group(s): 224.0.0.0/4
          RP: 165.87.20.4, v2
          Info source: 165.87.20.5, via bootstrap, priority 0
          Uptime: 00:03:11, expires: 00:02:46
          RP: 165.87.20.3, v2
          Info source: 165.87.20.5, via bootstrap, priority 0
          Uptime: 00:03:11, expires: 00:03:03
FTOS#
```
show ip pim snooping interface

Display information on VLAN interfaces with PIM-SM snooping enabled.

**Syntax**

```
show ip pim snooping interface [vlan vlan-id]
```

**Parameters**

- `vlan vlan-id` (OPTIONAL) Enter a VLAN ID to display information about a specified VLAN configured for PIM-SM snooping. Valid VLAN IDs: 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.4.1.1 Introduced on E-Series ExaScale

**Example**

**Figure 41-8. show ip pim snooping interface Command Example**

```
FTOS#show ip pim snooping interface
Interface   Ver   Nbr Count   DR Prio       DR
Vlan 2      v2    3      1       165.87.32.2
```

**Table 41-3. show ip pim snooping interface Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the VLAN interfaces with PIM-SM snooping enabled.</td>
</tr>
<tr>
<td>Ver/Mode</td>
<td>Displays the PIM version number for each VLAN interface with PIM-SM snooping enabled:</td>
</tr>
<tr>
<td></td>
<td>• v2 = PIM version 2</td>
</tr>
<tr>
<td></td>
<td>• S = PIM Sparse mode</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Displays the number of neighbors learned through PIM-SM snooping on the interface.</td>
</tr>
<tr>
<td>DR Prio</td>
<td>Displays the Designated Router priority value configured on the interface (ip pim dr-priority command).</td>
</tr>
<tr>
<td>DR</td>
<td>Displays the IP address of the Designated Router for that interface.</td>
</tr>
</tbody>
</table>
show ip pim snooping neighbor

Display information on PIM neighbors learned through PIM-SM snooping.

Syntax

```
show ip pim snooping neighbor [vlan vlan-id]
```

Parameters

- `vlan vlan-id` (OPTIONAL) Enter a VLAN ID to display information about PIM neighbors that was discovered by PIM-SM snooping on a specified VLAN. Valid VLAN IDs: 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.1.1 Introduced on E-Series ExaScale

Example

```
Figure 41-9. show ip pim snooping neighbor Command Example

FTOS#show ip pim snooping neighbor
Neighbor Address          Interface           Uptime/Expires     Ver DR Prio
165.87.32.2              Vl 2 [Gi 4/13 ]      00:04:03/00:01:42  v2  1
165.87.32.10             Vl 2 [Gi 4/11 ]      00:00:46/00:01:29  v2  0
165.87.32.12             Vl 2 [Gi 4/20 ]      00:00:51/00:01:24  v2  0
```

Table 41-4. show ip pim snooping neighbor Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor address</td>
<td>Displays the IP address of the neighbor learned through PIM-SM snooping.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.</td>
</tr>
<tr>
<td>Uptime/expires</td>
<td>Displays the amount of time the neighbor has been up followed by the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).</td>
</tr>
<tr>
<td>Ver</td>
<td>Displays the PIM version number.</td>
</tr>
<tr>
<td></td>
<td>• v2 = PIM version 2</td>
</tr>
<tr>
<td>DR prio/Mode</td>
<td>Displays the Designated Router priority and the mode.</td>
</tr>
<tr>
<td></td>
<td>• 1 = default Designated Router priority (use ip pim dr-priority)</td>
</tr>
<tr>
<td></td>
<td>• DR = Designated Router</td>
</tr>
<tr>
<td></td>
<td>• S = Sparse mode</td>
</tr>
</tbody>
</table>
**show ip pim snooping tib**

Display information from the tree information base (TIB) discovered by PIM-SM snooping about multicast group members and states.

**Syntax**

```
show ip pim snooping tib [vlan vlan-id] [group-address [source-address]]
```

**Parameters**

- **vlan vlan-id** (OPTIONAL) Enter a VLAN ID to display TIB information discovered by PIM-SM snooping on a specified VLAN. Valid VLAN IDs: 1 to 4094.
- **group-address** (OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D) to display TIB information discovered by PIM-SM snooping for a specified multicast group.
- **source-address** (OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D) to display TIB information discovered by PIM-SM snooping for a specified multicast source.

**Command Modes**

EXEC

EXEC Privilege

**Command History**

Version 8.4.1.1 Introduced on E-Series ExaScale

**Example**

**Figure 41-10. show ip pim snooping tib Command Example**

```
FTOS#show ip pim snooping tib

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
*: Inherited port

(*, 225.1.2.1), uptime 00:00:01, expires 00:02:59, RP 165.87.70.1, flags: J
            Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
            Outgoing interface list:
               GigabitEthernet 4/11  RPF 165.87.32.2            00:00:01/00:02:59
               GigabitEthernet 4/13  Upstream Port              -/-

FTOS#show ip pim snooping tib vlan 2 225.1.2.1 165.87.1.7

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
*: Inherited port

(165.87.1.7, 225.1.2.1), uptime 00:00:08, expires 00:02:52, flags: j
            Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
            Outgoing interface list:
               GigabitEthernet 4/11  Upstream Port              -/-
               GigabitEthernet 4/13  DR Port                    -/-
               GigabitEthernet 4/20  RPF 165.87.32.10           00:00:08/00:02:52
```
### Table 41-5. show ip pim snooping tib Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the entry in the PIM multicast snooping database.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the PIM multicast route</td>
</tr>
<tr>
<td></td>
<td>table.</td>
</tr>
<tr>
<td>expires</td>
<td>Displays the amount of time until the entry expires and is removed from the</td>
</tr>
<tr>
<td></td>
<td>database.</td>
</tr>
<tr>
<td>RP</td>
<td>Displays the IP address of the RP/source for this entry.</td>
</tr>
<tr>
<td>flags</td>
<td>List the flags to define the entries:</td>
</tr>
<tr>
<td></td>
<td>• S = PIM Sparse Mode</td>
</tr>
<tr>
<td></td>
<td>• C = directly connected</td>
</tr>
<tr>
<td></td>
<td>• L = local to the multicast group</td>
</tr>
<tr>
<td></td>
<td>• P = route was pruned</td>
</tr>
<tr>
<td></td>
<td>• R = the forwarding entry is pointing toward the RP</td>
</tr>
<tr>
<td></td>
<td>• F = FTOS is registering this entry for a multicast source</td>
</tr>
<tr>
<td></td>
<td>• T = packets were received via Shortest Tree Path</td>
</tr>
<tr>
<td></td>
<td>• J = first packet from the last hop router is received and the entry is</td>
</tr>
<tr>
<td></td>
<td>ready to switch to SPT</td>
</tr>
<tr>
<td></td>
<td>• K = acknowledge pending state</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) interface towards the RP/</td>
</tr>
<tr>
<td></td>
<td>source.</td>
</tr>
<tr>
<td>RPF neighbor</td>
<td>Displays the next hop from this interface towards the RP/source.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Lists the interfaces that meet one of the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• a directly connect member of the Group.</td>
</tr>
<tr>
<td></td>
<td>• statically configured member of the Group.</td>
</tr>
<tr>
<td></td>
<td>• received a (*,G) Join message.</td>
</tr>
</tbody>
</table>
show ip pim summary

View information about PIM-SM operation.

Syntax

show ip pim summary

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.4.1.1  Support for the display of PIM-SM snooping status was added on E-Series ExaScale

Version 8.1.1.0  Introduced on E-Series ExaScale

Version 7.8.1.0  Introduced on S-Series

Example

Figure 41-11.  show ip pim summary Command Example

FTOS#show ip pim summary

PIM TIB version 495
Uptime 22:44:52
Entries in PIM-TIB/MFC : 2/2
Active Modes :
PIM-SNOOPING

Interface summary:
1 active PIM interface
0 passive PIM interfaces
3 active PIM neighbors

TIB summary:
1/1 (*) entries in PIM-TIB/MFC
1/1 (S,G) entries in PIM-TIB/MFC
0/0 (S,G,Rpt) entries in PIM-TIB/MFC
0 PIM nexthops
0 RPs
0 sources
0 Register states

Message summary:
2582/2583 Joins sent/received
5/0 Prunes sent/received
0/0 Candidate-RP advertisements sent/received
0/0 BSR messages sent/received
0/0 State-Refresh messages sent/received
0/0 MSDP updates sent/received
0/0 Null Register messages sent/received
0/0 Register-stop messages sent/received

Data path event summary:
0 no-cache messages received
0 last-hop switchover messages received
0/0 pim-assert messages sent/received
0/0 register messages sent/received

Memory usage:

TIB : 3768 bytes
Nexthop cache : 0 bytes
Interface table : 992 bytes
Neighbor table : 528 bytes
RP Mapping : 0 bytes
show ip pim tib

View the PIM tree information base (TIB).

Syntax: show ip pim tib [group-address [source-address]]

Parameters:
- **group-address**: (OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).
- **source-address**: (OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes:
- EXEC
- EXEC Privilege

Command History:
- Version 8.1.1.0: Introduced on E-Series ExaScale
- Version 7.8.1.0: Introduced on S-Series

Example:

```plaintext
Figure 41-12. show ip pim tib Command Example

FTOS#show ip pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
M - MSDP created entry, A - Candidate for MSDP Advertisement,
K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 226.1.1.1), uptime 01:29:19, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0

(*, 226.1.1.2), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0

(*, 226.1.1.3), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0

(*, 226.1.1.4), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
Outgoing interface list:
  GigabitEthernet 8/0
```

Table 41-6. show ip pim tib Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the entry in the multicast PIM database.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the PIM route table.</td>
</tr>
<tr>
<td>expires</td>
<td>Displays the amount of time until the entry expires and is removed from the database.</td>
</tr>
<tr>
<td>RP</td>
<td>Displays the IP address of the RP/source for this entry.</td>
</tr>
</tbody>
</table>
show running-config pim

Display the current configuration of PIM-SM snooping.

Syntax  show running-config pim

Command Modes  EXEC Privilege

Command History

Version 8.4.1.0  Introduced on E-Series ExaScale.

Related Commands

ip pim snooping  Enable PIM-SM snooping.

Example  Command Example: show running-config pim

FTOS#show running-config pim
!
ip pim snooping enable
IPv6 PIM-Sparse Mode Commands

The IPv6 PIM-SM commands are:

- ipv6 pim bsr-border
- ipv6 pim bsr-candidate
- ipv6 pim dr-priority
- ipv6 pim join-filter
- ipv6 pim query-interval
- ipv6 pim neighbor-filter
- ipv6 pim register-filter
- ipv6 pim rp-address
- ipv6 pim rp-candidate
- ip pim sparse-mode
- ipv6 pim spt-threshold
- show ipv6 pim bsr-router
- show ipv6 pim interface
- show ipv6 pim neighbor
- show ipv6 pim rp
- show ipv6 pim tib

**clear ipv6 pim tib**

Clear the IPv6 PIM multicast-routing database (tree information base—tib).

**Syntax**

`clear ipv6 pim tib [group-address]`

**Parameters**

- `group-address` (OPTIONAL) Enter the multicast group address in the `X:XX:XX::X` format. The `::` notation specifies successive hexadecimal fields of zero.

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

- Version 7.4.1.0 Introduced

**Related Commands**

`show ipv6 pim tib` Display the IPv6 PIM tree information base (tib)

**debug ipv6 pim**

Invoke IPv6 PIM debugging.

**Syntax**

`debug ipv6 pim [bsr | events | group group | packet | register [group] | state | timer [assert | hello | joinprune | register]]`

To disable IPv6 PIM debugging, enter `no debug ipv6 pim`. 
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bsr</strong></td>
<td>(OPTIONAL) Enter the keyword <code>bsr</code> to invoke debugging of IPv6 PIM Candidate RP/BSR activities.</td>
</tr>
<tr>
<td><strong>events</strong></td>
<td>(OPTIONAL) Enter the keyword <code>events</code> to invoke debugging of IPv6 PIM events.</td>
</tr>
<tr>
<td><strong>group group</strong></td>
<td>(OPTIONAL) Enter the keyword <code>group</code> followed by the group address to invoke debugging on that specific group.</td>
</tr>
<tr>
<td><strong>packet</strong></td>
<td>(OPTIONAL) Enter the keyword <code>packet</code> to invoke debugging of IPv6 PIM packets.</td>
</tr>
<tr>
<td><strong>register [group]</strong></td>
<td>(OPTIONAL) Enter the keyword <code>register</code> and optionally the group address to invoke debugging of IPv6 PIM register messages for a particular group.</td>
</tr>
<tr>
<td><strong>state</strong></td>
<td>(OPTIONAL) Enter the keyword <code>state</code> to view IPv6 PIM state changes.</td>
</tr>
<tr>
<td>**timer [assert</td>
<td>hello</td>
</tr>
<tr>
<td></td>
<td>• assert: to view the assertion timer.</td>
</tr>
<tr>
<td></td>
<td>• hello: to view the IPv6 PIM neighbor keepalive timer.</td>
</tr>
<tr>
<td></td>
<td>• joinprune: to view the expiry timer (join/prune timer)</td>
</tr>
<tr>
<td></td>
<td>• register: to view the register suppression timer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Disabled</th>
</tr>
</thead>
</table>

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

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### IPv6 pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

**Syntax**

`ipv6 pim bsr-border`

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

This command is applied to the subsequent PIM-BSR messages. Existing BSR advertisements are cleaned up by time-out.

### IPv6 pim bsr-candidate

Configure the router as a bootstrap (bsr) candidate.

**Syntax**

`ipv6 pim bsr-candidate interface [hash-mask-length] [priority]`

To disable the bootstrap candidate, use the no `ipv6 pim bsr-candidate` command.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| interface  | Enter the following keywords and slot/port or number information:  
• For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.  
• 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:  
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.  
• For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.  
• For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094. |
| hash-mask-length | (OPTIONAL) Enter the hash mask length for RP selection.  
Range: 0 to 128  
Default: 126 |
| priority     | (OPTIONAL) Enter the priority value for Bootstrap election process.  
Range: 0 to 255  
Default: 0 |

### defaults
As above

#### Command Modes
**CONFIGURATION**

### Command History
| Version 7.4.1.0 | Introduced |

---

**ipv6 pim dr-priority**

Change the Designated Router (DR) priority for the IPv6 interface.

**Syntax**

```
ipv6 pim dr-priority priority-value
```

To remove the DR priority value assigned, use the **no ipv6 pim dr-priority** command.

**Parameters**

| priority-value | Enter a number. Preference is given to larger/higher number.  
Range: 0 to 4294967294  
Default: 1 |

### Defaults
1

#### Command Modes
**INTERFACE**

### Command History
| Version 7.4.1.0 | Introduced |

### Usage Information
The router with the largest value assigned to an interface becomes the Designated Router. If two interfaces contain the same DR priority value, the interface with the largest interface IP address becomes the Designated Router.
ipv6 pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

Syntax
ipv6 pim join-filter access-list

Parameters
- **access-list**: Enter the name of an extended access list.
- **in**: Enter this keyword to apply the access list to inbound traffic.
- **out**: Enter this keyword to apply the access list to outbound traffic.

Defaults
None

Command Modes
INTERFACE

Command History
Version 8.3.1.0 Introduced

Example
FTOS(conf)#ipv6 access-list JOIN-FIL_ACL
FTOS(conf-ipv6-acl)#permit ipv6 165:87:34::0/112 ff0e::225:1:2:0/112
FTOS(conf-ipv6-acl)#permit ipv6 any ff0e::230:1:2:0/112
FTOS(conf-ipv6-acl)#permit ipv6 165:87:32::0/112 any
FTOS(conf-ipv6-acl)#exit
FTOS(conf)#interface gigabitethernet 0/84
FTOS(conf-if-gi-0/84)#ipv6 pim join-filter JOIN-FIL_ACL in
FTOS(conf-if-gi-0/84)#ipv6 pim join-filter JOIN-FIL_ACL out

ipv6 pim query-interval

Change the frequency of IPv6 PIM Router-Query messages.

Syntax
ipv6 pim query-interval seconds

To return to the default value, enter no ipv6 pim query-interval seconds command.

Parameters
- **seconds**: Enter a number as the number of seconds between router query messages. Default: 30 seconds Range: 0 to 65535

Defaults
30 seconds

Command Modes
INTERFACE

Command History
Version 7.4.1.0 Introduced

ipv6 pim neighbor-filter

Prevent the system from forming a PIM adjacency with a neighboring system.

Syntax
ipv6 pim neighbor-filter access-list

Parameters
- **access-list**: Enter the name of a standard access list. Maximum 16 characters.
ipv6 pim register-filter

Configure the source DR so that it does not send register packets to the RP for the specified sources and groups.

Syntax

```
ipv6 pim register-filter access-list
```

Parameters

- `access-list`: Enter the name of the extended ACL that contains the sources and groups to be filtered.

Defaults

None

Command Modes

CONFIGURATION

Command History

Version 8.3.1.0 Introduced

Example

```
FTOS(conf)#ipv6 pim register-filter REG-FIL_ACL
FTOS(conf)#ipv6 access-list REG-FIL_ACL
FTOS(conf-ipv6-acl)#deny ipv6 165:87:34::10/128 ff0e::225:1:2:0/112
FTOS(conf-ipv6-acl)#permit ipv6 any any
FTOS(conf-ipv6-acl)#exit
```

ipv6 pim rp-address

Configure a static PIM Rendezvous Point (RP) address for a group. This address is used by first-hop routers to send Register packets on behalf of the source multicast host.

Syntax

```
ipv6 pim rp-address address group-address group-address mask override
```

Parameters

- `address`: Enter the IPv6 RP address in the X:XX:XX::X format. The :: notation specifies successive hexadecimal fields of zero.
- `group-address`: Enter the keyword group-address followed by the group address in the X:XX:XX::X format and then the mask in /nn format to assign that group address to the RP. The :: notation specifies successive hexadecimal fields of zero.
- `override`: Enter the keyword override to override the BSR updates with static RP. The override will take effect immediately during enable/disable. Note: This option is applicable to multicast group range.

To remove an RP address, use the `no ipv6 pim re-address address group-address mask override` command.

Defaults

None

Command Modes

CONFIGURATION

Command History

Version 8.3.1.0 Introduced

Example

```
FTOS(conf)#ipv6 pim rp-address 165:87:34::10/128 ff0e::225:1:2:0/112
```

Usage Information

Do not enter this command before creating the access-list.
ipv6 pim rp-candidate

Specify an interface as an RP candidate.

Syntax
ipv6 pim rp-candidate interface [priority-value]

Parameters

<table>
<thead>
<tr>
<th>interface</th>
<th>Enter the following keywords and slot/port or number information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a Loopback interface, enter the keyword loopback followed by a number from 0 to 16383.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword port-channel followed by a number:</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>priority-value</th>
<th>(OPTIONAL) Enter a number as the priority of this RP Candidate, which is included in the Candidate-RP-Advertisements.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range: 0 (highest) to 255 (lowest)</td>
</tr>
</tbody>
</table>

Defaults
No default values or behavior

Command Modes
CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.4.1.0</td>
<td></td>
</tr>
</tbody>
</table>
ipv6 pim sparse-mode

Enable IPv6 PIM sparse mode on the interface.

Syntax

ipv6 pim sparse-mode

To disable IPv6 PIM sparse mode, enter no ipv6 pim sparse-mode.

Defaults

Disabled

Command Modes

INTERFACE

Command History

Version 7.4.1.0 Introduced

Usage Information

The interface must be enabled (no shutdown command) and not have the switchport command configured. Multicast must also be enabled globally. PIM is supported on the port-channel interface.

ipv6 pim spt-threshold

Specifies when a PIM leaf router should join the shortest path tree.

Syntax

ipv6 pim spt-threshold {kbps | infinity}

To return to the default value, enter no ipv6 pim spt-threshold.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kbps</td>
<td>Enter a traffic rate in kilobytes per second. Range: 0 to 4294967 kbps Default: 10 kbps</td>
</tr>
<tr>
<td>infinity</td>
<td>Enter the keyword infinity to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).</td>
</tr>
</tbody>
</table>

Defaults

10 kbps

Command Modes

CONFIGURATION

Command History

Version 7.4.1.0 Introduced

Usage Information

PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.
show ipv6 pim bsr-router

View information on the bootstrap router (v2).

Syntax

show ipv6 pim bsr-router

Command Modes

EXEC
EXEC Privilege

Command History

Version 7.4.1.0 Introduced

Example

Figure 41-13. show ipv6 pim bsr-router Command Example

FTOS#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
BSR address: 14::2
Uptime: 00:02:54, BSR Priority: 0, Hash mask length: 126
Next bootstrap message in 00:00:06

This system is a candidate BSR
Candidate BSR address: 14::2, priority: 0, hash mask length: 126

FTOS#

show ipv6 pim interface

Display IPv6 PIM enabled interfaces.

Syntax

show ipv6 pim interface

Command Modes

EXEC
EXEC Privilege

Command History

Version 7.4.1.0 Introduced

Example

Figure 41-14. show ipv6 pim interface Command Example

FTOS#show ipv6 pim interface
Interface Ver/ Nbr Query DR
Mode Count Intvl Prio
Gi 10/3 v2/S 1 30 1
Address : fe80::201:e8ff:fe02:140f
DR : this router
Gi 10/11 v2/S 0 30 1
Address : fe80::201:e8ff:fe02:1417
DR : this router
FTOS#

show ipv6 pim neighbor

Display IPv6 PIM neighbor information.

Syntax

show ipv6 pim neighbor [detail]
show ipv6 pim rp
Syntax: show ipv6 pim rp [mapping | group-address]

Parameters:
- **mapping** (OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
- **group-address** (OPTIONAL) Enter the multicast group address in the `X::X::X::X` format to view RP mappings for a specific group. The `::` notation specifies successive hexadecimal fields of zero.

Command Modes:
- EXEC
- EXEC Privilege

Command History:
- Version 7.4.1.0 Introduced

Example 1:
```
FTOS#show ipv6 pim rp
Group  RP
ff0e::225:1:2:1  14::1
ff0e::225:1:2:2  14::1
ff0e::226:1:2:1  14::1
ff0e::226:1:2:2  14::1
FTOS#
```
show ipv6 pim tib

View the IPv6 PIM multicast-routing database (tree information base—tib).

**Syntax**

```
show ipv6 pim tib [group-address [source-address]]
```

**Parameters**

- **group-address** (OPTIONAL) Enter the IPv6 group address in the `X::X::X::X` format. The `::` notation specifies successive hexadecimal fields of zero.
- **source-address** (OPTIONAL) Enter the source address in the `X::X::X::X` format. The `::` notation specifies successive hexadecimal fields of zero.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 7.4.1.0 Introduced

**Example 2**

**Figure 41-17. show ipv6 pim rp mapping Command Example**

```
FTOS#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
 RP: 14::1, v2
   Info source: 14::1, via bootstrap, priority 192
   Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
 RP: 14::2, v2
FTOS#
```

**Example**

**Figure 41-18. show ipv6 pim tib Command Example**

```
FTOS#show ipv6 pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
 R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
 M - MSDP created entry, A - Candidate for MSDP Advertisement
 K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires 00:00:00, flags: CJ
 RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
Outgoing interface list:
 GigabitEthernet 10/11

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00, flags: CJ
 RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
Outgoing interface list:
 GigabitEthernet 10/11

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00, flags: CJ
 RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
Outgoing interface list:
 GigabitEthernet 10/11

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires 00:00:00, flags: CJ
 RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
Outgoing interface list:
 GigabitEthernet 10/11
FTOS#
```
PIM-Source Specific Mode (PIM-SSM)

Overview

The platforms on which a command is supported is indicated by the character — for the E-Series, for the C-Series, and for the S-Series — that appears below each command heading.

PIM is supported on E-Series ExaScale with Dell Networking OS 8.1.1.0 and later.

This chapter contains the following sections:

- IPv4 PIM Commands
- IPv4 PIM-Source Specific Mode Commands
- IPv6 PIM Commands
- IPv6 PIM-Source Specific Mode Commands

IPv4 PIM Commands

The following commands apply to IPv4 PIM-SM, PIM-SSM, and PIM-DM:

- clear ip pim tib
- debug ip pim
- ip pim dr-priority
- ip pim graceful-restart
- ip pim neighbor-filter
- ip pim query-interval
- show ip pim interface
- show ip pim neighbor
- show ip pim tib

IPv4 PIM-Source Specific Mode Commands

The IPv4 PIM-Source Specific Mode (PIM-SSM) commands are:

- ip pim ssm-range
- ip pim join-filter
- show ip pim ssm-range
### ip pim ssm-range

Specify the SSM group range using an access-list.

**Syntax**

```
ip pim ssm-range {access_list_name}
```

**Parameters**

- **access_list_name**: Enter the name of the access list.

**Defaults**

Default SSM range is 232/8 and ff3x/32

**Command Modes**

- Configuration

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Dell Networking OS supports standard access list for the SSM range. Extended ACL cannot be used for configuring SSM range. If an Extended ACL is configured and then used in the `ip pim ssm-range {access_list_name}` configuration, an error is reported.

However, if `ip pim ssm-range {access_list_name}` is configured first and then the ACL is configured as an Extended ACL, an error is not reported and the ACL is not applied to the SSM range.

Dell Networking OS recommended best-practices are to configure the standard ACL, and then apply the ACL to the SSM range. Once the SSM range is applied, the changes are applied internally without requiring clearing of the TIB.

When ACL rules change, the ACL and PIM modules apply the new rules automatically.

When SSM range is configured, Dell Networking OS supports SSM for configured group range as well as default SSM range.

When the SSM ACL is removed, PIM SSM is supported for default SSM range only.

---

### show ip pim ssm-range

Display the non-default groups added using the SSM range feature.

**Syntax**

```
show ip pim ssm-range
```

**Defaults**

No default behavior or values

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>
IPv6 PIM Commands

The following commands apply to IPv6 PIM-SM and PIM-SSM:

- `clear ipv6 pim tib`
- `debug ip pim`
- `ipv6 pim dr-priority`
- `ipv6 pim join-filter`
- `ipv6 pim query-interval`
- `ipv6 pim neighbor-filter`
- `show ipv6 pim interface`
- `show ipv6 pim neighbor`
- `show ipv6 pim tib`

IPv6 PIM-Source Specific Mode Commands

The IPv6 PIM-SSM commands are:

- `ipv6 pim ssm-range`
- `show ipv6 pim ssm-range`

**ipv6 pim ssm-range**

Specify the SSM group range using an access-list.

**Syntax**

```
ipv6 pim ssm-range \{access_list_name\}
```

**Parameters**

- `access_list_name`
  Enter the name of the access list. Maximum 16 characters.

**Defaults**

Default SSM range is 232/8 and ff3x/32

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

Once the SSM range is applied, the changes are applied internally without requiring clearing of the TIB. SSM ACL overrides the default range. To use the default range while SSM range is active, add the default range to the SSM ACL.

When ACL rules change, the ACL manager and PIM modules apply the new rules automatically.
When the SSM ACL is removed, the default range is restored. When SSM range is configured, Dell Networking OS supports SSM for configured group range as well as default SSM range.

**show ipv6 pim ssm-range**

Display the non-default groups added using the SSM range feature.

**Syntax**

```
show ipv6 pim ssm-range
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version 7.4.1.0 Introduced

**Example**

```
FTOS(conf)#ipv6 pim ssm-range SSM_ACL
FTOS(conf)#ipv6 access-list SSM_ACL
FTOS(conf-ipv6-acl)#permit ipv6 any ff0e::225:1:2:0/112
FTOS(conf-ipv6-acl)#
FTOS(conf-ipv6-acl)#do show ipv6 pim ssm-range
Group Address   /  MaskLen
ff0e::225:1:2:0 / 112
FTOS(conf-ipv6-acl)#
```
Power over Ethernet (PoE) and Power over Ethernet Plus (PoE+)

Overview

Dell Networking OS supports Power over Ethernet (PoE) on C-Series and S-Series systems (S25V and S50V models) as described by IEEE 802.3af. Dell Networking OS supports Power over Ethernet Plus (PoE+) on the C-Series system, as described by IEEE 802.3at.

Refer to the \(^{\text{C}}\) and \(^{\text{S}}\) characters that appear below each command heading. If a command supports both PoE and PoE+, PoE supports the S-Series.

Commands

This chapter contains the following commands:

- `power budget`
- `power inline`
- `power inline priority`
- `show power detail`
- `show power inline`
- `show power supply`

`power budget` \(^{\text{S}}\)

If an S25V or S50V model of the S-Series has an external power supply, this command allows the external power supply of the specified stack member to be used for powering PoE ports. An external DC power supply operates, by default, in Backup mode. However, if the power supply is the 470W Redundant Power Supply (catalog # S50-01-PSU-V) from Dell Networking, and it is attached to the Current Sharing terminal, use this command to convert its use to Load-Sharing mode to support additional PoE devices. Other external DC power supplies are not supported for PoE.

**Syntax**

\[ \text{[no] power budget stack-unit 0-7 321-790} \]

To disable the use of power for PoE from the external power supply on the designated stack member, enter `no power budget stack-unit 0-7`. 
Parameters

0-7 Enter the stack unit ID, from 0 to 7, of the stack member that you want to configure.

321-790 After entering the stack unit number, enter a value representing the watts to be used for PoE.
Range: 321 to 790

Defaults

320W (Redundancy mode)

Command Modes

CONFIGURATION

Command History

Version 7.7.1.0 Introduced on the S-Series.

Usage Information

Setting a value above 320W causes a warning to display stating the device might lose power redundancy.

power inline

Enable power to be supplied to a device connected to a port.

Syntax

[no] power inline {auto [max_milliwatts] | static [max_milliwatts]}

To disable power to a port that has been enabled for PoE/PoE+, use the no power inline command.

Parameters

auto Enter the keyword auto to allow the port to determine how much power the connected Class 0, 1, 2, 3, or 4 device requires, and supply it (up to 30.0 watts).

max_milliwatts (OPTIONAL) Enter the number of milliwatts to be the maximum amount of power that a port can provide.
Range: 440 to 30000 (milliwatts)

static Entering the keyword static without the max_milliwatts variable sets the amount of power available on the selected port to the maximum (up to 30.0 watts).

Defaults

no (power is disabled to the port)

Command Modes

INTERFACE

Command History

Version 7.7.1.0 Introduced on the S-Series.

Version 7.5.1.0 Introduced on the C-Series.

Usage Information

Ports configured with power inline auto have a lower priority for access to power than those configured with power inline static. As a second layer of priority setting, use the power inline priority command.

Dell Networking OS treats powered devices rated as Class 0 or 4 the same.

Related Commands

power inline priority Set the power priority of the selected port.

show power inline Display the ports that are enabled with PoE and the amount of power that each is consuming.
power inline priority

Set the power priority of the selected port.

**Syntax**

```
[no] power inline priority {critical | high | low}
```

**Parameters**

- `critical`: Enter the keyword `critical` to set the power priority of the port to the highest level.
- `high`: Enter the keyword `high` to set the power priority of the port to the second highest level.
- `low`: Enter the keyword `low` to set the power priority of the port to the lowest level.

**Defaults**

none

**Command Modes**

INTERFACE

**Command History**

Version 7.7.1.0 Introduced on the C-Series and S-Series.

**Usage Information**

Power allocation is a function of per-port power priority settings, port TLVs, port IDs, which ports request power first, and how much power is actually consumed by the active ports. Power priority is allocated by this formula:

\[
\text{PoE}_{\text{off}}_{\text{priority}} = \text{static\_or\_auto\_prio} \times 10000 + (\text{user/LLDP-MED or IEEE 802.3at power-via-mdi})_{\text{priority}} \times 1000 + \text{slotId} \times 100 + \text{portId}
\]

where:

- `static\_prio = 0`
- `auto\_prio = 1`

The lower the value of \(\text{PoE}_{\text{off}}_{\text{priority}}\) for the selected port, the higher its power priority. So, if a port is configured “static” (assigned a value of 0 in the formula), its priority is higher than a port configured as “auto” (assigned a value of 1). Two ports with the same static/auto settings are then prioritized by their user-set priorities and LLDP-MED or IEEE 802.3at power-via-mdi values.

In a similar fashion, lower numbered slots/ports get a higher priority than higher numbered slots/ports. For example, 0/1 has a higher priority than 1/10, which has a higher priority than 2/1. As the slot / port number increases, the value of “\(\text{PoE}_{\text{off}}_{\text{priority}}\)” for the port increases and hence a lower priority.

Priority is assigned in this order:

1. static/auto settings (using the `power inline` command)
2. user-set priorities (using this command)
3. LLDP-MED or IEEE 802.3at power-via-mdi TLV, only if user priority is not configured (see Link Layer Detection Protocol (LLDP).)
4. Slot ID (breaks tie of same-priority ports)
5. Port ID (breaks tie of same-priority ports in same slot)

**Related Commands**

- `power inline` Enable power to be supplied to a device connected to a port.
- `show power inline` Display the ports that are enabled with PoE/PoE+ and the amount of power that each is consuming.
show power detail

Display the total power consumption and power consumption by component.

Syntax

```
show power detail
```

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.1.0  Inline Power Used removed from the output.
- Version 7.7.1.0  Introduced on the S-Series.
- Version 4.2.1.0  Introduced on the C-Series.

Example

```
FTOS# show power detail
Catalog           slot    Logic Power      Inline Power      Inline Power
Name              Id      Consumed         Allocated         Consumed
(Watts)          (Watts)          (Watts)
---------------------------------------------------------------------------
E48IB              0         100               0.00              0.00
E48IB              1         100               0.00              0.00
EX8PB              2         120               0.00              0.00
E48TB              3         100               0.00              0.00
RPM                0         100                  -                 -
RPM                1         100                  -                 -
E48PB              4         130               0.00              0.00
E48VB              5         100               0.00              0.00
E48IB              6         130               0.00              0.00
E48VB              7         100               0.00              0.00
CC-C300-FAN        -          85                  -                 -
Total Inline Power Available: 0.00 W
Total Inline Power Allocated: 0.00 W
Total Inline Power Consumed : 0.00 W
Total Inline Power Remaining: 0.00 W
```

Table 43-1.  show power detail Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>(S-Series only) The stack member unit ID.</td>
</tr>
<tr>
<td>Catalog Name</td>
<td>(C-Series only) Displays the component's Dell Networking catalog number.</td>
</tr>
<tr>
<td>Slot ID</td>
<td>(C-Series only) Displays the slot number in which the line card or RPM is installed.</td>
</tr>
<tr>
<td>Total Power Available</td>
<td>(S-Series only) The total power available in the stack member or chassis. Note: On the S-Series a maximum of 790W can be allocated for PoE, even if you add the 470W external power supply. Note: This field is not shown on the C-Series. The total power available will vary, depending upon the type and number of PSUs installed.</td>
</tr>
<tr>
<td>Logic Power Consumed</td>
<td>The power consumed by the system logic.</td>
</tr>
<tr>
<td>Inline Power Available</td>
<td>Power available for PoE for the S-Series (whatever was configured using the power-budget command. Default: 320 watts There is no default value for the C-Series, as power will vary, depending upon type and number of PSUs installed.</td>
</tr>
<tr>
<td>Inline Power Allocated</td>
<td>Total power allocated to the ports.</td>
</tr>
<tr>
<td>Inline Power Consumed</td>
<td>Total power consumed by connected devices.</td>
</tr>
<tr>
<td>Inline Power Remaining</td>
<td>Difference between power available and power allocated.</td>
</tr>
</tbody>
</table>
show power inline

Display the ports that are enabled with PoE/PoE+ and the amount of power that each is consuming.

Syntax

show power inline

Command Modes

EXEC

EXEC Privilege

Command History

Table 43-2.  show power inline Command Output Field Description

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Allocated (Watts)</th>
<th>Consumed (Watts)</th>
<th>Class</th>
<th>Type</th>
<th>Priority</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GL 0/47</td>
<td>auto</td>
<td>0.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/0</td>
<td>static</td>
<td>30.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/1</td>
<td>static</td>
<td>30.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/2</td>
<td>static</td>
<td>30.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/3</td>
<td>static</td>
<td>30.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/4</td>
<td>static</td>
<td>30.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/5</td>
<td>static</td>
<td>30.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/6</td>
<td>auto</td>
<td>0.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/7</td>
<td>auto</td>
<td>0.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/8</td>
<td>auto</td>
<td>0.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/9</td>
<td>auto</td>
<td>0.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
<tr>
<td>GL 3/10</td>
<td>auto</td>
<td>0.00</td>
<td>0.00</td>
<td>NO_DEVICE</td>
<td>-</td>
<td>Low</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 43-2.  show power inline Command Output Field Description

| Interface | Displays the line card slot and port number. |
| Admin     | Displays the PoE/PoE+ mode of the port. The mode can be either Auto or Static. See power budget. |
| Inline Power Allocated | Displays the amount of power allocated to the port. |
| Inline Power Consumed | Displays the amount of power that is consumed by the connected device. Note: Overload protection is applied only when the power consumption is above the allocated power limit for duration above the time limit specified in the IEEE specification. Before the protection is applied, the power consumed value seen may be momentarily higher than the limit. |
| Class | Displays the power classification of the connected device. If the device is powered up properly, it displays Class 0, 1, 2, 3, or 4. Displays the following under different conditions: |
| | • NO_DEVICE if no device is present. |
| | • LEGACY if a legacy device is connected. |
| | • PD_S/C if a short-circuit condition is detected. |
| | • PD_OVRLD if overload condition is detected. |
| Device Type | Displays whether the device is Type 1 or Type 2. |
show power supply

Display the power supply status.

Syntax

```
show power supply
```

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.5.0 Added Line Mode to command output on the C-Series.
- Version 7.7.1.0 Introduced on the S-Series.
- Version 7.5.1.0 Introduced on the C-Series.

C-Series

Example

```
FTOS#show power supply
Power Supply Model               Type    Status             Line Mode
--------------------------------------------------------------
PEM0       CC-C-1600W-AC          AC      Powered Off        NA
PEM1       CC-C-1600W-AC          AC      Fail              NA
PEM2       CC-C-1600W-AC          AC      Active            High (1600W)
PEM3       CC-C-1600W-AC          AC      Power supply fan fail NA
PEM4       CC-C-1600W-AC          AC      Active            Low (1200W)
PEM5       CC-C-1600W-AC          AC      Overload          NA
PEM6       CC-C-1600W-AC          AC      Over Temperature Shutdown NA
PEM7       CC-C-1600W-AC          AC      AC Fail           NA
```

Table 43-3 describes the ten possible power supply status conditions for the C-Series.

Table 43-3. Power Supply Status Conditions for the C-Series

<table>
<thead>
<tr>
<th>Status conditions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Fail</td>
<td>The power supply is unplugged.</td>
</tr>
<tr>
<td>Active</td>
<td>The PSU is supplying power to the chassis.</td>
</tr>
<tr>
<td>Fail</td>
<td>The PSU has failed.</td>
</tr>
<tr>
<td>Absent</td>
<td>The PSU is not installed in the chassis.</td>
</tr>
<tr>
<td>Overload</td>
<td>The PSU has turned off due to overload.</td>
</tr>
<tr>
<td>Over Temperature Shutdown</td>
<td>The PSU has turned off due to a high temperature condition.</td>
</tr>
<tr>
<td>Over Temperature Warning</td>
<td>The temperature of the PSU is greater than the recommended maximum operating temperature.</td>
</tr>
<tr>
<td>Over Current Warning</td>
<td>The PSU load is almost or exceeded its recommended maximum load.</td>
</tr>
</tbody>
</table>
Table 43-3.  Power Supply Status Conditions for the C-Series

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Off</td>
<td>The PSU is present but the switch is in OFF position.</td>
</tr>
<tr>
<td>Power supply fan fail</td>
<td>The PSU fan has failed.</td>
</tr>
</tbody>
</table>

Table 43-4 describes the nine possible power supply conditions for the S-Series.

Table 43-4.  Power Supply Conditions for the S-Series

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Fail</td>
<td>The PSU is unplugged.</td>
</tr>
<tr>
<td>Active</td>
<td>The PSU is supplying power to the chassis.</td>
</tr>
<tr>
<td>Fail</td>
<td>The PSU has failed.</td>
</tr>
<tr>
<td>Not Present</td>
<td>The PSU is not installed in the chassis.</td>
</tr>
<tr>
<td>Over Current Shutdown</td>
<td>The PSU has turned off due to an high input current condition.</td>
</tr>
<tr>
<td>Over Temperature Shutdown</td>
<td>The PSU has turned off due to an high temperature condition.</td>
</tr>
<tr>
<td>Over Temperature Warning</td>
<td>The temperature of the PSU is greater than the recommended maximum operating temperature.</td>
</tr>
<tr>
<td>Over Current Warning</td>
<td>The current being supplied to the PSU is greater than the recommended maximum input current.</td>
</tr>
<tr>
<td>Power Off</td>
<td>The PSU is present but not on.</td>
</tr>
</tbody>
</table>

Figure 43-2.  show power supply (S-Series) Command Example

```
FTOS#show power supply
Unit Power Model Type Status
Supply Number
----------------------------------------------------------------------
0 PS0 S50-PWR-AC AC Active
0 PS1 S50-PWR-DC DC Active
1 PS0 S50-PWR-AC AC Active
1 PS1 Not present
2 PS0 S50-PWR-AC AC Active
2 PS1 Not present
Dell Networking OS
```
Port Monitoring

Overview

The Port Monitoring feature enables you to monitor network traffic by forwarding a copy of each incoming or outgoing packet from one port to another port.

The Remote Port Mirroring feature allows you to monitor traffic on multiple source ports on different switches and transport mirrored packets on a dedicated L2 VLAN to multiple destination ports on different switches.

The commands in this chapter are generally supported on the C-Series, E-Series, and S-Series, with one exception, as noted in the Command History fields and by these symbols under the command headings: C E S

Commands

- description
- flow-based enable
- mode remote-port-mirroring
- monitor session
- show config
- show monitor session
- show running-config monitor session
- source (port monitoring)
- source (remote port mirroring)
- source remote vlan (remote port mirroring)
- tagged destination
- untagged destination
**Important Points to Remember**

- On the E-Series, Port Monitoring is supported on TeraScale and ExaScale platforms.
- Port Monitoring is supported on physical ports only. Logical interfaces, such as Port Channels and VLANs, are not supported.
- Dell Networking OS supports as many monitor sessions on a system as the number of port-pipes.
- A SONET port can only be configured as a monitored port.
- 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.
- Dell Networking OS on the S-Series supports multiple source ports to be monitored by a single destination port in one monitor session.
- On the S-Series, one monitor session can have only one MG port. There is no restriction on the number of source ports, or destination ports on the chassis.

**Note:** The monitoring port should not be a part of any other configuration.

- Remote Port Mirroring is supported only on the E-Series ExaScale platform.

### description

**Enter a description of this monitoring session**

**Syntax**

description \( \{description\} \)

To remove the description, use the **no description \( \{\)description\}\) command.

**Parameters**

- \(description\) Enter a description regarding this session (80 characters maximum).

**Defaults**

No default behavior or values

**Command Modes**

MONITOR SESSION (conf-mon-sess-\{session-ID\})

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-7.7.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- **monitor session** Enable a monitoring session.
flow-based enable

Enable flow-based monitoring.

Syntax

```plaintext
flow-based enable
```

To disable flow-based monitoring, use the `no flow-based enable` command.

Defaults

Disabled, that is flow-based monitoring is not applied

Command Modes

MONITOR SESSION (conf-mon-sess-<session-ID>)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

To monitoring traffic with particular flows ingressing/egressing the interface, appropriate ACLs can be applied in both ingress and egress direction.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session</td>
<td>Create a monitoring session.</td>
</tr>
</tbody>
</table>
mode remote-port-mirroring

Configure a L2 VLAN as the VLAN used to transport mirrored traffic in a remote-port mirroring session.

Syntax

mode remote-port-mirroring

Defaults

No default values or behaviors

Command Modes

VLAN INTERFACE

Command History

Version 8.4.1.2
Introduced on the E-Series ExaScale.

Example

Figure 44-1. Command Example: mode remote-port-mirroring

FTOS(conf)# interface vlan 10
FTOS(conf-if-vlan)# mode remote-port-mirroring

Usage Information

A remote port mirroring session mirrors Layer 2 and Layer 3 traffic by prefixing the reserved VLAN tag to monitored packets so that they are copied to the reserve VLAN.

Mirrored traffic is transported across the network using 802.1Q-in-802.1Q tunneling. The source address, destination address and original VLAN ID of the mirrored packet are preserved with the tagged VLAN header. Untagged source packets are tagged with the reserved VLAN ID.

There is no restriction on the VLAN IDs used for the reserved remote-monitoring VLAN. Valid VLAN IDs are 1 to 4094. The default VLAN ID is not supported.

The reserved VLAN for remote port mirroring can be automatically configured in intermediate switches by using GVRP.

MAC address learning in the reserved VLAN is automatically disabled.

To change the reserved VLAN used in a source session, you can remove the current VLAN by entering the complete no source destination vlan vlan-id command. Then re-enter the source (remote port mirroring) command to configure a new reserved VLAN for the source session.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface vlan</td>
<td>Configure a VLAN.</td>
</tr>
<tr>
<td>show monitor session</td>
<td>Display the monitor session.</td>
</tr>
<tr>
<td>tagged destination</td>
<td>Configure a tagged port to carry mirrored traffic in a reserved VLAN.</td>
</tr>
</tbody>
</table>
Create a session for monitoring traffic with port monitoring or remote port mirroring.

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

```
Parameter          Description
-----------------------------------------------------
session-ID          Enter a session identification number.
                    Range: 0 to 65535
```

Defaults

No default values or behaviors

Command Modes

MONITOR SESSION (conf-mon-sess-session-ID)

Command History

```
Version 8.4.1.2   Support for remote port mirroring was added on the E-Series ExaScale.
Version 8.1.1.0   Introduced on E-Series ExaScale
Version 7.7.1.0   Introduced on S-Series
Version 7.5.1.0   Introduced on C-Series
Version 7.4.1.0   Introduced on E-Series
```

Example

```
Figure 44-2.  Command Example: monitor session

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.

In remote-port mirroring sessions:

- Up to 4 source sessions are supported on a switch. Up to 128 ports are supported in a source session, including all ports in source port channels and source VLANs.
- Up to 64 destination sessions are supported on a switch. Up to 64 ports are supported in a destination session.

Related Commands

```
show monitor session        Display the monitor session
show running-config monitor session   Display the running configuration of a monitor session
```
show config

Display the current monitor session configuration.

Syntax

show config

Defaults

No default values or behavior

Command Modes

MONITOR SESSION (conf-mon-sess-<session-ID>)

Command History

+-------------------+----------------------------------+
| Command History   | Description                      |
+-------------------+----------------------------------+
| Version 8.1.1.0   | Introduced on E-Series ExaScale  |
| Version 7.7.1.0   | Introduced on S-Series           |
| Version 7.5.1.0   | Introduced on C-Series           |
| Version 7.4.1.0   | Introduced on E-Series           |
+-------------------+----------------------------------+

Example

FTOS(conf-mon-sess-11)#show config
!
monitor session 11
  source GigabitEthernet 10/0 destination GigabitEthernet 10/47 direction rx
FTOS#
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

No default values or behavior

Command Modes

- EXEC
  - EXEC Privilege

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.7.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 7.4.1.0 Introduced on E-Series

Example

```
Figure 44-3. Commands Example: show monitor session

FTOS#show monitor session 11

SessionID | Source | Destination | Direction | Mode | Type
----------|--------|-------------|----------|------|------
11 | Gi 10/0 | Gi 10/47 | rx | interface | Port-based
12 | Po 1 | remote-vlan 12 | both | Remote-Port-Mirroring | Port-based
```

Related Commands

- `monitor session` Create a session for monitoring.
show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

Syntax

```
show running-config monitor session {session-ID}
```

To display the running configuration for all monitor sessions, use just the `show running-config monitor session` command.

Parameters

- **session-ID**
  - (OPTIONAL) Enter a session identification number.
  - Range: 0 to 65535

Defaults

No default values or behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.7.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **Version 7.4.1.0** Introduced on E-Series

Example

```
FTOS#show running-config monitor session
! monitor session 8
  source GigabitEthernet 10/46 destination GigabitEthernet 10/1 direction rx
! monitor session 11
  source GigabitEthernet 10/0 destination GigabitEthernet 10/47 direction rx

FTOS#show running-config monitor session 11
! monitor session 11
  source GigabitEthernet 10/0 destination GigabitEthernet 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**  
  Create a session for monitoring.
- **show monitor session**  
  Display 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 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the 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.
  - For a SONET interface, enter the keyword `sonet` 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**

No default behavior or values

**Command Modes**

MONITOR SESSION (conf-mon-sess-session-ID)

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.1.1.0** Introduced on E-Series ExaScale
- **Version 7.7.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **Version 7.4.1.0** Introduced on E-Series

**Example**

**Figure 44-4. Command Example: Configuring a Port Monitor Source**

```
FTOS(conf-mon-sess-11)#source gi 10/0 destination gi 10/47 direction rx
FTOS(conf-mon-sess-11)#
```

**Usage Information**

- **Note**: A SONET port can only be configured as a monitored port.
source (remote port mirroring)

Configure one or more source ports, the ingress/egress traffic to be mirrored, and the reserved L2 VLAN used to transport mirrored traffic.

Syntax

```
source {single-interface | vlan vlan-id | range {interface-list | interface-range | mixed-interface-list | vlan-list | vlan-range | mixed-vlan-list}} destination remote-vlan vlan-id
direction {rx | tx | both}
```

Parameters

- **single-interface**: Specifies one of the following interface types:
  - 1-Gigabit Ethernet: Enter `gigabitethernet slot/port`.
  - 10-Gigabit Ethernet: Enter `tengigabitethernet slot/port`.
  - Port channel: Enter `port-channel {1-511}`.

- **vlan vlan-id**: Specifies a single VLAN ID. Range: 1-4094

- **range interface-list**: Specifies multiple interfaces separated by a comma and space:
  `single-interface, single-interface, single-interface`...
  For example: `source range port-channel 2, gigabitethernet 3/4`

- **range interface-range**: Specifies one of the following interface ranges:
  - `gigabitethernet slot/first_port - last_port`
  - `tengigabitethernet slot/first_port - last_port`
  - `port-channel first_number - last_number`
  A space is required before and after the dash (-).
  For example: `source range gigabitethernet 1/2 - 4`
  Or: `source range port-channel 1 - 12`

- **range mixed-interface-list**: Specifies single interfaces and interface ranges in any order:
  `range single-interface, interface-range, single-interface`...
  For example: `source range port-channel 2, gigabitethernet 3/4 - 5`

- **range vlan-list**: Specifies multiple source VLANs separated by a comma and space:
  `range vlan vlan-id, vlan vlan-id`...
  For example: `source range vlan 2, vlan 12, vlan 22`

- **range vlan-range**: Specifies a range of source VLANs in the format:
  `range vlan first_vlanID - last_vlanID`.
  A space is required before and after the dash (-).
  For example: `source range vlan 9-11`

- **range mixed-vlan-list**: Specifies single VLANs and VLAN ranges in any order:
  `range vlan vlan-id, vlan first_vlanID - last_vlanID`...
  For example: `source range vlan 2, vlan 10 - 11, vlan 5`

- **destination remote-vlan vlan-id**: Associates the reserved L2 VLAN with the source ports used in the source session. Valid VLAN IDs are 1 to 4094. The default VLAN ID is not supported.

- **direction {rx | tx | both}**: Specifies the direction of the traffic to be mirrored:
  - `rx`: incoming packets only
  - `tx`: outgoing packets only
  - `both`: both incoming and outgoing packets

Defaults

No default behavior or values
Command Modes
MONITOR SESSION (conf-mon-sess-session-ID)

Command History
Version 8.4.1.2 Introduced on the E-Series ExaScale.

Figure 44-5. Command Example: Configuring a Source Port

FTOS(conf-mon-sess-11)#source gigabitethernet 10/0 destination remote-vlan 2
direction rx
FTOS(conf-mon-sess-11)#

Usage Information
You can configure physical ports, port-channels, and VLANs as sources in remote port mirroring and use them in the same source session. You can use both Layer 2 (configured with the switchport command) and Layer 3 ports as source ports.

In remote port mirroring:

- Up to 4 source sessions are supported on a switch.
- Up to 128 source ports are supported in a source session.

When you configure a port channel or VLAN in a source session, all ports in the port channel or VLAN are used as source ports, up to a maximum of 128 source ports.

You can configure trunk ports and access ports as source ports.

You can configure trunk ports and non-trunk ports as source ports in a remote-port mirroring session.

You can use the default VLAN and native VLANs as a source VLAN. You cannot configure the dedicated VLAN used to transport mirrored traffic as a source VLAN.

A destination port for remote port mirroring cannot be used as a source port, including the session in which the port functions as the destination port. A source port channel or source VLAN, which has a member port that is configured as a destination port, cannot be used as a source port channel or source VLAN.

You can use ACLs on a source port. In a flow-based source session, packets sent from the RPM are not monitored.

Rate-limiting tagged-VLAN egress traffic on a source port is supported.

To delete one or more monitored ports from a source session, enter the complete no source (remote port mirroring) command.

The dedicated L2 VLAN used for remote port mirroring is configured with the mode remote-port-mirroring command. To change the reserved VLAN used in a source session, you can remove the current VLAN by entering the no source destination vlan vlan-id command. Then re-enter the complete source (remote port mirroring) command as described above to configure a new reserved VLAN for the source session.
source remote vlan (remote port mirroring)

Associate the reserved L2 VLAN used to transport mirrored traffic in remote port mirroring with a destination session and configure the destination ports to which an analyzer is connected.

**Syntax**

```plaintext
source remote vlan vlan-id destination {single-interface | range {interface-list | interface-range | mixed-interface-list}}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vlan-id</strong></td>
<td>VLAN ID of the reserved L2 VLAN used for remote port mirroring. Valid VLAN IDs are 1 to 4094. The default VLAN ID is not supported.</td>
</tr>
</tbody>
</table>

**single-interface**

Specifies one of the following interface types:
- 1-Gigabit Ethernet: Enter `gigabitethernet slot/port`.
- 10-Gigabit Ethernet: Enter `tengigabitethernet slot/port`.

**range interface-list**

Specifies multiple interfaces separated by a comma and space:
- `single-interface, single-interface, single-interface`

For example:
```
source remote-vlan 4 destination range gig 1/2, tengig 3/4
```

**range interface-range**

Specifies one of the following interface ranges:
- `gigabitethernet slot/first_port - last_port`
- `tengigabitethernet slot/first_port - last_port`

A space is required before and after the dash (-).

For example:
```
source remote-vlan 4 destination range gig 1/2 - 4
```

**range mixed-interface-list**

Specifies single interfaces and interface ranges in any order:
- `single-interface, interface-range, single-interface`

For example:
```
source remote-vlan 4 destination range gig 3/4 - 5, tengig 1/0
```

**Defaults**

No default behavior or values

**Command Modes**

MONITOR SESSION (conf-mon-sess-session-ID)

**Command History**

Version 8.4.1.2 Introduced on the E-Series ExaScale.

**Example**

**Figure 44-6. Command Example: Associating the Reserved VLAN with a Destination Session**

```
FTOS(conf-mon-sess-11)#source remote vlan 10 destination gigabitethernet 10/0 - 2
FTOS(conf-mon-sess-11)#
```
Usage Information

You can configure any port as a destination port. You cannot configure a VLAN, port-channel, or SONET interface as a destination port.

You can configure additional destination ports in an active session.

You can tunnel the mirrored traffic from multiple remote-port source sessions to the same destination port.

You can configure a destination port to send only tagged or untagged traffic to the analyzer. By default, the port sends untagged packets so that the reserved VLAN ID is removed and the original monitored packet is analyzed.

By default, ingress traffic on a destination port is dropped.

A destination port for remote port mirroring cannot be used as a source port, including the session in which the port functions as the destination port.

A destination port cannot be used in any spanning tree instance.

The dedicated L2 VLAN used for remote port mirroring is configured with the mode remote-port-mirroring command.

To delete one or more destination ports from a destination session, enter the no source remote vlan (remote port mirroring) command.

To change the reserved VLAN used in the destination session, you must first remove all destination ports. Then delete the current VLAN by entering the no monitor session source remote vlan (remote port mirroring) command and re-enter the monitor session source remote vlan (remote port mirroring) command to configure the new VLAN ID.

tagged destination

Configure destination ports for remote port mirroring so that the reserved VLAN tag is added to mirrored traffic sent to an analyzer.

Syntax

tagged destination {single-interface | range interface-range}

Parameters

| single-interface | Specifies one of the following interface types:  
|                  | • 1-Gigabit Ethernet: Enter gigabitethernet slot/port.  
|                  | • 10-Gigabit Ethernet: Enter tengigabitethernet slot/port.  

| range interface-range | Specifies one of the following interface ranges:  
|                       | • gigabitethernet slot/first_port - last_port  
|                       | • tengigabitethernet slot/first_port - last_port  
|                       | A space is required before and after the dash (-).  
|                       | For example:  
|                       | tagged destination range gigabitethernet 1/2 - 4

Defaults

Destination ports send untagged packets to an analyzer so that the reserved VLAN ID is removed and the original monitored packet is mirrored.

Command Modes

MONITOR SESSION (conf-mon-sess-session-ID)
To reconfigure destination ports in a remote-port mirroring session as untagged ports, enter the `untagged destination` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>untagged destination</code></td>
<td>Configure destination ports to remove the reserved VLAN tag from mirrored traffic.</td>
</tr>
</tbody>
</table>

**Syntax**

```
untagged destination {single-interface | range interface-range}
```

**Parameters**

- **single-interface**
  - Specifies one of the following interface types:
    - 1-Gigabit Ethernet: Enter `gigabitethernet slot/port`.
    - 10-Gigabit Ethernet: Enter `tengigabitethernet slot/port`.

- **range interface-range**
  - Specifies one of the following interface ranges:
    - `gigabitethernet slot/first_port - last_port`
    - `tengigabitethernet slot/first_port - last_port`
  - A space is required before and after the dash (-).
  - For example:
    - `untagged destination range gigabitethernet 1/2 - 4`

**Defaults**

Destination ports send untagged packets to an analyzer so that the reserved VLAN ID is removed and the original monitored packet is mirrored.

**Command Modes**

MONITOR SESSION (conf-mon-sess-session-ID)
Private VLAN (PVLVAN)

Overview

Starting with Dell Networking OS 7.8.1.0, the Private VLAN (PVLVAN) feature of Dell Networking OS is available for the C-Series and S-Series:

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

See also the following commands. The command output is augmented in Dell Networking OS 7.8.1.0 to provide PVLVAN data:

- show arp in Chapter 24, IPv4 Routing
- show vlan in Chapter 30, Layer 2

Private VLANs extend the Dell Networking OS 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 Dell Networking OS 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 the 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 the 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
private-vlan mode

Set the 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 syntax.

Parameters

- **community**: Enter `community` to set the VLAN as a community VLAN, as described above.
- **isolated**: Enter `isolated` to configure the VLAN as an isolated VLAN, as described above.
- **primary**: Enter `primary` to configure the VLAN as a primary VLAN, as described above.

Defaults

none

Command Modes

INTERFACE VLAN

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.

Related Commands

- **private-vlan mapping secondary-vlan**: Set the mode of the selected VLAN to primary and then associate secondary VLANs to it.
- **show interfaces private-vlan**: Display type and status of PVLAN interfaces.
- **show vlan private-vlan**: Display PVLANs and/or interfaces that are part of a PVLAN.
private-vlan mapping secondary-vlan

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 syntax.

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 7.8.1.0 Introduced on C-Series and S-Series

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: Set the mode of the selected VLAN to community, isolated, or primary.
- show interfaces private-vlan: Display type and status of PVLAN interfaces.
- show vlan private-vlan: Display all PVLANs and/or interfaces that are part of a PVLAN.
- show vlan private-vlan mapping: Display primary-secondary VLAN mapping.
- switchport mode private-vlan: Set 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. Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number:
  - C-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- 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 the VLAN ID. The VLAN ID range is from 1 to 4094.

Defaults

`none`

Command Modes

- EXEC
- EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
</tbody>
</table>

Usage Information

This command has two types of display — a list of all PVLAN interfaces or for a specific interface. Examples of both types of output are shown below.

Examples

**Figure 45-1. show interfaces private-vlan Command Output**

```
FTOS# show interfaces private-vlan
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
Gi 2/1  10 Primary    Promiscuous  Up
Gi 2/2 100 Isolated  Host        Down
Gi 2/3 10 Primary    Trunk        Up
Gi 2/4 101 Community  Host        Up
```

```
FTOS# show interfaces private-vlan Gi 2/2
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
Gi 2/2 100 Isolated  Host        Up
```

The table, below, defines the fields in the output, above.

**Table 45-1. 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>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>
</tbody>
</table>
show vlan private-vlan

Display PVLANs and/or interfaces that are part of a PVLAN.

Syntax

```
show vlan private-vlan [community | interface | isolated | primary | primary_vlan | interface interface]
```

Parameters

- **community**: (OPTIONAL) Enter the keyword `community` to display VLANs configured as community VLANs, along with their interfaces.
- **interface**: (OPTIONAL) Enter the keyword `community` to display VLANs configured as community VLANs, along with their interfaces.
- **isolated**: (OPTIONAL) Enter the keyword `isolated` to display VLANs configured as isolated VLANs, along with their interfaces.
- **primary**: (OPTIONAL) Enter the keyword `primary` to display VLANs configured as primary VLANs, along with their interfaces.
- **primary_vlan**: (OPTIONAL) Enter a private VLAN ID or secondary VLAN ID to display interface details about the designated PVLAN.
- **interface interface**: (OPTIONAL) Enter the keyword `interface` and an interface ID to display the PVLAN configuration of the designated interface. Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **C-Series**: Range: 1-128
    - **E-Series**: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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 the VLAN ID. The VLAN ID range is from 1 to 4094.

Defaults

- none

Command Modes

- EXEC
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
</tbody>
</table>

**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 45-2. show vlan private-vlan Command Output**

```
FTOS# show vlan private-vlan
Primary  Secondary  Type      Active Ports
--------  ---------  ---------  --------------------
10        primary   Yes   Gi 2/1,3
100       isolated  Yes   Gi 2/2
101       community Yes  Gi 2/10
20        primary   Yes   Po 10, 12-13
            Gi 3/1
200       isolated  Yes   Gi 3/2,4-6
201       community No
202       community Yes  Gi 3/11-12
```

```
FTOS# show vlan private-vlan primary
Primary  Secondary  Type      Active Ports
--------  ---------  ---------  --------------------
10        primary   Yes   Gi 2/1,3
20        primary   Yes   Gi 3/1,3
```

```
FTOS# show vlan private-vlan isolated
Primary  Secondary  Type      Active Ports
--------  ---------  ---------  --------------------
10        primary   Yes   Gi 2/1,3
100       isolated  Yes   Gi 2/2,4-6
200       isolated  Yes   Gi 3/2,4-6
```

```
FTOS# show vlan private-vlan community
Primary  Secondary  Type      Active Ports
--------  ---------  ---------  --------------------
10        primary   Yes   Gi 2/1,3
101       community Yes  Gi 2/7-10
20        primary   Yes   Po 10, 12-13
            Gi 3/1
201       community No
202       community Yes  Gi 3/11-12
```

```
FTOS# show vlan private-vlan interface Gi 2/1
Primary  Secondary  Type      Active Ports
--------  ---------  ---------  --------------------
10        primary   Yes   Gi 2/1
```

If the VLAN ID is that of a primary VLAN, then the entire private VLAN output will be displayed, as shown in **Figure 45-3**. 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 45-4**.
Figure 45-3. Output of show vlan private-vlan (primary)

FTOS# show vlan private-vlan 10
Primary Secondary Type       Active Ports
---- ----------- ----------- ------------------------
10   primary    Yes  Gi 2/1,3
102  isolated   Yes  Gi 0/4
101  community  Yes  Gi 2/7-10

Figure 45-4. Output of show vlan private-vlan (secondary)

FTOS# show vlan private-vlan 102
Primary Secondary Type       Active Ports
---- ----------- ----------- ------------------------
10   primary    Yes  Gi 0/2
102  isolated   Yes  Gi 0/4

The table, below, defines the fields in the output, above.

Table 45-2. show interfaces description Command Example Fields

<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>

Related Commands

- `private-vlan mode` Set the mode of the selected VLAN to either community or isolated.
- `show interfaces private-vlan` Display type and status of PVLAN interfaces.
- `show vlan private-vlan mapping` Display primary-secondary VLAN mapping.
- `switchport mode private-vlan` Set the PVLAN mode of the selected port.

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 7.8.1.0 Introduced on C-Series and S-Series
```
The output of this command, shown below, displays the community and isolated VLAN IDs that are associated with each primary VLAN.

![Figure 45-5. show vlan private-vlan mapping Command Output](image)

```
FTOS# show vlan private-vlan mapping
Private Vlan:
    Primary  : 100
    Isolated  : 102
    Community : 101
    Unknown   : 200
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show-private-vlan mode</code></td>
<td>Set the mode of the selected VLAN to either community or isolated.</td>
</tr>
<tr>
<td><code>show interfaces private-vlan</code></td>
<td>Display type and status of PVLAN interfaces.</td>
</tr>
<tr>
<td><code>show vlan private-vlan mapping</code></td>
<td>Display primary-secondary VLAN mapping.</td>
</tr>
<tr>
<td><code>switchport mode private-vlan</code></td>
<td>Set the PVLAN mode of the selected port.</td>
</tr>
</tbody>
</table>

### switchport mode private-vlan

Set the 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 a 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 7.8.1.0**
  Introduced on C-Series and S-Series

**Usage Information**

The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is demonstrated below.
**Example**

**Figure 45-6. Examples of switchport mode private-vlan Command**

FTOS#conf
FTOS(conf)#interface GigabitEthernet 2/1
FTOS(conf-if-gi-2/1)#switchport mode private-vlan promiscuous

FTOS(conf)#interface GigabitEthernet 2/2
FTOS(conf-if-gi-2/2)#switchport mode private-vlan host

FTOS(conf)#interface GigabitEthernet 2/3
FTOS(conf-if-gi-2/3)#switchport mode private-vlan trunk

FTOS(conf)#interface port-channel 10
FTOS(conf-if-gi-2/3)#switchport mode private-vlan promiscuous

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>private-vlan mode</td>
<td>Set the mode of the selected VLAN to either community or isolated.</td>
</tr>
<tr>
<td>private-vlan mapping</td>
<td>Set the mode of the selected VLAN to primary and then associate secondary VLANs to it.</td>
</tr>
<tr>
<td>secondary-vlan</td>
<td></td>
</tr>
<tr>
<td>show interfaces private-vlan</td>
<td>Display type and status of PVLAN interfaces.</td>
</tr>
<tr>
<td>show vlan private-vlan mapping</td>
<td>Display primary-secondary VLAN mapping.</td>
</tr>
</tbody>
</table>
Per-VLAN Spanning Tree plus (PVST+)

Overview

The Dell Networking OS 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.

PVST+ (Per-VLAN Spanning Tree plus) is supported by Dell Networking OS on all Dell Networking systems, as indicated by the characters that appear below each command heading:

- C-Series: C
- E-Series: E
- S-Series: S

Commands

The Dell Networking OS PVST+ commands are:

- disable
- description
- extend system-id
- 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

Syntax: disable

Disable PVST+ globally.
To enable PVST+, enter `no disable`.

**Defaults**
PVST+ is disabled

**Command Modes**
CONFIGURATION (conf-pvst)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol spanning-tree pvst</td>
<td>Enter PVST+ mode.</td>
</tr>
</tbody>
</table>

### description

Enter a description of the PVST+

**Syntax**

description `{description}`

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

**Parameters**

- `{description}`: Enter a description to identify the Spanning Tree (80 characters maximum).

**Defaults**
No default behavior or values

**Command Modes**
SPANNING TREE PVST+ (The prompt is “config-pvst”.)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre-7.7.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol spanning-tree pvst</td>
<td>Enter SPANNING TREE mode on the switch.</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 on 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example

FTOS(conf-pvst)#do show spanning-tree pvst vlan 5 brief

VLAN 5
Executing IEEE compatible Spanning Tree Protocol
Root ID  Priority 32773, Address 0001.e832.73f7
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32773 (priority 32768 sys-id-ext 5), Address 0001.e832.73f7
We are the root of Vlan 5
Configured hello time 2, max age 20, forward delay 15

Interface                                          Designated
Name      PortID   Prio Cost    Sts Cost        Bridge ID        PortID
---------- -------- ---- ------  --- ------- -------------------- --------
Gi 0/10    128.140  128  200000  FWD 0       32773 0001.e832.73f7  128.140
Gi 0/12    128.142  128  200000  DIS 0       32773 0001.e832.73f7  128.142

Interface
Name      Role   PortID   Prio Cost    Sts Cost    Link-type Edge
---------- ------ -------- ---- ------- --- ------- --------- ------------------------
Gi 0/10    Desg   128.140  128  200000  FWD 0       P2P        No
Gi 0/12    Dis    128.142  128  200000  DIS 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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

```
Figure 46-1. 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)#
FTOS(conf-pvst)#show config
!
protocol spanning-tree pvst
  no disable
  vlan 2 bridge-priority 4096
  vlan 3 bridge-priority 16384
FTOS#
```

**Usage Information**

Once PVST+ is enabled, the device runs an STP instance for each VLAN it supports.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disable PVST+.</td>
</tr>
<tr>
<td>show spanning-tree pvst</td>
<td>Display the PVST+ configuration.</td>
</tr>
</tbody>
</table>
show spanning-tree pvst

View the Per-VLAN Spanning Tree configuration.

**Syntax**

show spanning-tree pvst [vlan vlan-id] [brief] [guard]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vlan vlan-id</strong></td>
<td>(OPTIONAL) Enter the keyword vlan followed by the VLAN ID. Range: 1 to 4094</td>
</tr>
<tr>
<td><strong>brief</strong></td>
<td>(OPTIONAL) Enter the keyword brief to view a synopsis of the PVST+ configuration information.</td>
</tr>
</tbody>
</table>
| **Interface** | (OPTIONAL) Enter one of the interface keywords along with the slot/port information:  
  - For a Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.  
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.  
  - For a Port Channel interface, enter the keyword port-channel followed by a number:  
    - C-Series and S-Series Range: 1-128  
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.  
  - 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 8.4.6.0 Added support for the keyword fortyGigE.
- Version 8.5.1.0 Support for the optional guard keyword was added on the E-Series ExaScale.
- Version 8.4.2.1 Support for the optional guard keyword was added on the C-Series, S-Series, and E-Series TeraScale.
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 6.4.1.0 Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency and Port VLAN ID inconsistency.
- Version 6.2.1.1 Introduced
Example 1

**Figure 46-2. show spanning-tree pvst brief Command**

```
FTOS#show spanning-tree pvst vlan 3 brief
VLAN 3
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 4096, Address 0001.e801.6a83
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15

Interface Name PortID Prio Cost Sts Cost Bridge ID PortID
---------- -------- ---- ------  --- ------- -------------------- --------
Gi 1/0 128.130 128 20000 FWD 20000 4096 0001.e801.6a83 128.426
Gi 1/1 128.131 128 20000 BLK 20000 4096 0001.e801.6a83 128.427
Gi 1/16 128.146 128 20000 FWD 20000 16384 0001.e805.e306 128.146
Gi 1/17 128.147 128 20000 FWD 20000 16384 0001.e805.e306 128.147
```

Example 2

**Figure 46-3. show spanning-tree pvst vlan Command**

```
FTOS#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 4096, Address 0001.e805.e306
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 4096, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15
We are the root of VLAN 2
Current root has priority 4096, Address 0001.e805.e306
Number of topology changes 3, last change occurred 00:57:00

Port 130 (GigabitEthernet 1/0) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.130
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.130, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 3
The port is not in the Edge port mode

Port 131 (GigabitEthernet 1/1) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.131
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.131, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 0
The port is not in the Edge port mode

Port 146 (GigabitEthernet 1/16) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.146
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.146, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1578, received 0
The port is in the Edge port mode

Port 147 (GigabitEthernet 1/17) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.147
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.147, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1579, received 0
The port is in the Edge port mode
```
Example 3  Figure 46-4. show spanning-tree pvst command with EDS and LBK

FTOS#show spanning-tree pvst vlan 2 interface gigabitethernet 1/0
GigabitEthernet 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 guard :disable (default)
Bpdus sent 152, received 27562

<table>
<thead>
<tr>
<th>Interface</th>
<th>Designated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>PortID</td>
</tr>
<tr>
<td>Gi 1/0</td>
<td>128.1223</td>
</tr>
</tbody>
</table>

Example 4  Figure 46-5. show spanning-tree pvst with EDS and PVID

FTOS#show spanning-tree pvst vlan 2 interface gigabitethernet 1/0
GigabitEthernet 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 (default)
Bpdus sent 1, received 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Designated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>PortID</td>
</tr>
<tr>
<td>Gi 1/0</td>
<td>128.1223</td>
</tr>
</tbody>
</table>

Example 5  Figure 46-6. show spanning-tree pvst guard Command

FTOS#show spanning-tree pvst vlan 5 guard
Interface
Name       | Instance | Sts        | Guard type |
-----------|----------|------------|------------|
Gi 0/1     | 5        | INCON(Root)| Rootguard  |
Gi 0/2     | 5        | FWD        | Loopguard  |
Gi 0/3     | 5        | EDS(Shut)  | Bpduguard  |

Table 46-1. 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>

Related Commands

spanning-tree pvst Configure PVST+ on an interface.
spanning-tree pvst

Configure a PVST+ interface with one of these settings: edge port with optional Bridge Port Data Unit (BPDU) guard, port disablement if an error condition occurs, port priority or cost for a VLAN range, loop guard, or root guard.

**Syntax**

```
spanning-tree pvst {edge-port [bpduguard [shutdown-on-violation]]} | err-disable | vlan vlan-range {cost number | priority value} | loopguard | rootguard
```

**Parameters**

- **edge-port**
  - Enter the keyword `edge-port` to configure the interface as a PVST+ edge port.

- **bpduguard**
  - Enter the keyword `portfast` to enable Portfast 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.

- **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.

- **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 200000
  - Defaults:
    - 100 Mb/s Ethernet interface = 200000
    - 1-Gigabit Ethernet interface = 20000
    - 10-Gigabit Ethernet interface = 2000
    - 40-Gigabit Ethernet interface = 1400
    - Port Channel interface with one 100 Mb/s Ethernet = 200000
    - Port Channel interface with one 1-Gigabit Ethernet = 20000
    - Port Channel interface with one 10-Gigabit Ethernet = 2000
    - Port Channel with two 1-Gigabit Ethernet = 18000
    - Port Channel with two 10-Gigabit Ethernet = 1800
    - Port Channel with two 100-Mbps Ethernet = 180000

- **priority value**
  - Enter the keyword `priority` followed the Port priority value in increments of 16.
  - Range: 0 to 240. Default: 128

- **loopguard**
  - Enter the keyword `loopguard` to enable loop guard on a PVST+ port or port-channel interface.

- **rootguard**
  - Enter the keyword `rootguard` to enable root guard on a PVST+ port or port-channel interface.

**Defaults**

Not Configured

**Command Modes**

INTERFACE
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.

If `shutdown-on-violation` is not enabled, BPDUs will still be sent to the RPM CPU.

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 a PVST+ network, loop guard is performed per-port or per-port channel at a VLAN level. If no BPDUs are received on a VLAN interface, the port or port-channel transitions to a loop-inconsistent (blocking) state only for this VLAN.

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 46-7. spanning-tree pvst vlan Command Example**

```
FTOS(conf-if-gi-1/1)#spanning-tree pvst vlan 3 cost 18000
FTOS(conf-if-gi-1/1)#end
FTOS(conf-if-gi-1/1)#show config
!
interface GigabitEthernet 1/1
 no ip address
 switchport
 spanning-tree pvst vlan 3 cost 18000
 no shutdown
FTOS(conf-if-gi-1/1)#end
FTOS#
```

### Related Commands

- `show spanning-tree pvst` View PVST+ configuration
spanning-tree pvst err-disable

Place ports in an err-disabled state if they receive a PVST+ BPDU when they are members an untagged VLAN.

Syntax

```
spanning-tree pvst err-disable cause invalid-pvst-bpdu
```

Defaults

Enabled; ports are placed in err-disabled state if they receive a PVST+ BPDU when they are members of an untagged VLAN.

Command Modes

- INTERFACE

Command History

```
Version 8.2.1.0 Introduced
```

Usage Information

Some non-Dell Networking systems that have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU.

Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, Dell Networking OS places the port in error-disable state. This behavior might result in the network not converging. To prevent Dell Networking OS from executing this action, use the command

```
no spanning-tree pvst err-disable cause invalid-pvst-bpdu
```

Related Commands

- show spanning-tree pvst

---

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 7.6.1.0 Support added for S-Series
Version 7.5.1.0 Support added for C-Series
Version 6.5.1.0 Introduced
```

Usage Information

By default Dell Networking OS 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.
Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

**Syntax**

```
vlan vlan-range 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 7.6.1.0: Support added for S-Series
- Version 7.5.1.0: Support added for C-Series
- Version 6.2.1.1: Introduced

**Related Commands**

- `vlan forward-delay` Change the time interval before Dell Networking OS transitions to the forwarding state
- `vlan hello-time` Change the time interval between BPDUs
- `vlan max-age` Change the time interval before PVST+ refreshes
- `show spanning-tree pvst` Display the PVST+ configuration
**vlan forward-delay**

Set the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

**Syntax**

```
vlan vlan-range 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 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 6.2.1.1 Introduced

**Related Commands**

- `vlan bridge-priority` Set the bridge-priority value
- `vlan hello-time` Change the time interval between BPDUs
- `vlan max-age` Change the time interval before PVST+ refreshes
- `show spanning-tree pvst` Display the PVST+ configuration
**vlan hello-time**

Set the time interval between generation of PVST+ Bridge Protocol Data Units (BPDUs).

**Syntax**

`vlan vlan-range 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 7.6.1.0** Support added for S-Series
- **Version 7.5.1.0** Support added for C-Series
- **Version 6.2.1.1** Introduced

**Related Commands**

- `vlan bridge-priority` Set the bridge-priority value
- `vlan forward-delay` Change the time interval before Dell Networking OS transitions to the forwarding state
- `vlan max-age` Change the time interval before PVST+ refreshes
- `show spanning-tree pvst` Display the PVST+ configuration
**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 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 6.2.1.1 Introduced

**Related Commands**

- `vlan bridge-priority` Set the bridge-priority value
- `vlan forward-delay` Change the time interval before Dell Networking OS 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

Dell Networking OS commands for Quality of Service (QoS) include traffic conditioning and congestion control. QoS commands are not universally supported on all Dell Networking platforms. Support is indicated by the [ ] and [ ] characters under command headings.

This chapter contains the following sections:

- Global Configuration Commands
- Per-Port QoS Commands
- Policy-Based QoS Commands
- Queue-Level Debugging (E-Series Only)

Global Configuration Commands

- qos-rate-adjust

qos-rate-adjust

By default, while rate limiting, policing, and shaping, Dell Networking OS 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 limiting, policing, and shaping calculations.

  C-Series and S-Series Range: 1-31
  E-Series Range: 1-144

Defaults: QoS Rate Adjustment is disabled by default, and no qos-rate-adjust is listed in the running-configuration

Command Modes: CONFIGURATION

Command History:

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
Per-Port QoS Commands

Per-port QoS ("port-based QoS") allows users to define QoS configuration on a per-physical-port basis. The commands include:

- dot1p-priority
- rate limit
- rate police
- rate shape
- service-class dynamic dot1p
- show interfaces rate
- strict-priority queue

**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, enter `no dot1p-priority`.

**Parameters**

<table>
<thead>
<tr>
<th>priority-value</th>
<th>dot1p</th>
<th>Queue Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

For the C-Series and S-Series, enter a value 0, 2, 4, or 6

<table>
<thead>
<tr>
<th>dot1p</th>
<th>Queue Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</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>2</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>E-Series</td>
</tr>
</tbody>
</table>
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 a `dot1p-priority` command to individual interfaces in a Port Channel.

**rate limit**

Limit the outgoing traffic rate on the selected interface.

**Syntax**

```
rate limit [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]
```

**Parameters**

- **kbps**
  - Enter this keyword to specify the rate limit in Kilobits per second (Kbps). On the E-Series, Dell Networking recommends using a value greater than or equal to 512 as lower values does not yield accurate results. The default granularity is Megabits per second (Mbps).
  - Range: 0 to 10000000
- **committed-rate**
  - Enter the bandwidth in Mbps
  - Range: 0 to 10000
- **burst-KB**
  - (OPTIONAL) Enter 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 limit 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 Modes**

INTERFACE

**Command History**

- Version 8.2.1.0 Added `kbps` option on E-Series.
- Version 7.7.1.0 Removed from C-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.1.1.1 Introduced on E-Series

**Usage Information**

- **Note:** Per Port rate limit and rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate limit and rate police is supported on only tagged ports with Layer 2 switched traffic.

On one interface, you can configure the `rate limit` or `rate police` command for a VLAN or you can configure the `rate limit` or the `rate police` command for the interface. For each physical interface, you can configure six `rate limit` commands specifying different VLANS.
If you receive the error message:

```
%Error: Specified VLANs overlap with existing config.
```

after configuring VLANs in the `rate police` command, check to see if the same VLANs are used in `rate limit` command on other interfaces. To clear the problem, remove the `rate limit` configuration(s), and re-configure the `rate police` command. After the `rate police` command is configured, return to the other interfaces and re-apply the `rate limit` configuration.

**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 limit in Kilobits per second (Kbps). On C-Series and S-Series make the following value a multiple of 64. On the E-Series, Dell Networking recommends using a value greater than or equal to 512 as lower values does not yield accurate results. The default granularity is Megabits per second (Mbps).
    - Range: 0 to 10000000
  - **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

- **Command History**
  
<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Added <code>kbps</code> option on C-Series, E-Series, and Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

- **Usage Information**

  - **Note:** Per Port rate limit and rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate limit and rate police is supported on only tagged ports with Layer 2 switched traffic.
C-Series and S-Series

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.

E-Series

On one interface, you can configure the rate limit or rate police command for a VLAN or you can configure the rate limit or the rate police command for the interface.

For each physical interface, you can configure six 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.

Check to see if the same VLANS are used with the rate limit command on other interfaces. To clear the problem, remove the rate limit configuration(s), and re-configure the rate police command. After the rate police command is configured, return to the other interfaces and re-apply the rate limit configuration.

Related Commands

rate-police Police traffic output as part of the designated policy.

rate shape

Shape the traffic output on the selected interface.

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 C-Series and S-Series make the following value a multiple of 64. The default granularity is Megabits per second (Mbps). Range: 0-10000000</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: 10</td>
</tr>
</tbody>
</table>

Defaults

Granularity for rate is Mbps unless the kbps option is used.

Command Modes

INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added kbps option on C-Series, E-Series, and Series.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Time: 1195</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series and on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

On 40-port 10G line cards, if the traffic is shaped between 64 and 1000kbs, for some values the shaped rate is much less than the value configured. Do not use values in this range for 10G interfaces.
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, enter `no service-class dynamic dot1p`.

**Defaults**

All dot1p traffic is mapped to Queue 0 unless `service-class dynamic dot1p` is enabled. Then the default mapping is as follows:

<table>
<thead>
<tr>
<th>dot1p</th>
<th>E-Series Queue ID</th>
<th>C-Series Queue ID</th>
<th>S-Series Queue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Command Modes**

- **INTERFACE**
- **CONFIGURATION** (C-Series and S-Series only)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Available globally on the C-Series and S-Series so that the configuration applies to all ports.</td>
<td></td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
<td></td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Expanded command to permit configuration on port channels</td>
<td></td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Information**

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 C-Series and S-Series 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.

```
On the C-Series and S-Series 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-weight**

Specify a minimum bandwidth for queues

**Syntax**

```
service-class bandwidth-weight queue0 number queue1 number queue2 number queue3 number
```

**Parameters**

- `number`: Enter the bandwidth-weight. The value must be a power of 2.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

Version 8.2.1.0 Introduced on C-Series and S-Series.

**Usage Information**

Guarantee a minimum bandwidth to different queues globally using the command `service-class bandwidth-weight` from CONFIGURATION mode. The command is applied in the same way as the `bandwidth-weight` command in an output QoS policy. The `bandwidth-weight` command in QOS-POLICY-OUT mode supersedes the `service-class bandwidth-weight` command.

**show interfaces rate**

Display information of either rate limiting or rate policing on the interface.

**Syntax**

```
show interfaces [interface] rate [limit | police]
```

**Parameters**

- `interface`: (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

- `limit`: (OPTIONAL) Enter the keyword `limit` to view the outgoing traffic rate.

- `police`: (OPTIONAL) Enter the keyword `police` to view the incoming traffic rate.
Command Mode
- EXEC
- EXEC Privilege

Command History
- pre-Version 6.1.1.1 Introduced on E-Series

Example

**Figure 47-1. show interfaces rate limit Command Example**

```
FTOS#show interfaces gigabitEthernet 1/1 rate limit
Rate limit 300 (50) peak 800 (50)
  Traffic Monitor 0: normal 300 (50) peak 800 (50)
    Out of profile yellow 23386960 red 320605113
  Traffic Monitor 1: normal NA peak NA
    Out of profile yellow 0 red 0
  Traffic Monitor 2: normal NA peak NA
    Out of profile yellow 0 red 0
  Traffic Monitor 3: normal NA peak NA
    Out of profile yellow 0 red 0
  Traffic Monitor 4: normal NA peak NA
    Out of profile yellow 0 red 0
  Traffic Monitor 5: normal NA peak NA
    Out of profile yellow 0 red 0
  Traffic Monitor 6: normal NA peak NA
    Out of profile yellow 0 red 0
  Traffic Monitor 7: normal NA peak NA
    Out of profile yellow 0 red 0
Total: yellow 23386960 red 320605113
```

**Table 47-2. show interfaces Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate limit</td>
<td>Committed rate (Mbs) and burst size (KB) of the committed rate</td>
</tr>
<tr>
<td>peak</td>
<td>Peak rate (Mbs) and burst size (KB) of the peak rate</td>
</tr>
<tr>
<td>Traffic monitor 0</td>
<td>Traffic coming to class 0</td>
</tr>
<tr>
<td>Normal</td>
<td>Committed rate (Mbs) and burst size (KB) of the committed rate</td>
</tr>
<tr>
<td>peak</td>
<td>Peak rate (Mbs) and burst size (KB) of the peak rate</td>
</tr>
<tr>
<td>Out of profile yellow</td>
<td>Number of packets that have exceeded the configured committed rate</td>
</tr>
<tr>
<td>Out of profile Red</td>
<td>Number of packets that have exceeded the configured peak rate</td>
</tr>
<tr>
<td>Traffic monitor 1</td>
<td>Traffic coming to class 1</td>
</tr>
<tr>
<td>Traffic monitor 2</td>
<td>Traffic coming to class 2</td>
</tr>
<tr>
<td>Traffic monitor 3</td>
<td>Traffic coming to class 3</td>
</tr>
<tr>
<td>Traffic monitor 4</td>
<td>Traffic coming to class 4</td>
</tr>
<tr>
<td>Traffic monitor 5</td>
<td>Traffic coming to class 5</td>
</tr>
<tr>
<td>Traffic monitor 6</td>
<td>Traffic coming to class 6</td>
</tr>
<tr>
<td>Traffic monitor 7</td>
<td>Traffic coming to class 7</td>
</tr>
<tr>
<td>Total: yellow</td>
<td>Total number of packets that have exceeded the configured committed rate</td>
</tr>
<tr>
<td>Total: red</td>
<td>Total number of packets that have exceeded the configured peak rate</td>
</tr>
</tbody>
</table>
**Table 47-3. show interfaces police Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate police</td>
<td>Committed rate (Mbs) and burst size (KB) of the committed rate</td>
</tr>
<tr>
<td>peak</td>
<td>Peak rate (Mbs) and burst size (KB) of the peak rate</td>
</tr>
<tr>
<td>Traffic monitor 0</td>
<td>Traffic coming to class 0</td>
</tr>
<tr>
<td>Normal</td>
<td>Committed rate (Mbs) and burst size (KB) of the committed rate</td>
</tr>
<tr>
<td>peak</td>
<td>Peak rate (Mbs) and burst size (KB) of the peak rate</td>
</tr>
<tr>
<td>Out of profile Yellow</td>
<td>Number of packets that have exceeded the configured committed rate</td>
</tr>
<tr>
<td>Out of profile Red</td>
<td>Number of packets that have exceeded the configured peak rate</td>
</tr>
<tr>
<td>Traffic monitor 1</td>
<td>Traffic coming to class 1</td>
</tr>
<tr>
<td>Traffic monitor 2</td>
<td>Traffic coming to class 2</td>
</tr>
<tr>
<td>Traffic monitor 3</td>
<td>Traffic coming to class 3</td>
</tr>
<tr>
<td>Traffic monitor 4</td>
<td>Traffic coming to class 4</td>
</tr>
<tr>
<td>Traffic monitor 5</td>
<td>Traffic coming to class 5</td>
</tr>
<tr>
<td>Traffic monitor 6</td>
<td>Traffic coming to class 6</td>
</tr>
<tr>
<td>Traffic monitor 7</td>
<td>Traffic coming to class 7</td>
</tr>
<tr>
<td>Total: yellow</td>
<td>Total number of packets that have exceeded the configured committed rate</td>
</tr>
<tr>
<td>Total: red</td>
<td>Total number of packets that have exceeded the configured peak rate</td>
</tr>
</tbody>
</table>

**strict-priority queue**

Configure a unicast queue as a strict-priority (SP) queue.

**Syntax**

```
strict-priority queue unicast number
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unicast</td>
<td>Enter the keyword <code>unicast</code> followed by the queue number.</td>
</tr>
</tbody>
</table>

**C-Series and S-Series**

Range: 1 to 3

**E-Series**

Range: 1 to 7
### Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of eight classes in E-Series and one of four classes in C-Series and S-Series. Dell Networking OS 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-weight`
- `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`
- `queue backplane ignore-backpressure`
- `queue egress`
- `queue ingress`
- `rate-limit`
- `rate-police`
- `rate-shape`
- `service-policy input`
- `service-policy output`
- `service-queue`
- `set`
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: 0 to 100% (granularity 1%)

Defaults

No default behavior or values

Command Modes

- **CONFIGURATION (conf-qos-policy-out)**

Command History

- **Version 6.2.1.1** Introduced on E-Series

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 eight classes exceeds 100%, the bandwidth percentage will automatically scale down to 100%.

Related Commands

- `qos-policy-output` Create a QoS output policy.

bandwidth-weight

Assign a priority weight to a queue.

Syntax

```
bandwidth-weight weight
```

To remove the bandwidth weight, use the `no bandwidth-weight` command.
### Parameters

| **weight** | Enter the weight assignment to queue.  
Range: 1 to 1024 (in increments of powers of 2: 2, 4, 8, 16, 32, 64, 128, 256, 512, or 1024).  
The weight values 2, 4, 8 and 16 are treated as the same weight for the following line card types: EX6QB and EX16TB. |

### Defaults

No default behavior or values

### Command Modes

**CONFIGURATION (conf-qos-policy-out)**

### Command History

| Version 7.7.1.0 | Introduced on S-Series |
| Version 7.6.1.0 | Introduced on C-Series |

### Usage Information

This command provides a minimum bandwidth guarantee to traffic flows in a particular queue. The minimum bandwidth is provided by scheduling packets from that queue a certain number of times relative to scheduling packets from the other queues using the Deficit Round Robin method.

### Related Commands

| **qos-policy-output** | Create 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 8.2.1.0 | Class-map names can be 32 characters. **layer2** available on C-Series and S-Series. |
| Version 7.6.1.0 | Introduced on S-Series |
| Version 7.5.1.0 | Introduced on C-Series |
| Version 7.4.1.0 | E-Series Only: Expanded to add support for Layer 2 |
Usage Information

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>clear qos statistics</code></td>
<td>Clears Matched Packets, Matched Bytes, and Dropped Packets. For TeraScale, clears Matched Packets, Matched Bytes, Queued Packets, Queued Bytes, and Dropped Packets.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td><code>clear qos statistics interface-name</code>.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td><code>interface-name</code> Enter one of the following keywords:</td>
</tr>
<tr>
<td></td>
<td>- For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For 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**          | No default behavior or values                                               |
| **Command Modes**     | EXEC, EXEC Privilege                                                        |
| **Command History**   | Version 8.4.6.0 Added support for the keyword `fortyGigE`.                  |
|                       | Version 7.6.1.0 Introduced on S-Series                                      |
|                       | Version 7.5.1.0 Introduced on C-Series                                      |
|                       | pre-Version 6.1.1.1 Introduced on E-Series                                 |
Usage Information

E-Series Only Behavior

If a Policy QoS is applied on an interface when clear qos statistics is issued, it will clear the egress counters in show queue statistics and vice versa. This behavior is due to the values being read from the same hardware registers.

The clear qos statistics command clears both the queued and matched byte and packet counters if the queued counters incremented based on classification of packets to the queues because of policy-based QoS. If the queued counters were incremented because of some other reason and do not reflect a matching QoS entry in CAM, then this command clears the matched byte and packet counters only.

Related Commands

show qos statistics Display qos statistics.

match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

Syntax

match ip access-group access-group-name [set-ip-dscp value]

To remove ACL match criteria from a class map, enter no match ip access-group access-group-name [set-ip-dscp value] command.

Parameters

access-group-name Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class specified by class-map.

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

No default behavior or values

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

Version 7.7.1.0 Added DSCP Marking option support on S-Series
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
Version 7.5.1.0 Added support for DSCP Marking option
pre-Version 6.1.1.1 Introduced on E-Series

Usage Information

You must enter the class-map command in order to access this command. Once 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

class-map Identify the class map.
### description

**Description:** Add a description to the selected policy map or QOS policy.

**Syntax:**
```
description {description}
```

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

**Parameters**
- `description`: Enter a description to identify the policies (80 characters maximum).

**Defaults**
No default behavior or values

**Command Modes**
CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)

**Command History**
- pre-Version 7.7.1.0: Introduced

**Related Commands**
- `policy-map-input`: Create an input policy map.
- `policy-map-output`: Create an output policy map.
- `qos-policy-input`: Create an input QOS-policy on the router.
- `qos-policy-output`: Create an output QOS-policy on the router.
- `wred-profile`: Create a WRED profile.

### match ip dscp

**Description:** Use a DSCP (Differentiated Services Code Point) value as a match criteria.

**Syntax:**
```
match ip dscp dscp-list [multicast set-ip-dscp value]
```

To remove a DSCP value as a match criteria, enter `no match ip dscp dscp-list [multicast set-ip-dscp value]` command.

**Parameters**
- `dscp-list`: Enter the IP DSCP value(s) that is to be the match criteria. Separate values by commas—no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3).
  - Range: 0 to 63
- `multicast`: (OPTIONAL) Enter the keyword `multicast` to match against multicast traffic.
  - **Note:** This option is not supported on C-Series or S-Series.
- `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
  - **Note:** This option is not supported on S-Series.

**Defaults**
No default behavior or values

**Command Modes**
CLASS-MAP CONFIGURATION (config-class-map)
You must enter the `class-map` command in order to access this command. Once 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.

```
match ip precedence
```

Use IP precedence values as a match criteria.

**Syntax**

```
match ip precedence ip-precedence-list [[multicast] set-ip-dscp value]
```

To remove IP precedence as a match criteria, enter `no match ip precedence ip-precedence-list [[multicast] set-ip-dscp value]` command.

**Parameters**

- **ip-precedence-list**
  - Enter the IP precedence value(s) as the match criteria. Separate values by commas—no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3).
  - Range: 0 to 7

- **multicast**
  - (OPTIONAL) Enter the keyword `multicast` to match against multicast traffic.
  - **Note:** This option is not supported on C-Series or S-Series.

- **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
  - **Note:** This option is not supported on S-Series.

**Defaults**

No default behavior or values

**Command Modes**

CLASS-MAP CONFIGURATION (conf-class-map)
You must enter the `class-map` command in order to access this command. Once 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` Identify the class map.

### match mac access-group

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

**Syntax**

```
match mac access-group {mac-acl-name}
```

**Parameters**

- `mac-acl-name` Enter a MAC ACL name. Its contents will be used as the match criteria in the class map.

**Defaults**

No default values or behavior

**Command Modes**

CLASS-MAP

**Command History**

- **Version 8.2.1.0** Available on the C-Series and S-Series.
- **Version 7.5.1.0** Added support for DSCP Marking option
- **Version 7.4.1.0** Introduced

**Usage Information**

You must enter the `class-map` command in order to access this command. Once the class map is identified, you can configure the match criteria.

**Related Commands**

- `class-map` Identify the class map.
### match mac dot1p

Configure a match criterion for a class map, based on a dot1p value.

**Syntax**

`match mac dot1p {dot1p-list}`

**Parameters**

- **dot1p-list**
  - Enter a dot1p value.
  - Range: 0–7

**Defaults**

No default values or behavior

**Command Modes**

CLASS-MAP

**Command History**

- Version 8.2.1.0: Available on the C-Series and S-Series.
- Version 7.5.1.0: Added support for DSCP Marking option
- Version 7.4.1.0: Introduced

**Usage Information**

You must enter the `class-map` command in order to access this command. Once the class map is identified, you can configure the match criteria.

**Related Commands**

- `class-map`: Identify the class map.

### match mac vlan

Configure a match criterion for a class map based on a VLAN ID.

**Syntax**

`match mac vlan {vlan-id | vlan-list | vlan-range | mixed-vlan-list}`

**Parameters**

- **vlan-id**
  - Enter the VLAN ID. Valid VLAN IDs are from 1 to 4094

- **vlan-list**
  - **S25 and S50 only**: Enter two or more VLAN IDs separated by a comma:
    `vlan-id,vlan-id,vlan-id,...`
  - For example: `match mac vlan 2,4,6`
  - There is no space between VLAN IDs and the comma.

- **vlan-range**
  - **S25 and S50 only**: Enter a range VLAN IDs separated by a dash (`-`):
    `vlan-id-vlan-id`
  - For example: `match mac vlan 3-5`
  - There is no space between VLAN IDs and the comma.

- **mixed-vlan-list**
  - **S25 and S50 only**: Enter single VLAN IDs and VLAN ranges in any order:
    `vlan-id,vlan-range,vlan-id...`
  - For example: `match mac vlan 1,3-5,8`

**Defaults**

None

**Command Modes**

CLASS-MAP

**Command History**

- Version 8.4.2.4: Support for multiple VLAN IDs as match criteria was introduced on the S25 and S50.
- Version 8.2.0.1: Introduced.
### Usage Information
You must first enter the **class-map** command in order to access this command. In a class map, you can match and classify traffic using a VLAN ID.

**Note:** The use of multiple VLAN IDs (VLAN list or range) as match criteria in a class map is supported only on the S25 and S50.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map</td>
<td>Create/access a class map.</td>
</tr>
</tbody>
</table>
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 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

No default behavior or values

Command Modes

CONFIGURATION (policy-map-input and policy-map-output)

Command History

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
<td>Policy name character limit increased from 16 to 32.</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

C-Series and S-Series

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 rate police configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.

E-Series

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 an aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) will apply. Any marking configurations in the aggregate input QoS policy will be ignored.

2. If an aggregate input QoS policy and a per-class input QoS policy co-exist, then the aggregate input QoS policy will preempt the per-class input QoS policy on input traffic conditioning (rate-police). In other words, if a rate police configuration exists in the aggregate QoS policy, the rate police configurations in the per-class QoS are ignored. Marking configurations in the per-class input QoS policy still apply to each queue.

3. If only an aggregate output QoS policy exists, egress traffic conditioning configurations (rate-limit and rate-shape) in the aggregate output QoS policy will apply. Scheduling and queuing configurations in the aggregate output QoS policy (if existing) are ignored. Each queue will use default scheduling and queuing configuration (Weighted Random Early Detection (WRED) and Bandwidth).

4. If the aggregate output QoS policy and per-queue output QoS policy co-exist, the aggregate output QoS policy will preempt a per-queue output QoS policy on egress traffic conditioning (rate-limit). In other words, if a rate limit configuration exists in the aggregate output QoS policy, the rate limit
configurations in per-queue output QoS policies are ignored. Scheduling and queuing configurations (WRED and Bandwidth) in the per-queue output QoS policy still apply to each queue.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy-map-input</strong></td>
<td>Create an input policy map</td>
</tr>
<tr>
<td><strong>policy-map-output</strong></td>
<td>Create an output policy map (E-Series Only)</td>
</tr>
</tbody>
</table>

#### 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 8.2.1.0 Policy name character limit increased from 16 to 32.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 7.4.1.0 Expanded to add support for Layer 2
- pre-Version 6.1.1.1 Introduced on E-Series

**Usage Information**

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>Assign a class map and QoS policy to different queues.</td>
</tr>
<tr>
<td>policy-aggregate</td>
<td>Allow an aggregate method of configuring per-port QoS via policy maps.</td>
</tr>
<tr>
<td>service-policy input</td>
<td>Apply 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.
Output policy map is used to assign traffic to different flows using QoS policy. This command enables the policy-map-output configuration mode (conf-policy-map-out).

**Related Commands**
- `service-queue` Assign a class map and QoS policy to different queues.
- `policy-aggregate` Allow an aggregate method of configuring per-port QoS via policy maps.
- `service-policy output` Apply an output policy map to the selected interface.

### qos-policy-input

Create a QoS input policy on the router.

**Syntax**
```
qos-policy-input qos-policy-name [layer2]
```

To remove an existing input QoS policy from the router, use `no qos-policy-input qos-policy-name [layer2]` command.

**Parameters**
- `qos-policy-name` Enter your input QoS policy name in character format (32 character maximum).
- `layer2` (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. Default: Layer 3

**Defaults**
Layer 3

**Command Modes**
CONFIGURATION

**Command History**
- Version 8.2.1.0 Policy name character limit increased from 16 to 32.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 7.4.1.0 E-Series Only: Expanded to add support for Layer 2

**Usage Information**
Use this command to specify the name of the input QoS policy. Once 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.

Note: On ExaScale, Dell Networking OS cannot classify IGMP packets on a Layer 2 interface using Layer 3 policy map. The packets always take the default queue, Queue 0, and cannot be rate-policed.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-police</td>
<td>Incoming traffic policing function</td>
</tr>
</tbody>
</table>

### qos-policy-output

**Syntax**

```
qos-policy-output qos-policy-name
```

To remove an existing output QoS policy, use the `no qos-policy-output qos-policy-name` command.

**Parameters**

- `qos-policy-name` Enter your output QoS policy name in character format (32 character maximum).

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

- **Version 8.2.1.0** Policy name character limit increased from 16 to 32.
- **Version 7.6.1.0** Introduced on C-Series and S-Series
- **pre-Version 6.1.1.1** Introduced on E-Series

**Usage Information**

Use this command to specify the name of the output QoS policy. Once 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit</td>
<td>Outgoing traffic rate-limit functionality</td>
</tr>
<tr>
<td>bandwidth-percentage</td>
<td>Assign weight to class/queue percentage</td>
</tr>
<tr>
<td>bandwidth-weight</td>
<td>Assign a priority weight to a queue.</td>
</tr>
<tr>
<td>wred</td>
<td>Assign yellow or green drop precedence</td>
</tr>
</tbody>
</table>

### queue backplane ignore-backpressure

**Syntax**

```
queue backplane ignore-backpressure
```

Reduce egress pressure by ignoring the ingress backpressure.

**Parameters**

- `queue` Enter your queue name

**Usage Information**

To return to the default, use the `no queue backplane ignore-backpressure` command.
Assign a WRED Curve to all eight egress Multicast queues or designate the percentage for the Multicast bandwidth queue.

**Syntax**

```
queue egress multicast linecard {slot number port-set number | all} [wred-profile name | multicast-bandwidth percentage]
```

To return to the default, use the `no queue egress multicast linecard {slot number port-set number | all} [wred-profile name | multicast-bandwidth percentage]` command.

**Parameters**

- **linecard number**
  - Enter the keyword `linecard` followed by the line card slot number.  
  - E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

- **port-set number**
  - Enter the keyword `port-set` followed by the line card’s port pipe.  
  - Range: 0 or 1

- **all**
  - Enter the keyword `all` to apply to all line cards.

- **wred-profile name**
  - (OPTIONAL) Enter the keyword `wred-profile` followed by your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names.  
  - Pre-defined Profiles:  
    - wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g

- **multicast-bandwidth percentage**
  - (OPTIONAL) Enter the keyword `multicast-bandwidth` followed by the bandwidth percentage.  
  - Range: 0 to 100%

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

- **Version 7.7.1.0** Introduced on E-Series

**Usage Information**

This command does not uniquely identify a queue, but rather identifies only a set of queues. The WRED curve is applied to all eight egress Multicast queues.

### Important Points to Remember—multicast-bandwidth option

- A unique Multicast Weighted Fair Queuing (WFQ) setting can be applied only on a per port-pipe basis. The minimum percentage of the multicast bandwidth assigned to any of the ports in the port-pipe will take effect for the entire port-pipe.
- If the percentage of multicast bandwidth is 0, control traffic going through multicast queues are dropped.
• The no form of the command without **multicast-bandwidth** and **wred-profile**, will remove both the wred-profile and multicast-bandwidth configuration.

• On 10 Gigabit ports only, the multicast bandwidth option will work only if the total unicast bandwidth is more than the multicast bandwidth.

• If strict priority is applied along with multicast-bandwidth, the effect of strict priority is on all ports where unicast and multicast bandwidth are applied.

• When multicast bandwidth is assigned along with unicast bandwidth, first multicast bandwidth will be reserved for that port, then the remaining unicast bandwidth configured is adjusted according to the bandwidth available after reserving for multicast bandwidth.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show queue statistics egress</strong></td>
<td>Display the egress queue statistics</td>
</tr>
</tbody>
</table>

**queue ingress**

Assign a WRED Curve to all eight ingress Multicast queues or designate the percentage for the Multicast bandwidth queue.

**Syntax**

```
queue ingress multicast {linecard slot number port-set number | all} [wred-profile name]
```

To return to the default, use the **no queue ingress multicast {linecard slot number port-set number | all} [wred-profile name]** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linecard number</td>
<td>Enter the keyword <code>linecard</code> followed by the line card slot number. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.</td>
</tr>
<tr>
<td>port-set number</td>
<td>Enter the keyword <code>port-set</code> followed by the line card’s port pipe. Range: 0 or 1</td>
</tr>
<tr>
<td>all</td>
<td>Enter the keyword <code>all</code> to apply to all line cards.</td>
</tr>
<tr>
<td>wred-profile name</td>
<td>(OPTIONAL) Enter the keyword <code>wred-profile</code> followed by your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

This command does not uniquely identify a queue, but rather identifies only a set of queues. The WRED Curve is applied to all eight ingress Multicast queues.

**Note:** The multicast-bandwidth option is not supported on queue ingress. If you attempt to use the multicast-bandwidth option, the following reject error message is generated:

```
% Error:Bandwidth-percent is not allowed for ingress multicast
```
rate-limit

Specify the rate-limit functionality on outgoing traffic as part of the selected policy.

**Syntax**

```
rerate-limit [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]]
```

**Parameters**

- **kbps**: Enter this keyword to specify the rate limit in Kilobits per second (Kbps). On the E-Series, Dell Networking recommends using a value greater than or equal to 512 as lower values does not yield accurate results. The default granularity is Megabits per second (Mbps).
  - Range: 0 to 10000000

- **committed-rate**: Enter the committed rate in Mbps.
  - Range: 0 to 10000 Mbps

- **burst-KB** (OPTIONAL): Enter the burst size in KB.
  - Range: 16 to 200000 KB
  - Default: 50 KB

- **peak peak-rate** (OPTIONAL): Enter the keyword peak followed by the peak rate in Mbps.
  - Range: 0 to 10000 Mbps
  - Default: Same as designated for committed-rate

**Defaults**

Burst size is 50 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-OUT

**Command History**

- Version 8.2.1.0: Added kbps option on E-Series.
- Version 7.7.1.0: Removed from C-Series
- Version 7.5.1.0: Introduced on C-Series
- pre-Version 6.1.1.1: Introduced on E-Series

**Related Commands**

- **rate limit**: Specify rate-limit functionality on the selected interface.
- **qos-policy-output**: Create a QoS output policy.
rate-police

Specify the policing functionality on incoming traffic.

Syntax

rate-police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]]

Parameters

kbps Enter this keyword to specify the rate limit in Kilobits per second (Kbps). On C-Series and S-Series make the following value a multiple of 64. On the E-Series, Dell Networking recommends using a value greater than or equal to 512 as lower values does not yield accurate results. The default granularity is Megabits per second (Mbps).
Range: 0 to 10000000

committed-rate Enter the committed rate in Mbps.
Range: 0 to 10000 Mbps

burst-KB (OPTIONAL) Enter the burst size in KB.
Range: 16 to 200000 KB
Default: 50 KB

peak peak-rate (OPTIONAL) Enter the keyword peak followed by the peak rate in Mbps.
Range: 0 to 10000 Mbps
Default: Same as designated for committed-rate

Defaults

Burst size is 50 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 8.2.1.0 Added kbps option on C-Series, E-Series, and Series.
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
pre-Version 6.1.1.1 Introduced on E-Series

Related Commands

rate police Specify traffic policing on the selected interface.
qos-policy-input Create a QoS output policy.

rate-shape

Shape traffic output as part of the designated policy.

Syntax

rate-shape [kbps] rate [burst-KB]

Parameters

kbps Enter this keyword to specify the rate limit in Kilobits per second (Kbps). On C-Series and S-Series make the following value a multiple of 64. The default granularity is Megabits per second (Mbps).
Range: 0-10000000
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: 10

Defaults
Burst size is 10 KB. Granularity for rate is Mbps unless the kbps option is used.

Command Modes
QOS-POLICY-OUT

Command History
Version 8.2.1.0 Added kbps option on C-Series, E-Series, and S-Series.
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
pre-Version 6.1.1.1 Introduced on E-Series

Usage Information
rate-shape can be applied only as an aggregate policy. If it is applied as a class-based policy, then rate-shape will not take effect.

On 40-port 10G line cards, if the traffic is shaped between 64 and 1000kbs, for some values the shaped rate is much less than the value configured. Do not use values in this range for 10G interfaces.

Related Commands
rate shape
Shape the traffic output of the selected interface.
qos-policy-output
Create a QoS output policy.

service-policy input
Apply an input policy map to the selected interface.

Syntax
service-policy input policy-map-name [layer2]

To remove the input policy map from the interface, use the no service-policy input policy-map-name [layer2] command.

Parameters
policy-map-name
Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

layer2
(OPTIONAL) Enter the keyword layer2 to specify a Layer 2 Class Map.
Default: Layer 3

Defaults
Layer 3

Command Modes
INTERFACE

Command History
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
Version 7.4.1.0 E-Series Only: Expanded to add support for Layer 2
pre-Version 6.1.1.1 Introduced on E-Series
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. However, the `service-policy input` command (without the `policy-map-name` option) and the `service-class dynamic dot1p` command are allowed on an interface.

**Related Commands**

- `policy-map-input` Create 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.

**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.

**Defaults**

No default behavior or values

**Command Modes**

- INTERFACE

**Command History**

- Introduced on C-Series and S-Series
- Introduced on E-Series

**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.

**Related Commands**

- `policy-map-output` Create an output policy map.

**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.
### set

Mark outgoing traffic with a Differentiated Service Code Point (DSCP) or dot1p value.

**Syntax**

```
set {ip-dscp value | mac-dot1p value}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-dscp value</td>
<td>(OPTIONAL) Enter the keyword <code>ip-dscp</code> followed by the IP DSCP value. Range: 0 to 63</td>
</tr>
<tr>
<td>mac-dot1p value</td>
<td>Enter the keyword <code>mac-dot1p</code> followed by the dot1p value. Range: 0 to 7 On the C-Series and S-Series allowed values are: 0, 2, 4, 6</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION (conf-qos-policy-in)

**Command History**

- Version 8.2.1.0  
  mac-dot1p available on the C-Series and S-Series
- Version 7.6.1.0  
  Introduced on S-Series
- Version 7.5.1.0  
  Introduced on C-Series
Usage Information

C-Series and S-Series
Once the IP DSCP bit is set, other QoS services can then operate on the bit settings.

E-Series
Once the IP DSCP bit is set, other QoS services can then operate on the bit settings. WRED (Weighted Random Early Detection) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

show cam layer2-qos
Display the Layer 2 QoS CAM entries.

Syntax
show cam layer2-qos ([linecard number | port-set number] | [interface interface]) [summary]

Parameters

linecard number
Enter the keyword linecard followed by the line card slot number.
E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

port-set number
Enter the keyword port-set followed by the line card’s port pipe.
Range: 0 or 1

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

summary
(Optional) Enter the keyword summary to display only the total number of CAM entries.

Defaults
No default behavior or values

Command Modes
EXEC

Command History

Version 7.4.1.0 E-Series Only: Expanded to add support for mac-dot1p
pre-Version 6.1.1.1 Introduced on E-Series
Example Figure 47-3. show cam layer2-qos interface Command Output

```
FTOS#show cam layer2-qos interface gigabitethernet 2/0
Cam   Port Dot1p Proto       SrcMac            SrcMask           DstMac            DstMask            Dot1p      DSCP     Queue
Index                                                                                                 Marking    Marking
-------------------------------------------------------------------------------------------------------------------------
-------
01817 0    -     0           00:00:00:00:cc:cc 00:00:00:00:ff:ff 00:00:00:00:dd:dd 00:00:00:00:ff:ff  -          -        7
01818 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  -          -        5
01819 0    4     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  4          -        4
01820 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  4          45       5
02047 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  -          -        0
FTOS#
```

Example Figure 47-4. show cam layer2-qos linecard Command Output

```
FTOS#show cam layer2-qos linecard 2 port-set 0
Cam   Port Dot1p Proto       SrcMac            SrcMask           DstMac            DstMask            Dot1p      DSCP     Queue
Index                                                                                                 Marking    Marking
----------------------------------------------------------------------------------------------------------------------=-
01817 0    -     0           00:00:00:00:cc:cc 00:00:00:00:ff:ff 00:00:00:00:dd:dd 00:00:00:00:ff:ff  -          -        7
01818 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  -          -        5
01819 0    4     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  4          -        4
01820 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  4          45       5
02047 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  -          -        0
FTOS#
```

show cam layer3-qos

Display the Layer 3 QoS CAM entries.

```
show cam layer3-qos {[linecard number port-set number] | [interface interface] [summary]}
```

**Parameters**

- **linecard number**: Enter the keyword `linecard` followed by the line card slot number.
  - **E-Series**: Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300.

- **port-set number**: Enter the keyword `port-set` followed by the line card’s port pipe.
  - Range: 0 or 1

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

- **summary** (OPTIONAL): Enter the keyword `summary` to display only the total number of CAM entries.

**Defaults**

No default behavior or values

**Command Modes**

EXEC
Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on E-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.1.0</td>
<td>FTOS#</td>
</tr>
</tbody>
</table>

Example

**Figure 47-5. show cam layer3-qos linecard interface Command Output**

FTOS#sh cam layer3-qos interface gigabitethernet 2/1

<table>
<thead>
<tr>
<th>Cam Index</th>
<th>Port</th>
<th>Dscp</th>
<th>Proto</th>
<th>Tcp</th>
<th>Src</th>
<th>Dst</th>
<th>SrcIp</th>
<th>DstIp</th>
<th>DSCP</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>23488</td>
<td>1</td>
<td>0</td>
<td>0x0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0/0</td>
<td>-</td>
<td>TRUST-DSCP</td>
</tr>
</tbody>
</table>

In these figures outputs, note that:

- The entry TRUST-DSCP in the Queue column indicates that the trust diffserv is configured on the policy-map.
- A hyphen (-) entry in the DSCP Marking column indicates that there is no DSCP marking.
- In the Proto column (Protocol), IP, ICMP, UDP, and TCP strings are displayed. For other protocols, the corresponding protocol number is displayed.

Example

**Figure 47-6. show cam layer3-qos linecard port-set Command Output**

FTOS#show cam layer3-qos linecard 13 port-set 0

<table>
<thead>
<tr>
<th>Cam Index</th>
<th>Port</th>
<th>Dscp</th>
<th>Proto</th>
<th>Tcp</th>
<th>Src</th>
<th>Dst</th>
<th>SrcIp</th>
<th>DstIp</th>
<th>DSCP</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>24511</td>
<td>1</td>
<td>0</td>
<td>TCP</td>
<td>0x5</td>
<td>2</td>
<td>5</td>
<td>1.0.0.1/24</td>
<td>2.0.0.2/24</td>
<td>-</td>
<td>TRUST-DSCP</td>
</tr>
<tr>
<td>24512</td>
<td>1</td>
<td>0</td>
<td>UDP</td>
<td>0x2</td>
<td>2</td>
<td>5</td>
<td>8.0.0.8/24</td>
<td>8.0.0.8/24</td>
<td>23</td>
<td>3</td>
</tr>
</tbody>
</table>

Example

**Figure 47-7. show cam layer3-qos linecard interface Command without Trust Output**

FTOS#sh cam layer3-qos interface gigabitethernet 2/1

<table>
<thead>
<tr>
<th>Cam Index</th>
<th>Port</th>
<th>Dscp</th>
<th>Proto</th>
<th>Tcp</th>
<th>Src</th>
<th>Dst</th>
<th>SrcIp</th>
<th>DstIp</th>
<th>DSCP</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>23488</td>
<td>1</td>
<td>56</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0/0</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td>23489</td>
<td>1</td>
<td>48</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0/0</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td>23490</td>
<td>1</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0/0</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td>23491</td>
<td>1</td>
<td>0</td>
<td>IP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10.1.1.1/32</td>
<td>20.1.1.1/32</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>23492</td>
<td>1</td>
<td>0</td>
<td>IP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10.1.1.1/32</td>
<td>20.1.1.2/32</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>24511</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0/0</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>

Example

**Figure 47-8. show cam layer3-qos summary Command Output**

FTOS#show cam layer3-qos linecard 13 port-set 0 summary

Total number of CAM entries for Port-Set 0 is 100

FTOS#
show qos class-map

View the current class map information.

**Syntax**

```
show qos class-map [class-name]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-name</td>
<td>(Optional) Enter the name of a configured class map.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS#show qos class-map
Class-map match-any CM
  Match ip access-group ACL
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map</td>
<td>Identify the class map</td>
</tr>
</tbody>
</table>
show qos policy-map

View the QoS policy map information.

**Syntax**

```plaintext
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 Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port 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.

- **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 Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
  - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port 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**

No default behavior or values

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Updated Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series only: Added Trust IPv6 diffserv</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
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

No default behavior or values
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 name.
- **qos-policy-output qos-policy-name**: Enter the keyword `qos-policy-output` followed by the QoS policy name.

Defaults

No default behavior or values

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 7.6.1.0**: Introduced on C-Series and S-Series
- pre-Version 6.1.1.1: Introduced on E-Series
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
No default behavior or values

Command Modes
EXEC
EXEC Privilege

Command History
Version 7.6.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series
pre-Version 6.1.1.1 Introduced on E-Series

Example

Figure 47-16. show qos qos-policy-input Command Output

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
No default behavior or values

Command Modes
EXEC
EXEC Privilege

Command History
Version 7.6.1.0 Introduced on C-Series and S-Series
pre-Version 6.1.1.1 Introduced on E-Series
Example

Figure 47-17. show qos qos-policy-output Command Output

ftos#show qos qos-policy-output
qos-policy-output qosOut
   Rate-limit 50 50 peak 50 50
   Wred yellow 1
   Wred green 1

show qos statistics

View QoS statistics.

Syntax

show qos statistics [wred-profile [interface]] | [interface]

Parameters

wred-profile interface  Platform—E-Series Only: Enter the keyword wred-profile and optionally one of the following keywords and slot/port or number information:
- For a Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.
- For a Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a SONET interface, enter the keyword sonet followed by the slot/port 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.

interface  Enter one of the following keywords and slot/port or number information:
- On the C-Series and E-Series, For a Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.
- For a Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a SONET interface, enter the keyword sonet followed by the slot/port 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

No default behavior or values

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.4.6.0  Added support for the keyword fortyGigE.
Version 7.7.1.1  Introduced on S-Series
Version 7.5.1.0  Introduced on C-Series
pre-Version 6.1.1.1  Introduced on E-Series
The `show qos statistics` command can be used on the C-Series, but the `wred-profile` keyword must be omitted in the syntax. The `show qos statistics` output differs from the ED and EE series line cards and the EF series line cards. The QoS statistics for the EF series generates two extra columns, Queued Pkts and Dropped Pkts, see Example 2.

**Note:** The `show qos statistics` command displays Matched Packets and Matched Bytes. The `show queue statistics egress` command (E-Series only) displays Queued Packets and Queued Bytes. The following example explains how these two displays relate to each other.

- 9000 byte size packets are sent from Interface A to Interface B.
- The Matched Packets on Interface A are equal to the Queued Packets on Interface B.
- Matched bytes on Interface A = matched packets *9000
- Queued bytes on Interface B = queued packets *(9020)—Each packet has an additional header of 20 bytes.

### Example 1

**Figure 47-18. `show qos statistics` Command Output (ED and EE Series of E-Series)**

```
FTOS#show qos statistics

Interface Gi 0/0

Queue#  Queued Bytes             Matched Pkts            Matched Bytes
0      0                       0                       0
1      0                       0                       0
2      0                       0                       0
3      0                       0                       0
4      0                       0                       0
5      0                       0                       0
6      0                       0                       0
7      0                       0                       0

Interface Gi 0/1

Queue#  Queued Bytes             Matched Pkts            Matched Bytes
0      0                       0                       0
1      0                       0                       0
2      0                       0                       0
3      0                       0                       0
4      0                       0                       0
5      0                       0                       0
6      0                       0                       0
7      0                       0                       0
```

Table 47-4. `show qos statistics` Command Example Fields (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>Queued Bytes</td>
<td>Snapshot of the byte count in that queue.</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>
<tr>
<td>Matched Bytes</td>
<td>The number of bytes that matched the class-map criteria.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When trust is configured, matched byte counters are not</td>
</tr>
<tr>
<td></td>
<td>incremented in this field.</td>
</tr>
</tbody>
</table>
Example 2  
Figure 47-19. show qos statistics Command Output (EF Series of E-Series)

FTOS#show qos statistics gig 0/1

<table>
<thead>
<tr>
<th>Queue#</th>
<th>Queued Bytes (Cumulative)</th>
<th>Queued Pkts (Cumulative)</th>
<th>Matched Pkts</th>
<th>Matched Bytes</th>
<th>Dropped Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>1883724</td>
<td>1883724000</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>1883720</td>
<td>1883720000</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>1883720</td>
<td>1883720000</td>
<td>0</td>
</tr>
</tbody>
</table>

FTOS#

Table 47-5. show qos statistics Command Example Fields (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>Queued Bytes</td>
<td>Cumulative byte count in that queue</td>
</tr>
<tr>
<td>Queued Pkts</td>
<td>Cumulative packet count in that queue</td>
</tr>
<tr>
<td>Matched Pkts</td>
<td>The number of packets that matched the class-map criteria. Note: When trust is configured, matched packet counters are not incremented in this field.</td>
</tr>
<tr>
<td>Matched Bytes</td>
<td>The number of bytes that matched the class-map criteria. Note: When trust is configured, matched byte counters are not incremented in this field.</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The total of the number of packets dropped for green, yellow and out-of-profile.</td>
</tr>
</tbody>
</table>

Example 3  
Figure 47-20. show qos statistics wred-profile Command Output (ED, EE, and EF Series)

FTOS#show qos statistics wred-profile

<table>
<thead>
<tr>
<th>Interface Gi 5/11</th>
<th>Queue#</th>
<th>Drop-statistic</th>
<th>WRED-name</th>
<th>Dropped Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>0</td>
<td>WRED1</td>
<td>51623</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>51300</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>1</td>
<td>WRED1</td>
<td>52082</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>51004</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>2</td>
<td>WRED1</td>
<td>50567</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>49965</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>3</td>
<td>WRED1</td>
<td>50477</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>49815</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>4</td>
<td>WRED1</td>
<td>50695</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>49476</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>5</td>
<td>WRED1</td>
<td>50245</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>49535</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>6</td>
<td>WRED1</td>
<td>50033</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>49595</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>7</td>
<td>WRED1</td>
<td>50474</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>WRED2</td>
<td>49522</td>
<td></td>
</tr>
<tr>
<td>Out of Profile</td>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

FTOS#
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

No default behavior or values

Command Modes

- EXEC
- EXEC Privilege

Command History

- pre-Version 6.1.1.1 Introduced on E-Series

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 linecard {number port-set portpipe number} | [all]}
```

Parameters

- **policy-map**: Enter the policy map name.
- **linecard number**: (OPTIONAL) Enter the keyword `linecard` followed by the line card slot number.
**port-set portpipe number**  
Enter the keyword **port-set** followed by the line card’s port pipe number.  
Range: 0 or 1

**linecard all**  
(Optional) Enter the keywords **linecard all** to indicate all line cards.

**Defaults**  
No default values or behavior

**Command Modes**  
EXEC

**Command History**  
Version 7.6.1.0  
Introduced on C-Series and S-Series

Version 7.4.1.0  
Introduced on E-Series

**Example**  
**Figure 47-22.  test cam-usage service-policy input policy-map linecard all Example Command**

FTOS# test cam-usage service-policy input pmap_l2 linecard all

For a L2 Input Policy Map pmap_l2, the output must be as follows,

<table>
<thead>
<tr>
<th>Linecard</th>
<th>Portpipe</th>
<th>CAM Partition</th>
<th>Available CAM</th>
<th>Estimated CAM</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>L2ACL</td>
<td>500</td>
<td>200</td>
<td>Allowed (2)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L2ACL</td>
<td>100</td>
<td>200</td>
<td>Exception</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>L2ACL</td>
<td>1000</td>
<td>200</td>
<td>Allowed (5)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>L2ACL</td>
<td>0</td>
<td>200</td>
<td>Exception</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>L2ACL</td>
<td>400</td>
<td>200</td>
<td>Allowed (2)</td>
</tr>
</tbody>
</table>

FTOS#

**Note:** In a Layer 2 Policy Map, IPv4/IPv6 rules are not allowed and hence the output contains only L2ACL CAM partition entries.

**Table 47-7.  test cam-usage Command Example Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linecard</td>
<td>Indicates the line card slot number.</td>
</tr>
<tr>
<td>Portpipe</td>
<td>Indicates the portpipe number.</td>
</tr>
<tr>
<td>CAM Partition</td>
<td>The CAM space where the rules are added.</td>
</tr>
<tr>
<td>Available CAM</td>
<td>Indicates the free CAM space, in the partition, for the classification rules.</td>
</tr>
</tbody>
</table>

**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.
Usage Information
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.

threshold
Specify the minimum and maximum threshold values for the configured WRED profiles.

Syntax
threshold min number max number

To remove the threshold values, use the no threshold min number max number command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min number</td>
<td>Enter the keyword min followed by the minimum threshold number for the WRED profile. Range: 1024 to 77824 KB</td>
</tr>
<tr>
<td>max number</td>
<td>Enter the keyword max followed by the maximum threshold number for the WRED profile. Range: 1024 to 77824 KB</td>
</tr>
</tbody>
</table>

Defaults
No default behavior or values

Command Modes
CONFIGURATION (config-wred)

Command History
pre-Version 6.1.1.1 Introduced on E-Series

Usage Information
Use this command to configure minimum and maximum threshold values for user defined profiles. Additionally, use this command to modify the minimum and maximum threshold values for the pre-defined WRED profiles. If you delete threshold values of the pre-defined WRED profiles, the profiles will revert to their original default values.
**Table 47-8. Pre-defined WRED Profile Threshold Values**

<table>
<thead>
<tr>
<th>Pre-defined WRED Profile Name</th>
<th>Minimum Threshold</th>
<th>Maximum Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>wred_drop</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>wred_ge_y</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td>wred_ge_g</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td>wred_teng_y</td>
<td>4096</td>
<td>8192</td>
</tr>
<tr>
<td>wred_teng_g</td>
<td>8192</td>
<td>16384</td>
</tr>
</tbody>
</table>

**Related Commands**

- `wred-profile`: Create a WRED profile.

**trust**

Specify dynamic classification (DSCP) or dot1p to trust.

**Syntax**

```
trust {diffserv [fallback] | dot1p [fallback] | ipv6-diffserv}
```

**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.
- `ipv6-diffserv`: On E-Series only, enter the keyword `ipv6-diffserv` to specify trust configuration of IPv6 DSCP.

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION (conf-policy-map-in)

**Command History**

- Version 8.3.1.0 `fallback` available on the E-Series.
- Version 8.2.1.0 `dot1p` available on the C-Series and S-Series.
- Version 7.6.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- Version 7.4.1.0 Expanded to add support for dot1p and IPv6 DSCP
- pre-Version 6.1.1.1 Introduced on E-Series

**Usage Information**

When trust is configured, matched bytes/packets counters are not incremented in the `show qos statistics` command.

The `trust diffserv` feature is not supported on E-Series ExaScale when an IPv6 microcode is enabled.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The default mapping table is detailed in the following table.
Designate the WRED profile to yellow or green traffic.

**Syntax**

```
wred {yellow | green} profile-name
```

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_ge_y`
  - `wred_ge_g`
  - `wred_teng_y`
  - `wred_teng_g`

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION (conf-qos-policy-out)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Profile name character limit increased from 16 to 32.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to assign drop precedence to green or yellow traffic. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.

**Related Commands**

- `wred-profile`: Create a WRED profile and name that profile
- `trust`: Define the dynamic classification to trust DSCP
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

- `pre-Version 6.1.1.1` Introduced on E-Series

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).

Related Commands

- `threshold`: Specify the minimum and maximum threshold values of the WRED profile

---

### Queue-Level Debugging

Queue-Level Debugging is an E-Series-only feature, as indicated by the `[E]` character that appears below each command heading.

The following queuing statistics are available on both the EtherScale and TeraScale versions of E-Series systems.

- `clear queue statistics egress`
- `clear queue statistics ingress`
- `show queue statistics egress`
- `show queue statistics ingress`
clear queue statistics egress

Clear egress queue statistics.

Syntax

clear queue statistics egress [unicast | multicast] [Interface]

Parameters

unicast | multicast (OPTIONAL) Enter the keyword multicast to clear only Multicast queue statistics. Enter the keyword unicast to clear only Unicast queue statistics. Default: Both Unicast and Multicast queue statistics are cleared.

Interface

(OPTIONAL) Enter one of the following interfaces to display the interface specific queue statistics.

- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
- For a SONET interface, enter the keyword sonet followed by the slot/port information.
- Fast Ethernet is not supported

Defaults

No default behavior or values

Command Modes

EXEC

EXEC Privilege

Command History

Version 6.2.1.1 Introduced

Usage Information

If a Policy QoS is applied on an interface when clear queue statistics egress is issued, it will clear the egress counters in show queue statistics and vice-versa. This behavior is due to the values being read from the same hardware registers.

Related Commands

clear queue statistics egress Clear ingress queue statistics
show queue statistics egress Display egress queue statistics
show queue statistics ingress Display ingress queue statistics

clear queue statistics ingress

Clear ingress queue statistics.

Syntax

clear queue statistics ingress [unicast [src-card ID [dst-card ID ]] | [multicast] [src-card ID ]]
show queue statistics egress

Display the egress queue statistics.

**Syntax**

```
show queue statistics egress [unicast | multicast] [Interface] [brief]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unicast</td>
<td>multicast</td>
</tr>
<tr>
<td>Interface</td>
<td>(OPTIONAL) Enter one of the following interfaces to display the interface specific queue statistics.</td>
</tr>
<tr>
<td></td>
<td>- For a 1-Gigabit Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a 10-Gigabit Ethernet interface, enter the keyword <strong>TenGigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a SONET interface, enter the keyword <strong>sonet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- Fast Ethernet is not supported.</td>
</tr>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword <strong>brief</strong> to display only ingress per link buffering and egress per port buffering statistics.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

EXEC

EXEC Privilege
EtherScale systems display cumulative dropped packets, while TeraScale systems display cumulative queued bytes (in KB), cumulative queued packets (in KB), and cumulative dropped packets (in KB).

The display area is limited to 80 spaces to accommodate the screen and for optimal readability. Numbers, that is values, are limited to 12 characters. The numbering conventions are detailed in the table below.

### Table 47-10. Numbering Conventions for show queue egress statistics Output

<table>
<thead>
<tr>
<th>Value</th>
<th>Divide the number by</th>
<th>Quotient Display</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10^11) - (10^14)</td>
<td>1024</td>
<td>K</td>
<td>12345678901K</td>
</tr>
<tr>
<td>(10^14) - (10^17)</td>
<td>1024*1024</td>
<td>M</td>
<td>12345678901M</td>
</tr>
<tr>
<td>&gt; (10^17)</td>
<td>1024<em>1024</em>1024</td>
<td>T</td>
<td>12345678901T</td>
</tr>
</tbody>
</table>

**Note:** The `show queue statistics` command displays Queued Packets and Queued Bytes. The `show qos statistics` command displays Matched Packets and Matched Bytes. The following example explains how these two outputs relate to each other.

- 9000 byte size packets are sent from Interface A to Interface B.
- The Matched Packets on Interface A are equal to the Queued Packets on Interface B.
- Matched bytes on Interface A = matched packets *9000
- Queued bytes on Interface B = queued packets *(9020)—Each packet has an additional header of 20 bytes.

### Example 1

**Figure 47-23. show queue statistics egress Command (TeraScale)**

```
FTOS#show queue statistics egress unicast gigabitethernet 9/1

Interface Gi 9/1

<table>
<thead>
<tr>
<th>Egress Queued bytes</th>
<th>Queued packets</th>
<th>Packet Type</th>
<th>Min</th>
<th>Max</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>281513847K</td>
<td>31959000</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>99281660K</td>
<td>11271000</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>99281660K</td>
<td>11271000</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>38984440000</td>
<td>43220000</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>99281660K</td>
<td>11271000</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>39760160000</td>
<td>4408000</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>39642900000</td>
<td>4395000</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>99274410K</td>
<td>11270177</td>
<td>Green</td>
<td>2048</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

FTOS#
### Table 47-11. show queue statistics egress Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Port Queue#</td>
<td>Egress Port Queue Number</td>
</tr>
<tr>
<td>Queued bytes</td>
<td>Cumulative byte count in that queue</td>
</tr>
<tr>
<td>Queued packets</td>
<td>Cumulative packet count in that queue.</td>
</tr>
<tr>
<td>Packet type</td>
<td>Green, yellow, and out-of-profile packets</td>
</tr>
<tr>
<td>Min KB</td>
<td>Minimum threshold for WRED queue</td>
</tr>
<tr>
<td>Max KB</td>
<td>Maximum threshold for WRED queue</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The number of packets dropped for green, yellow and out-of-profile</td>
</tr>
</tbody>
</table>

### Example 2

**Figure 47-24. show queue statistics egress multicast Command Output (EtherScale)**

```
FTOS#show queue statistics egress multicast

Linecard 3 port pipe 0, multicast
Packet Type    Min  Max  Dropped
   Green        8192 16384     0
   Yellow       4096  8192     0
   Out of Profile                         0

Linecard 3 port pipe 1, multicast
Packet Type    Min  Max  Dropped
   Green        8192 16384     0
   Yellow       4096  8192     0
   Out of Profile                         0

Linecard 7 port pipe 0, multicast
Packet Type    Min  Max  Dropped
   Green        2048  4096     0
   Yellow       1024  2048     0
   Out of Profile                         0

Linecard 7 port pipe 1, multicast
Packet Type    Min  Max  Dropped
   Green        2048  4096     0
   Yellow       1024  2048     0
   Out of Profile                         0

FTOS#
```

### Table 47-12. show queue statistics egress multicast Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet type</td>
<td>Green, yellow, and out-of-profile packets</td>
</tr>
<tr>
<td>Min KB</td>
<td>Minimum threshold for WRED queue</td>
</tr>
<tr>
<td>Max KB</td>
<td>Maximum threshold for WRED queue</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The number of packets dropped for green, yellow and out-of-profile</td>
</tr>
</tbody>
</table>
Example 3

Figure 47-25.  show queue statistics egress brief Command Output

FTOS#show queue statistics egress brief

<table>
<thead>
<tr>
<th>LC</th>
<th>Portpipe</th>
<th>Port</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>M</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>M</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

FTOS#

Table 47-13.  show queue statistics egress brief Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LC</td>
<td>Line Card</td>
</tr>
<tr>
<td>Portpipe</td>
<td>Portpipe number</td>
</tr>
<tr>
<td>Port</td>
<td>Port Queue. Where M is Multicast queue</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The number of packets dropped for green, yellow and out-of-profile</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear queue statistics egress</td>
<td>Clear egress queue statistics.</td>
</tr>
<tr>
<td>clear queue statistics ingress</td>
<td>Clear ingress queue statistics.</td>
</tr>
<tr>
<td>show queue statistics ingress</td>
<td>Display ingress queue statistics</td>
</tr>
</tbody>
</table>

show queue statistics ingress

Display the ingress queue statistics.

Syntax

show queue statistics ingress [unicast [src-card/ID [dst-card/ID]] | [multicast [src-card/ID]] [brief]
Parameters

**unicast [src-card ID [dst-card ID]]**

(OPTIONAL) Enter the keyword **unicast** to display Unicast queue statistics. Optionally, enter the source card identification (**src-card ID**) and the destination card identification (**dst-card ID**) to display the unicast statistics from the source card to the destination card.

Destination card Identification: Range 0 to 13 or RPM

**multicast [src-card ID]**

(OPTIONAL) Enter the keyword **multicast** to display only Multicast queue statistics. Optionally, enter the source card identification (**src-card ID**) to display the multicast statistics from the source card.

Default: Both Unicast and Multicast queue statistics are displayed.

**brief**

(OPTIONAL) Enter the keyword **brief** to display only ingress per link buffering and egress per port buffering statistics.

Defaults

No default behavior or values

Command Modes

EXEC

EXEC Privilege

Command History

Version 6.2.1.1 Introduced

Usage Information

EtherScale systems display cumulative dropped packets, while TeraScale systems display cumulative queued bytes (in KB), cumulative queued packets (in KB), and cumulative dropped packets (in KB).

The display area is limited to 80 spaces to accommodate the screen and for optimal readability. Numbers, that is values, are limited to 12 characters. The conventions are detailed in the following table.

<table>
<thead>
<tr>
<th>Value</th>
<th>Divide the number by</th>
<th>Quotient Display</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>((10^{11}) - (10^{14}))</td>
<td>1024</td>
<td>K</td>
<td>12345678901K</td>
</tr>
<tr>
<td>((10^{14}) - (10^{17}))</td>
<td>1024*1024</td>
<td>M</td>
<td>12345678901M</td>
</tr>
<tr>
<td>&gt; ((10^{17}))</td>
<td>1024<em>1024</em>1024</td>
<td>T</td>
<td>12345678901T</td>
</tr>
</tbody>
</table>

**Note:** The **show queue statistics** command displays Queued Packets and Queued Bytes. The **show qos statistics** command displays Matched Packets and Matched Bytes. The following example explains how these two displays relate to each other:

- 9000 byte size packets are sent from Interface A to Interface B.
- The Matched Packets on Interface A are equal to the Queued Packets on Interface B.
- Matched bytes on Interface A = matched packets *9000
- Queued bytes on Interface B = queued packets *(9020)—Each packet has an additional header of 20 bytes.
**Figure 47-26. show queue statistics ingress Command (EtherScale) Partial**

FTOS#show queue statistics ingress unicast src-card 7 dst-card 3

Linecard 7 port pipe 0, to linecard 3 port pipe 0, unicast

<table>
<thead>
<tr>
<th>SF</th>
<th>Packet Type</th>
<th>Min</th>
<th>Max</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>KB</td>
<td>KB</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Linecard 7 port pipe 0, to linecard 3 port pipe 1, unicast

<table>
<thead>
<tr>
<th>SF</th>
<th>Packet Type</th>
<th>Min</th>
<th>Max</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>KB</td>
<td>KB</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 47-15. show queue statistics Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF Ingress Queue #</td>
<td>Switch Fabric Queue Number</td>
</tr>
<tr>
<td>Packet type</td>
<td>Green, yellow, and out-of-profile packets</td>
</tr>
<tr>
<td>Min KB</td>
<td>Minimum threshold for WRED queue</td>
</tr>
<tr>
<td>Max KB</td>
<td>Maximum threshold for WRED queue</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The number of packets dropped for green, yellow and out-of-profile</td>
</tr>
</tbody>
</table>
Example 2

Figure 47-27. show queue statistics ingress Multicast Command Output (EtherScale)

FTOS#show queue statistics ingress multicast src-card 7

Linecard 7 port pipe 0, multicast

<table>
<thead>
<tr>
<th>SF Ingress Queue#</th>
<th>Packet Type</th>
<th>Min KB</th>
<th>Max KB</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Linecard 7 port pipe 1, multicast

<table>
<thead>
<tr>
<th>SF Ingress Queue#</th>
<th>Packet Type</th>
<th>Min KB</th>
<th>Max KB</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Green</td>
<td>4096</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>3276</td>
<td>3276</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Out of Profile</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Table 47-16. show queue statistics ingress Multicast Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF Ingress Queue #</td>
<td>Switch Fabric Queue Number</td>
</tr>
<tr>
<td>Packet type</td>
<td>Green, yellow, and out-of-profile packets</td>
</tr>
<tr>
<td>Min KB</td>
<td>Minimum threshold for WRED queue</td>
</tr>
<tr>
<td>Max KB</td>
<td>Maximum threshold for WRED queue</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The number of packets dropped for green, yellow and out-of-profile</td>
</tr>
</tbody>
</table>
Example 3

**Figure 47-28. show queue statistics ingress brief Command Output**

```
FTOS#show queue statistics ingress src-card 0 brief
Source Linecard 0

Dest LC | Src Port set | Dest Port set | Dropped packets
--------|--------------|---------------|-------------------
 0       | 0            | 0             | 0
 0       | 0            | 1             | 100
 0       | 1            | 0             | 0
 1       | 0            | 0             | 0
 1       | 0            | 1             | 100
 1       | 1            | 0             | 0
 2       | 0            | 0             | 0
 2       | 0            | 1             | 100
 2       | 1            | 0             | 0
 3       | 0            | 1             | 100
 3       | 0            | 1             | 0
 3       | 1            | 0             | 0
 3       | 1            | 1             | 100
 4       | 0            | 0             | 0
 4       | 0            | 1             | 100
 4       | 1            | 0             | 0
 4       | 1            | 1             | 100
 5       | 0            | 0             | 0
 5       | 0            | 1             | 100
 5       | 1            | 0             | 0
 5       | 1            | 1             | 100
 6       | 0            | 0             | 0
 6       | 0            | 1             | 100
 6       | 1            | 0             | 0
 6       | 1            | 1             | 100
 RPM     | 0            |               | 0
 RPM     | 1            |               | 100
 Multicast| 0            |               | 0
 Multicast| 1            |               | 0
FTOS#
```

**Table 47-17. show queue statistics ingress brief Command Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest LC</td>
<td>Destination Line Card</td>
</tr>
<tr>
<td>Src Port Set</td>
<td>Source PortPipe Number</td>
</tr>
<tr>
<td>Dest Port Set</td>
<td>Destination PortPipe Number</td>
</tr>
<tr>
<td>Dropped Pkts</td>
<td>The number of packets dropped</td>
</tr>
</tbody>
</table>

**Related Commands**

- clear queue statistics egress
- clear queue statistics ingress
- show queue statistics ingress
Router Information Protocol (RIP)

Overview

Router Information Protocol (RIP) is a Distance Vector routing protocol. FTOS supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2) on C-Series and E-Series and S-Series systems, as indicated by the characters that appear below each command heading:

- C-Series: C
- E-Series: E
- S-Series: S

Note: The C-Series platform supports RIP with Dell Networking OS version 7.6.1.0 and later. The S-Series platform supports RIP with Dell Networking OS version 7.8.1.0 and later. Prior to 7.6.1.0, only the E-Series platform supported RIP.

The FTOS implementation of RIP is based on IETF RFCs 2453 and RFC 1058. For more information on configuring RIP, refer to FTOS Configuration Guide.

Commands

The following commands enable 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 isis
• redistribute ospf
• router rip
• show config
• show ip rip database
• show running-config rip
• timers basic
• version

auto-summary

Use auto-summary to 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, enter no auto-summary .

Default
Enabled.

Command Modes
ROUTER RIP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

clear ip rip

Update all the RIP routes in the Dell Networking OS routing table.

Syntax
clear ip rip

Command Modes
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

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.

**Parameters**

- **interface**  (OPTIONAL) Enter the interface type and ID as one of the following:
  - For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword **sonet** followed by the 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.
  - For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
  **Note:** This option is available only on E-Series when entered as a standalone option. It is available on both C-Series and E-Series as a sub-option.

- **database**  (OPTIONAL) Enter the keyword **database** to display messages when there is a change to the RIP database.

- **events**  (OPTIONAL) Enter the keyword **events** to debug only RIP protocol changes.

- **packet**  (OPTIONAL) Enter the keyword **events** to debug only RIP protocol packets.
  **Note:** This option is available only on C-Series.

- **trigger**  (OPTIONAL) Enter the keyword **trigger** to debug only RIP trigger extensions.

**Command Modes**

EXEC Privilege

**Command History**

- Version 8.4.6.0 Added support for the keyword **fortyGigE**.
- Version 7.8.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

**default-information originate**

**Syntax**

```
default-information originate [always] [metric metric-value] [route-map map-name]
```

Generate a default route for the RIP traffic.

To return to the default values, enter no default-information originate.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>always</code></td>
<td>(OPTIONAL) Enter the keyword <code>always</code> to enable the switch software to always advertise the default route.</td>
</tr>
<tr>
<td><code>metric metric-value</code></td>
<td>(OPTIONAL) Enter the keyword <code>metric</code> followed by a number as the metric value. Range: 1 to 16. Default: 1.</td>
</tr>
<tr>
<td><code>route-map map-name</code></td>
<td>(OPTIONAL) Enter the keyword <code>route-map</code> followed by the name of a configured route-map.</td>
</tr>
</tbody>
</table>

### Defaults

- Disabled.
- metric: 1

### Command Modes

- ROUTER RIP

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>Pre-Version 6.2.1.1</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

The default route must be present in the switch routing table for the `default-information originate` command to take effect.

### default-metric

**Description**

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, enter `no default-metric`.

**Parameters**

- `number` Specify a number. Range: 1 to 16. The default is 1.

**Default**

1

**Command Modes**

- ROUTER RIP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>Pre-Version 6.2.1.1</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

**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**

No default behavior or values

**Command Modes**

ROUTER RIP

**Command History**

- Version 7.8.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- pre-7.7.1.0 Introduced on E-Series

**Related Commands**

- router rip Enter 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**: 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 7.8.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

**Related Commands**

- default-metric Assign 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` command.

**Parameters**

- `prefix-list-name` (OPTIONAL) Enter the name of a configured prefix list.
- `interface` Identifies the interface type slot/port as one of the following:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
  - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

ROUTER RIP

**Command History**

- Version 7.8.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

**Related Commands**

- `ip prefix-list` Enter the PREFIX-LIST mode and configure a prefix list.

---

**distribute-list out**

Configure a filter for outgoing routing updates.

**Syntax**

```
   distribute-list prefix-list-name out [interface | bgp | connected | isis | ospf | static]
```

To delete the filter, use the `no distribute-list prefix-list-name out` 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) Identifies the interface type slot/port as one of the following:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port 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>C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For a SONET interface, enter the keyword sonet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword fortyGigE followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>connected</th>
<th>(OPTIONAL) Enter the keyword connected to filter only directly connected routes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis</td>
<td>(OPTIONAL) Enter the keyword isis to filter only IS-IS routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>(OPTIONAL) Enter the keyword ospf to filter all OSPF routes.</td>
</tr>
<tr>
<td>static</td>
<td>(OPTIONAL) Enter the keyword static to filter manually configured routes.</td>
</tr>
</tbody>
</table>

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for the keyword fortyGigE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>ip prefix-list</th>
<th>Enter the PREFIX-LIST mode and configure a prefix list.</th>
</tr>
</thead>
</table>

ip poison-reverse

Set the prefix of the RIP routing updates to the RIP infinity value.

Syntax

```
ip poison-reverse
```

To disable poison reverse, enter `no ip poison-reverse`.

Defaults

Disabled.

Command Modes

INTERFACE
Command History

Version 7.8.1.0 Introduced on S-Series
Version 7.6.1.0 Introduced on C-Series
pre-Version 6.2.1.1 Introduced on E-Series

Related Commands

ip split-horizon Set RIP routing updates to exclude routing prefixes.

ip rip receive version

Set the interface to receive specific versions of RIP. The RIP version you set on the interface overrides the version command in the ROUTER RIP mode.

Syntax

ip rip receive version [1] [2]

To return to the default, enter no ip rip receive version.

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 7.8.1.0 Introduced on S-Series
Version 7.6.1.0 Introduced on C-Series
pre-Version 6.2.1.1 Introduced on E-Series

Usage Information

If you want the interface to receive both versions of RIP, enter ip rip receive version 1 2.

Related Commands

ip rip send version Sets the RIP version to be used for sending RIP traffic on an interface.
version Sets the RIP version to be used for the switch software.

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 the ROUTER RIP mode.

Syntax

ip rip send version [1] [2]

To return to the default value, enter no ip rip send version.

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**

<table>
<thead>
<tr>
<th>Command History</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

To enable the interface to send both version of RIP packets, enter `ip rip send version 1 2`.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip rip receive version</code></td>
<td>Sets the RIP version for the interface to receive traffic.</td>
</tr>
<tr>
<td><code>version</code></td>
<td>Sets the RIP version to be used for the switch software.</td>
</tr>
</tbody>
</table>

---

**ip split-horizon**

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

**Syntax**

`ip split-horizon`

**Defaults**

Enabled

**Command Modes**

<table>
<thead>
<tr>
<th>Command History</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip poison-reverse</code></td>
<td>Set the prefix for RIP routing updates.</td>
</tr>
</tbody>
</table>

---

**maximum-paths**

Set RIP to forward packets over multiple paths.

**Syntax**

`maximum-paths number`

**Parameters**

- `number` Enter the number of paths.
  
  Range: 1 to 16.
  
  The default is 4 paths.

**Defaults**

4

**Command Modes**

| ROUTER RIP |}

```markdown
Router Information Protocol (RIP)
```

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>ROUTER RIP</th>
</tr>
</thead>
</table>

---
neighbor

Define a neighbor router with which to exchange RIP information.

Syntax

neighbor ip-address

To delete a neighbor setting, use the no neighbor ip-address command.

Parameters

ip-address Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults

Not configured.

Command Modes

ROUTER RIP

Usage Information

When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible.

Use the passive-interface command in conjunction with the neighbor command to ensure that only specific interfaces are receiving and sending data.

Related Commands

passive-interface Sets the interface to only listen to RIP broadcasts.

network

Enable RIP for a specified network. Use this command to enable RIP on all networks connected to the switch.

Syntax

network ip-address

To disable RIP for a network, use the no network ip-address command.

Parameters

ip-address Specify an IP network address in dotted decimal format. You cannot specify a subnet.

Defaults

No RIP network is configured.

Command Modes

ROUTER RIP
offset-list

Specify a number to add to the incoming or outgoing route metrics learned via RIP.

Syntax

offset-list prefix-list-name {in | out} offset [interface]

To delete an offset list, use the no offset-list prefix-list-name {in | out} offset [interface] command.

Parameters

- prefix-list-name: Enter the name of an established Prefix list to determine which incoming routes will be modified.
- offset: Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified.
  If you set an offset value to zero (0), no action is taken.
- interface: (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For a Port Channel interface, enter the keyword port-channel followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword sonet followed by the 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.
  - 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 8.4.6.0: Added support for the keyword fortyGigE.
- Version 7.6.1.0: Introduced on C-Series
- Version 7.8.1.0: Introduced on S-Series
- Pre-Version 6.2.1.1: Introduced on E-Series

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.
### output-delay

Set the interpacket delay of successive packets to the same neighbor.

**Syntax**

```plaintext
output-delay delay
```

To return to the switch software defaults for interpacket delay, enter `no output-delay`.

**Parameters**

- **delay**
  - Specify a number of milliseconds as the delay interval.
  - Range: 8 to 50.

**Default**

Not configured.

**Command Modes**

- ROUTER RIP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>Pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

This command is intended for low-speed interfaces.

### passive-interface

Suppress routing updates on a specified interface.

**Syntax**

```plaintext
passive-interface interface
```

To delete a passive interface, use the `no passive-interface interface` command.

**Parameters**

- **interface**
  - Enter the following information:
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
      - **C-Series** and **S-Series**: Range: 1-128
      - **E-Series**: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword `sonet` followed by the 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.
    - For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

Not configured.
Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in RIP updates sent via other interfaces.

Related Commands

- **neighbor** - Enable RIP for a specified network.
- **network** - Define 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 7.8.1.0** - Introduced on S-Series
- **Version 7.6.1.0** - Introduced on C-Series
- **pre-Version 6.2.1.1** - Introduced on E-Series

To redistribute the default route (0.0.0.0/0), configure the **default-information originate** command.

**Related Commands**

- **default-information originate** - Generate a default route for RIP traffic.

**redistribute isis**

Redistribute routing information from an IS-IS instance.

**Syntax**

```
redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]
```

To disable redistribution, use the **no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]** command.
**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, enter 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 indicate 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

---

**Router Information Protocol (RIP)**

- **Router Information Protocol (RIP)**
- **www.dell.com | support.dell.com**
- **Parameters**
  - **Defaults**
    - Not configured.
  - **Command Modes**
    - ROUTER RIP
  - **Command History**
    - Introduced on E-Series, pre-Version 6.2.1.1
  - **Usage Information**
    - IS-IS is not supported on S-Series systems.

**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, enter 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 indicate 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
router rip

Enter the ROUTER RIP mode to configure and enable RIP.

Syntax  router rip

To disable RIP, enter no router rip.

Defaults  Disabled.

Command Modes  CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

To enable RIP, you must assign a network address using the network command.

Example

Figure 48-1.  router rip Command Example

FTOS(conf)#router rip
FTOS(conf-router_rip)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>Enable RIP.</td>
</tr>
<tr>
<td>exit</td>
<td>Return to the CONFIGURATION mode.</td>
</tr>
</tbody>
</table>

show config

Display the changes you made to the RIP configuration. Default values are not shown.

Syntax  show config

Command Modes  ROUTER RIP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
show ip rip database

Display the routes learned by RIP. If the switch learned no RIP routes, no output is generated.

**Syntax**

```
show ip rip database [ip-address mask]
```

**Parameters**

- `ip-address` (OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only.
  
  If you enter an IP address, you must also enter a mask for that IP address.

- `mask` (OPTIONAL) Specify a mask, in /network format, for the IP address.

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 48-3.  show ip rip database Command Example (partial)**

```
FTOS#show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
   [50/1] via 192.14.1.3, 00:00:12, GigabitEthernet 9/15
   auto-summary
204.250.54.0/24
203.250.49.0/24
   [50/1] via 192.13.1.3, 00:00:12, GigabitEthernet 9/14
   auto-summary
203.250.49.0/24
210.250.40.0/24
   [50/2] via 1.1.18.2, 00:00:14, Vlan 18
   auto-summary
   [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
210.250.40.0/24
207.250.53.0/24
   [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
   auto-summary
   [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
   [50/2] via 1.1.10.2, 00:00:18, Vlan 10
207.250.53.0/24
208.250.42.0/24
   [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
   [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
   [50/2] via 1.1.10.2, 00:00:18, Vlan 10
208.250.42.0/24
```

**Example**

**Figure 48-2.  show config Command Example in ROUTER RIP Mode**

```
FTOS(conf-router_rip)#show config
!
router rip
network 172.31.0.0
passive-interface GigabitEthernet 0/1
FTOS(conf-router_rip)#
```
**Router Information Protocol (RIP)**

**show running-config rip**

Use this feature to display the current RIP configuration.

**Syntax**

```
show running-config rip
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Example**

```
Figure 48-4.  show running-config rip Command Example

show running-config rip
  !
  router rip
  distribute-list Test1 in
distribute-list Test21 out
  network 10.0.0.0
  passive-interface GigabitEthernet 2/0
  neighbor 20.20.20.20
  redistribute ospf 999
  version 2
```

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**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, enter `no timers basic`.

---

**Table 48-1.  Fields in show ip rip database Command Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of routes in RIP database</td>
<td>Displays the number of RIP routes stored in the RIP database.</td>
</tr>
<tr>
<td>100.10.10.0/24 directly connected</td>
<td>Lists the route(s) directly connected.</td>
</tr>
<tr>
<td>150.100.0.0 redistributed</td>
<td>Lists the routes learned through redistribution.</td>
</tr>
<tr>
<td>209.9.16.0/24...</td>
<td>Lists the routes and the sources advertising those routes.</td>
</tr>
</tbody>
</table>
**Parameters**

*update* Enter the number of seconds to specify the rate at which RIP routing updates are sent.
- Range: zero (0) to 4294967295.
- Default: 30 seconds.

*invalid* Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The *invalid* value should be at least three times the *update* timer value.
- Range: zero (0) to 4294967295.
- Default: 180 seconds.

*holddown* Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The *holddown* value should be at least three times the *update* timer value.
- Range: zero (0) to 4294967295.
- Default: 180 seconds.

*flush* 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 *flush* value should be greater than the *update* value.
- Range: zero (0) to 4294967295.
- Default is 240 seconds.

**Defaults**

*update* = 30 seconds; *invalid* = 180 seconds; *holddown* = 180 seconds; *flush* = 240 seconds.

**Command Modes**

ROUTER RIP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If the timers on one router are changed, 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, enter no version.

**Parameters**

*1* Enter the keyword 1 to specify RIP version 1.

*2* Enter the keyword 2 to specify RIP version 2.

**Default**

The FTOS sends RIPv1 and receives RIPv1 and RIPv2.

**Command Modes**

ROUTER RIP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ip rip receive version</td>
<td>Set the RIP version to be received on the interface.</td>
</tr>
<tr>
<td>ip rip send version</td>
<td>Set the RIP version to be sent out the interface.</td>
</tr>
</tbody>
</table>
Remote Monitoring (RMON)

Overview

Dell Networking OS RMON is implemented on all Dell Networking switching platforms (C-Series, E-Series, and S-Series), as indicated by the characters that appear below each command heading:

- C-Series: C
- E-Series: E
- S-Series: S

Dell Networking OS RMON is based on IEEE standards, providing both 32-bit and 64-bit monitoring, and long-term statistics collection. Dell Networking OS 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

Dell Networking OS RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization

Note: Only SNMP GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

Commands

The Dell Networking OS Remote Network Monitoring RMON commands are:

- rmon alarm
- rmon collection history
- rmon collection statistics
- rmon event
rmon alarm

Set an alarm on any MIB object.

Syntax

\texttt{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 \texttt{no rmon 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 32 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 \texttt{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 \texttt{absolute} to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.</td>
</tr>
<tr>
<td>rising-threshold</td>
<td>Enter the keyword \texttt{rising-threshold} followed by the value (32bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.</td>
</tr>
<tr>
<td>event-number</td>
<td></td>
</tr>
<tr>
<td>falling-threshold</td>
<td>Enter the keyword \texttt{falling-threshold} followed by the value (32bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.</td>
</tr>
<tr>
<td>event-number</td>
<td></td>
</tr>
<tr>
<td>owner string</td>
<td>(OPTIONAL) Enter the keyword \texttt{owner} followed by the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.</td>
</tr>
</tbody>
</table>

Default

owner

Command Modes

CONFIGURATION
Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

rmon collection history

Syntax

```markdown
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

rmon collection statistics

Syntax

```markdown
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.
rmon event

Add an event in the RMON event table.

Syntax

rmon event number [log] [trap community] [description string] [owner name]

To disable RMON on an interface, use the no rmon event number [log] [trap community] [description string] command.

Parameters

number Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON Event Table.

log (OPTIONAL) Enter the keyword log to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. Default: No log

trap community (OPTIONAL) Enter the keyword trap followed by an SNMP community string to configure the eventType setting in the RMON MIB. This sets either snmp-trap or log-and-trap. Default: public

description string (OPTIONAL) Enter the keyword description followed by a string describing the event.

owner name (OPTIONAL) Enter the keyword owner followed by the name of the owner of this event.

Defaults

as described above

Command Modes

CONFIGURATION

Command History

Version 7.6.1.0 Support added for S-Series
Version 7.5.1.0 Support added for C-Series
Version 6.1.1.0 Introduced for E-Series
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>
<tr>
<td>rising-threshold value event-number</td>
<td>Enter the keyword rising-threshold followed by the value (64 bit) 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>falling-threshold value event-number</td>
<td>Enter the keyword falling-threshold followed by the value (64 bit) 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>owner string</td>
<td>(OPTIONAL) Enter the keyword owner followed 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>

Defaults

owner

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

show rmon

Display the RMON running status including the memory usage.

Syntax  show rmon

Defaults  No default behavior
Example

**show rmon alarms**

Display the contents of the RMON Alarm Table.

**Syntax**

```
show rmon alarms [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 Alarm Table in an easy-to-read format.

**Defaults**

No default behavior

**Command Modes**

EXEC

**Command History**

- **Version 7.6.1.0** Support added for S-Series
- **Version 7.5.1.0** Support added for C-Series
- **Version 6.1.1.0** Introduced for E-Series

**Example 1**

**Figure 49-2.  show rmon alarms index Command Example**

```
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#
```
### 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

No default behavior

#### Command Modes

EXEC

#### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

#### Example 1

**Figure 49-4. show rmon event index Command Example**

```plaintext
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#
```
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**

No default behavior

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example 1**

**Figure 49-6. 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#
```
**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**

No default behavior

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example 1**

Figure 49-8.  show rmon history index Command Example

```
FTOS#show rmon history 6001
RMON history control entry 6001
  interface: ifIndex.100974631 GigabitEthernet 2/0
  bucket requested: 1
  bucket granted: 1
  sampling interval: 5 sec
  owner: 1
  status: OK
FTOS#
```
show rmon log

Command: show rmon log [index] [brief]

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: No default behavior

Command Modes: EXEC

Command History:

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

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 1

Example 2
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

No default behavior

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Example 1

Figure 49-12. show rmon statistics index Command Example

FTOS#show rmon statistics 6001
RMON statistics entry 6001
  interface: ifIndex.100974631 GigabitEthernet 2/0
  packets dropped: 0
  bytes received: 0
  packets received: 0
  broadcast packets: 0
  multicast packets: 0
  CRC error: 0
  under-size packets: 0
  over-size packets: 0
  fragment errors: 0
  jabber errors: 0
  collision: 0
  64bytes packets: 0
  65-127 bytes packets: 0
  128-255 bytes packets: 0
  256-511 bytes packets: 0
  512-1023 bytes packets: 0
  1024-1518 bytes packets: 0
  owner: 1
  status: OK
  <high-capacity data>
  HC packets received overflow: 0
  HC packets received: 0
  HC bytes received overflow: 0
  HC bytes received: 0
  HC 64bytes packets overflow: 0
  HC 64bytes packets: 0
  HC 65-127 bytes packets overflow: 0
  HC 65-127 bytes packets: 0
  HC 128-255 bytes packets overflow: 0
  HC 128-255 bytes packets: 0
  HC 256-511 bytes packets overflow: 0
  HC 256-511 bytes packets: 0
  HC 512-1023 bytes packets overflow: 0
  HC 512-1023 bytes packets: 0
  HC 1024-1518 bytes packets overflow: 0
  HC 1024-1518 bytes packets: 0
FTOS#
### Example 2

**Figure 49-13. show rmon statistics brief Command Example**

```
FTOS#show rmon statistics br
index     ifIndex     interface
-----------------------------------------------
6001       100974631   GigabitEthernet 2/0
6002       100974631   GigabitEthernet 2/0
6003       101236775   GigabitEthernet 2/1
6004       101236775   GigabitEthernet 2/1
9001       134529054   GigabitEthernet 3/0
9002       134529054   GigabitEthernet 3/0
9003       134791198   GigabitEthernet 3/1
9004       134791198   GigabitEthernet 3/1
FTOS#
```
Rapid Spanning Tree Protocol (RSTP)

Overview

The Dell Networking OS implementation of RSTP (Rapid Spanning Tree Protocol) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a bridged LAN that is comprised of LANs interconnected by bridges.

RSTP is supported by Dell Networking OS on all Dell Networking systems, as indicated by the characters that appear below each command heading:

- C-Series: C
- E-Series: E
- S-Series: S

Commands

The Dell Networking OS RSTP commands are:

- bridge-priority
- debug spanning-tree rstp
- description
- description
- forward-delay
- hello-time
- max-age
- protocol spanning-tree rstp
- show config
- show spanning-tree rstp
- spanning-tree rstp
- tc-flush-standard

bridge-priority

Set the bridge priority for RSTP.

Syntax

```
bridge-priority priority-value
```

To return to the default value, enter `no bridge-priority`. 
debug spanning-tree rstp

Enable debugging of RSTP and view information on the protocol.

Syntax

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

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 Fast Ethernet interface, enter the keyword FastEthernet followed by the slot/port information.
    - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
    - For a Port Channel interface, enter the keyword port-channel followed by a number:
      - C-Series and S-Series Range: 1-128
      - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword sonet followed by the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet 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 7.6.1.0 Support added for S-Series
description

Enter a description of the Rapid Spanning Tree.

Syntax
description {description}

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

Parameters

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

Defaults

No default behavior or values.

Command Modes

- SPANNING TREE (The prompt is “config-rstp.”)

Command History

- pre-7.7.1.0: Introduced

Related Commands

- protocol spanning-tree rstp: Enter SPANNING TREE mode on the switch.

disable

Disable RSTP globally on the system.

Syntax
disable

To enable Rapid Spanning Tree Protocol, enter no disable.

Defaults

RSTP is disabled.

Command Modes

- CONFIGURATION RSTP (conf-rstp)

Command History

- Version 7.5.1.0: Support added for C-Series
- Version 7.6.1.0: Support added for S-Series
- Version 7.5.1.0: Support added for C-Series
- Version 6.2.1.1: Introduced for E-Series

Related Commands

- protocol spanning-tree rstp: Enter the Rapid Spanning Tree mode.
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, enter `no forward-delay`.

Parameters

- **seconds**: Enter the number of seconds that Dell Networking OS waits before transitioning RSTP to the forwarding state.
  - Range: 4 to 30
  - Default: 15 seconds

Defaults

15 seconds

Command Modes

- **CONFIGURATION RSTP (conf-rstp)**

Command History

- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 6.2.1.1 Introduced for E-Series

Related Commands

- **hello-time**: Change the time interval between BPDUs.
- **max-age**: Change the wait time before RSTP refreshes protocol configuration information.

hello-time

Set the time interval between generation of RSTP Data Units (BPDUs).

Syntax

```
hello-time [milli-second] seconds
```

To return to the default value, enter `no hello-time`.

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 8.3.1.0 Added **milli-second** to S-Series.
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 6.2.1.1 Introduced for E-Series
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 \((x/1000)\times 256\).

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** Change the wait time before RSTP transitions to the Forwarding state.
- **max-age** Change the wait time before RSTP refreshes protocol configuration information.

## max-age

**Syntax**

```
max-age seconds
```

To return to the default values, enter `no max-age`.

**Parameters**

- **max-age** Enter a number of seconds the Dell Networking OS waits before refreshing configuration information.
  - Range: 6 to 40 seconds
  - Default: 20 seconds

**Defaults**

20 seconds

**Command Modes**

CONFIGURATION RSTP (conf-rstp)

**Command History**

- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 6.2.1.1 Introduced for E-Series

**Related Commands**

- **max-age** Change the wait time before RSTP transitions to the Forwarding state.
- **hello-time** Change 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, enter **exit**

**Defaults**

Not configured

**Command Modes**

CONFIGURATION RSTP (conf-rstp)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

RSTP is not enabled when you enter the RSTP mode. To enable RSTP globally on the system, enter **no description** from the RSTP mode.

**Related Commands**

- **description**
  
  Disable RSTP globally on the system.

**show config**

View the current configuration for the mode. Only non-default values are displayed.

**Syntax**

```
show config
```

**Command Modes**

CONFIGURATION RSTP (conf-rstp)

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>(OPTIONAL) Enter the keyword <code>brief</code> to view a synopsis of the RSTP configuration information.</td>
</tr>
<tr>
<td>guard</td>
<td>(OPTIONAL) Enter the keyword <code>guard</code> to display the type of guard enabled on an RSTP interface and the current port state.</td>
</tr>
</tbody>
</table>

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 8.5.1.0 Support for the optional `guard` keyword was added on the E-Series ExaScale.
- Version 8.4.2.1 Support for the optional `guard` keyword was added on the C-Series, S-Series, and E-Series TeraScale.
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- Version 6.4.1.0 Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency
- Version 6.2.1.1 Introduced for E-Series

**Example 1**

Figure 50-4. 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

Interface Name   PortID   Prio Cost    Sts Cost    Bridge ID
----------------- -------- ---- ------- --------- --------------------
Gi 4/0           128.418 128  20000   FWD 20000   16384 0001.e801.6aa8 128.418
Gi 4/1           128.419 128  20000   FWD 20000   16384 0001.e801.6aa8 128.419
Gi 4/8           128.426 128  20000   FWD 20000   8192  0001.e805.e306 128.130
Gi 4/9           128.427 128  20000   BLK 20000   8192  0001.e805.e306 128.131

Interface Name   Role    PortID   Prio Cost    Sts Cost    Link-type Edge
----------------- ------ -------- ---- ------- --------- ----------
Gi 4/0           Desg   128.418 128  20000   FWD 20000   P2P       Yes
Gi 4/1           Desg   128.419 128  20000   FWD 20000   P2P       Yes
Gi 4/8           Root   128.426 128  20000   FWD 20000   P2P       No
Gi 4/9           Altr   128.427 128  20000   BLK 20000   P2P       No
```

FTOS#
Figure 50-5. 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

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts</th>
<th>Cost</th>
<th>Bridge ID</th>
<th>PortID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 0/0</td>
<td>128.257</td>
<td>128</td>
<td>20000</td>
<td>EDS</td>
<td>0</td>
<td>32768 0001.e801.6aa8</td>
<td>128.257</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Role</th>
<th>PortID</th>
<th>Prio</th>
<th>Cost</th>
<th>Sts</th>
<th>Cost</th>
<th>Link-type</th>
<th>Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 0/0</td>
<td>ErrDis</td>
<td>128.257</td>
<td>128</td>
<td>20000</td>
<td>EDS</td>
<td>0</td>
<td>P2P</td>
<td>No</td>
</tr>
</tbody>
</table>

FTOS#show spanning-tree rstp
Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 0
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 0
We are the root
Current root has priority 32768, Address 0001.e801.6aa8
Number of topology changes 1, last change occurred 00:00:31 ago on Gi 0/0
Port 257 (GigabitEthernet 0/0) is LBK INC Discarding
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU : sent 27, received 9
The port is not in the Edge port mode

Example 3 Figure 50-6. show spanning-tree rstp guard Command Example

FTOS#show spanning-tree rstp guard

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Instance</th>
<th>Sts</th>
<th>Guard type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 0/1</td>
<td>0</td>
<td>INCON(Root)</td>
<td>Rootguard</td>
</tr>
<tr>
<td>Gi 0/2</td>
<td>0</td>
<td>FWD</td>
<td>Loopguard</td>
</tr>
<tr>
<td>Gi 0/3</td>
<td>0</td>
<td>BLK</td>
<td>Bpduguard</td>
</tr>
</tbody>
</table>

Table 50-1. show spanning-tree rstp guard Command Information

<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), 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>
spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional Bridge Port Data Unit (BPDU) guard, port priority, loop guard, or root guard.

**Syntax**

```
spanning-tree rstp {cost port-cost | edge-port [bpdu-guard [shutdown-on-violation]] | priority priority | {loopguard | rootguard}}
```

**Parameters**

- **cost port-cost**
  - Enter the keyword `cost` followed by the port cost value.
  - Range: 1 to 200000
  - Defaults:
    - 100 Mb/s Ethernet interface = 200000
    - 1-Gigabit Ethernet interface = 20000
    - 10-Gigabit Ethernet interface = 2000
    - 40-Gigabit Ethernet interface = 1400
    - Port Channel interface with one 100 Mb/s Ethernet = 200000
    - Port Channel interface with one 1-Gigabit Ethernet = 20000
    - Port Channel interface with one 10-Gigabit Ethernet = 2000
    - Port Channel with two 1-Gigabit Ethernet = 18000
    - Port Channel with two 10-Gigabit Ethernet = 1800
    - Port Channel with two 100-Mbps Ethernet = 180000

- **edge-port**
  - Enter the keyword `edge-port` to configure the interface as a Rapid Spanning Tree edge port.

- **bpdu-guard**
  - (OPTIONAL) Enter the keyword `bpdu-guard` 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.

- **priority priority**
  - Enter keyword `priority` followed by a value in increments of 16 as the priority.
  - Range: 0 to 240. Default: 128

- **loopguard**
  - Enter the keyword `loopguard` to enable loop guard on an RSTP port or port-channel interface.

- **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 8.5.1.0  Introduced the **loopguard** and **rootguard** options on the E-Series ExaScale.
- Version 8.4.2.1  Introduced the **loopguard** and **rootguard** options on the E-Series TeraScale, C-Series, and S-Series.
- Version 8.2.1.0  Introduced hardware shutdown-on-violation options
- Version 7.6.1.0  Support added for S-Series
- Version 7.5.1.0  Support added for C-Series
- Version 7.4.1.0  Added the optional Bridge Port Data Unit (BPDU) guard.
- Version 6.2.1.1  Introduced for E-Series
The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, 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.

**Note:** A port configured as an edge port, on an RSTP switch, will immediately transition 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 **shutdown-on-violation** is not enabled, BPDUs will still be sent to the RPM CPU.

STP 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:

```plaintext
% 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 50-7. spanning-tree rstp edge-port Command**

```plaintext
FTOS(conf)#interface gigabitethernet 4/0
FTOS(conf-if-gi-4/0)#spanning-tree rstp edge-port
FTOS(conf-if-gi-4/0)#show config
! interface GigabitEthernet 4/0
   no ip address
   switchport
   spanning-tree rstp edge-port
   no shutdown
FTOS#
```
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

By default Dell Networking OS 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, this knob command can be turned on to enable flushing MAC addresses upon receiving every topology change notification.
Security

Overview

Except for the Trace List feature (E-Series only), most of the commands in this chapter are available on all three Dell Networking platforms — C-Series, E-Series, and S-Series (the S-Series models that run FTOS), as noted by the following icons that appear under each command icon:

Commands

This chapter contains various types of security commands in Dell Networking OS, in the following sections:

- AAA Accounting Commands
- Authorization and Privilege Commands
- Authentication and Password Commands
- RADIUS Commands
- TACACS+ Commands
- Port Authentication (802.1X) Commands
- SSH Server and SCP Commands
- Trace List Commands
- Secure DHCP Commands

For configuration details, see the Security chapter in the Dell Networking OS Configuration Guide.

Note: Starting with Dell Networking OS v7.2.1.0, 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 AAA Accounting is enabled, the network server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record is comprised of accounting 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 apply that list to various interfaces. The commands are:

- `aaa 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. Dell Networking OS currently only supports TACACS+ accounting.

Defaults

No default configuration or behavior

Command Modes

- **CONFIGURATION**

Command History

- **Version 7.6.1.0** Introduced for S-Series
- **Version 7.5.1.0** Introduced for C-Series
- **Version 6.3.1.0** Introduced for E-Series

Example

```
FTOS(conf)# aaa accounting exec default start-stop tacacs+
FTOS(conf)# aaa accounting command 15 default start-stop tacacs+
Dell Networking OS (config)#
```

Usage Information

In the example above, 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable password</td>
<td>Change the password for the enable command.</td>
</tr>
<tr>
<td>login authentication</td>
<td>Enable AAA login authentication on terminal lines.</td>
</tr>
<tr>
<td>password</td>
<td>Create a password.</td>
</tr>
<tr>
<td>tacacs-server host</td>
<td>Specify a TACACS+ server host.</td>
</tr>
</tbody>
</table>

### 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 7.6.1.0** Introduced for S-Series
- **Version 7.5.1.0** Introduced for C-Series
- **Version 6.3.1.0** Introduced

### Usage Information

Dell Networking OS 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exec</td>
<td>Enter this keyword to apply an EXEC level accounting method list.</td>
</tr>
<tr>
<td>commands level</td>
<td>Enter this keyword to apply an EXEC and CONFIGURATION level accounting method list.</td>
</tr>
<tr>
<td>method-list</td>
<td>Enter a method list that you defined using the command <code>aaa accounting exec</code> or <code>aaa accounting commands</code>.</td>
</tr>
</tbody>
</table>

#### Defaults

None

#### Command Modes

- **LINE**
show accounting

Syntax

Usage Information

Example

Figure 51-2. show accounting Command Example

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.
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}
```

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 7.6.1.0** Introduced for S-Series
- **Version 7.5.1.0** Introduced for C-Series
- **Version 6.1.1.0** Added support for RADIUS

Usage Information:

- `aaa authorization commands`: Set parameters that restrict (or permit) a user’s access to EXEC and CONFIGURATION level commands.
- `aaa authorization exec`: Set parameters that restrict (or permit) a user’s access to EXEC level commands.

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 7.6.1.0** Introduced for S-Series
- **Version 7.5.1.0** Introduced for C-Series
- **Version 6.3.1.0** Introduced on E-Series

Usage Information:

- `aaa authorization commands`: Set parameters that restrict (or permit) a user’s access to EXEC and CONFIGURATION level commands.
- `aaa authorization exec`: Set parameters that restrict (or permit) a user’s access to EXEC level commands.
aaa authorization config-commands

Set parameters that restrict (or permit) a user’s access to EXEC level commands.

Syntax

```
aaa authorization config-commands
```

Disable authorization checking for CONFIGURATION level commands using the command `no aaa authorization config-commands`.

Defaults

Enabled when you configure `aaa authorization commands`.

Command Modes

`CONFIGURATION`

Command History

- Version 7.5.1.0 Introduced for E-Series

Usage Information

By default, the command `aaa authorization commands` configures the system to check both EXEC level and CONFIGURATION level commands. Use the command `no aaa authorization config-commands` to enable only EXEC-level command checking.

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}
```

Disable authorization checking for EXEC level commands using the command `no aaa authorization exec`.

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Define a name for the list of authorization methods.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Define the default list of authorization methods.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>Use the authorization parameters on the system to perform authorization.</td>
</tr>
<tr>
<td><code>tacacs+</code></td>
<td>Use the TACACS+ protocol to perform authorization.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Enter this keyword to apply no authorization.</td>
</tr>
</tbody>
</table>

Defaults

None

Command Modes

`CONFIGURATION`

Command History

- Version 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- Version 6.1.1.0 Added support for RADIUS
privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

Syntax

```
privilege mode {level level | reset}
```

To delete access to a level and command, use the `no privilege mode level level` 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, ROUTER ISIS 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

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

Use the `enable password` command to define a password for the level to which you are assigning privilege or access.

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 and commands.

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]
```

To return to the default setting, use the `no aaa authentication enable {default | method-list-name} method [... method2]` command.

**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.
Use the enable password.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
<td></td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Information**

By default, the Enable password is used. If `aaa authentication enable default` is configured, Dell Networking OS will use 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, Dell Networking OS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, Dell Networking OS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable password</td>
<td>Change the password for the enable command.</td>
</tr>
<tr>
<td>login authentication</td>
<td>Enable AAA login authentication on terminal lines.</td>
</tr>
<tr>
<td>password</td>
<td>Create a password.</td>
</tr>
<tr>
<td>radius-server host</td>
<td>Specify a RADIUS server host.</td>
</tr>
<tr>
<td>tacacs-server host</td>
<td>Specify a TACACS+ server host.</td>
</tr>
</tbody>
</table>

**aaa authentication login**

Configure AAA Authentication method lists for user access to the EXEC mode (Enable log-in).

**Syntax**

`aaa authentication login {method-list-name | default} method [... method4]`

To return to the default setting, use the `no aaa authentication login {method-list-name | default}` command.

**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 <code>default</code> 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, Dell Networking OS applies the next configured method (up to four configured methods).

Default

Not configured (that is, no authentication is performed)

Command Modes

**CONFIGURATION**

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

By default, the locally configured **username password** will be used. If **aaa authentication login default** is configured, Dell Networking OS will use 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, Dell Networking OS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, Dell Networking OS 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, configure the **login authentication** command to enable the authentication scheme on terminal lines.

Connections to the SSH server will work with the following login mechanisms: local, radius and tacacs.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>login authentication</strong></td>
<td>Apply an authentication method list to designated terminal lines.</td>
</tr>
<tr>
<td><strong>password</strong></td>
<td>Create a password.</td>
</tr>
<tr>
<td><strong>radius-server host</strong></td>
<td>Specify a RADIUS server host.</td>
</tr>
<tr>
<td><strong>tacacs-server host</strong></td>
<td>Specify 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 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

**Related Commands**

- `line` — Apply an authentication method list to designated terminal lines.
- `ip access-list standard` — Name (or select) a standard access list to filter based on IP address.
- `ip access-list extended` — Name (or select) 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.

**Defaults**

No password is configured. `level = 15`

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series
Usage Information

Use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command to control access to command modes.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, you must use CNTL + v prior to entering regular expression. For example, to create the password `abcd\]e`, you type “`abcd CNTL v ] e`”. When the password is created, you do not use the CNTL + v key combination and enter “`abcd ] e`”.

**Note:** The question mark (?) and the tilde (~) are not supported characters.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>View the current configuration.</td>
</tr>
<tr>
<td><code>privilege level (CONFIGURATION mode)</code></td>
<td>Control access to command modes within the switch.</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>level level</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>level</strong> followed by a number as the level of access. Range: 1 to 15</td>
</tr>
<tr>
<td><strong>encryption-type</strong></td>
<td>(OPTIONAL) Enter the number 5 or 0 as the encryption type. Enter a 5 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 <code>show running-config</code> file of another Dell Force10 router.</td>
</tr>
<tr>
<td><strong>password</strong></td>
<td>Enter a text string, up to 32 characters long, as the clear text password.</td>
</tr>
</tbody>
</table>

### Defaults

No password is configured. **level** = 15

### Command Modes

**CONFIGURATION**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

### Usage Information

Use this command to define a password for a level and 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\]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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>View the current configuration.</td>
</tr>
<tr>
<td><code>privilege level</code> (CONFIGURATION mode)</td>
<td>Control access to command modes within the E-Series.</td>
</tr>
</tbody>
</table>

### 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, enter `no login authentication`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>method-list-name</strong></td>
<td>Enter the <code>method-list-name</code> to specify that method list, created in the <code>aaa authentication login</code> command, to be applied to the designated terminal line.</td>
</tr>
<tr>
<td><strong>default</strong></td>
<td>Enter the keyword <code>default</code> to specify that the default method list, created in the <code>aaa authentication login</code> command, is applied to the terminal line.</td>
</tr>
</tbody>
</table>

**Defaults**

No authentication is performed on the console lines, and local authentication is performed on the virtual terminal and auxiliary lines.
If you configure the `aaa authentication login default` command, then the `login authentication default` command automatically is applied to all terminal lines.

Related Commands

- `aaa authentication login` Select 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 text 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**

<table>
<thead>
<tr>
<th>Version 7.6.1.0</th>
<th>Introduced for S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>Pre-Version 6.2.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Dell Networking OS prompts users for these passwords when the method for authentication or authorization used is “line”.

**Related Commands**

- `enable password` Set the password for the `enable` command.
- `login authentication` Configure an authentication method to log in to the switch.
- `service password-encryption` Encrypt all passwords configured in Dell Networking OS.
- `radius-server key` Configure a key for all RADIUS communications between the switch and the RADIUS host server.
- `tacacs-server key` Configure a key for communication between a TACACS+ server and client.
- `username` Establish an authentication system based on user names.
**password-attributes**

Configure the password attributes (strong password).

**Syntax**

```
password-attributes [min-length number] [max-retry number] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]
```

To return to the default, use the no password-attributes [min-length number] [max-retry number] [character-restriction [upper number] [lower number] [numeric number] [special-char number]] command.

**Parameters**

- **min-length number** (OPTIONAL) Enter the keyword min-length followed by the number of characters.
  Range: 0 - 32 characters
- **max-retry number** (OPTIONAL) Enter the keyword max-retry followed by the number of maximum password retries.
  Range: 0 - 16
- **character-restriction** (OPTIONAL) Enter the keyword character-restriction to indicate a character restriction for the password.
- **upper number** (OPTIONAL) Enter the keyword upper followed the upper number.
  Range: 0 - 31
- **lower number** (OPTIONAL) Enter the keyword lower followed the lower number.
  Range: 0 - 31
- **numeric number** (OPTIONAL) Enter the keyword numeric followed the numeric number.
  Range: 0 - 31
- **special-char number** (OPTIONAL) Enter the keyword special-char followed the number of special characters permitted.
  Range: 0 - 31

**Defaults**

No default values or behavior

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- Version 7.4.1.0 Introduced

**Related Commands**

- **password** Specify a password for users on terminal lines.

---

**service password-encryption**

Encrypt all passwords configured in FTOS.

**Syntax**

```
service password-encryption
```

To store new passwords as clear text, enter no service password-encryption.

**Defaults**

Enabled
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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
<td></td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
FTOS#show privilege
Current privilege level is 15
FTOS#
```

**Related Commands**

- `privilege level (CONFIGURATION mode)` — Assign access control to different command modes.

### show users

View information on all users logged into the switch.

**Syntax**

```
show users [all]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(OPTIONAL) Enter the keyword <code>all</code> to view all terminal lines in the switch.</td>
</tr>
</tbody>
</table>
Table 1 describes the information in the `show users` command example.

### Table 1  show users Command Example Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(untitled)</td>
<td>Indicates with a * 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Enable a user.</td>
</tr>
</tbody>
</table>

### timeout login response

Specify how long the software will wait for login input (for example, user name and password) before timing out.

**Syntax**

```
timeout login response seconds
```

To return to the default values, enter `no timeout login response`.

**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

**Command Modes**

- **LINE**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
The software measures the period of inactivity defined in this command as the period between consecutive keystrokes. For example, if your password is "password" you can enter "p" and wait 29 seconds to enter the next letter.

**username**

Establish an authentication system based on user names.

**Syntax**

```
username name [access-class access-list-name] [nopassword | {password | secret; [encryption-type] password}] [privilege level]
```

If you do not want a specific user to enter a password, use the **nopassword** option.

To delete authentication for a user, use the **no username name** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Enter a text string for the name of the user up to 63 characters.</td>
</tr>
<tr>
<td>access-class</td>
<td>Enter the keyword <strong>access-class</strong> followed by the name of a configured access control list (either a IP access control list or MAC access control list).</td>
</tr>
<tr>
<td>access-list-name</td>
<td>Enter the keyword <strong>access-class</strong> followed by the name of a configured access control list (either a IP access control list or MAC access control list).</td>
</tr>
<tr>
<td>nopassword</td>
<td>Enter the keyword <strong>nopassword</strong> to specify that the user should not enter a password.</td>
</tr>
<tr>
<td>password</td>
<td>Enter the keyword <strong>password</strong> followed by the <strong>encryption-type</strong> or the password.</td>
</tr>
<tr>
<td>secret</td>
<td>Enter the keyword <strong>secret</strong> followed by the <strong>encryption-type</strong> or the password.</td>
</tr>
<tr>
<td>encryption-type</td>
<td>Enter an encryption type for the <strong>password</strong> that you will enter.</td>
</tr>
<tr>
<td>privilege level</td>
<td>Enter the keyword <strong>privilege</strong> followed by a number from zero (0) to 15.</td>
</tr>
<tr>
<td>secret</td>
<td>Enter the keyword <strong>secret</strong> followed by the <strong>encryption-type</strong> or the password.</td>
</tr>
</tbody>
</table>

**Defaults**

The default encryption type for the **password** option is 0. The default encryption type for the **secret** option is 0.

**Command Modes**

**CONFIGURATION**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Added support for <strong>secret</strong> option and MD5 password encryption. Extended <strong>name</strong> from 25 characters to 63.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series original Command</td>
</tr>
</tbody>
</table>

**Usage Information**

To view the defined user names, use the **show running-config user** command.
RADIUS Commands

The RADIUS commands supported by FTOS are:

- debug radius
- ip radius source-interface
- radius-server deadtime
- radius-server host
- radius-server key
- radius-server retransmit
- radius-server timeout

**debug radius**

View RADIUS transactions to assist with troubleshooting.

**Syntax**

```
debug radius
```

To disable debugging of RADIUS, enter `no debug radius`.

**Defaults**

Disabled.

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**ip radius source-interface**

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

**Syntax**

```
ip radius source-interface interface
```

To delete a source interface, enter `no ip radius source-interface`. 
**radius-server deadtime**

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

**Syntax**

```
radius-server deadtime seconds
```

To disable this function or return to the default value, enter `no radius-server deadtime`.

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for the keyword fortyGigE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
Dell(config)#radius-server deadtime 120
Dell(config)#radius-server deadtime
Dell(config)#no radius-server deadtime
```
radius-server host

Configure a RADIUS server host.

Syntax

radius-server host {hostname | ipv4-address | ipv6-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 | ipv6-address

Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X), of the RADIUS server host.

auth-port port-number

(Optional) Enter the keyword auth-port followed by a number as the port number.

Range: zero (0) to 65535

The default port-number is 1812.

retransmit retries

(Optional) Enter the keyword retransmit followed by a number as the number of attempts. This parameter overwrites the radius-server retransmit command.

Range: zero (0) to 100

Default: 3 attempts

timeout seconds

(Optional) Enter the keyword timeout followed by the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the radius-server timeout command.

Range: 0 to 1000

Default: 5 seconds

key [encryption-type] key

(Optional) Enter the keyword key followed by an optional encryption-type and a string up to 42 characters long as the authentication key. This authentication key is used by the RADIUS host server and the RADIUS daemon operating on this switch.

For the encryption-type, enter either zero (0) or 7 as the encryption type for the key entered. The options are:

- 0 is the default and means the password is not encrypted and stored as clear text.
- 7 means that the password is encrypted and hidden.

Configure this parameter last because leading spaces are ignored.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 8.4.1.0 Added support for IPv6
Version 7.7.1.0 Authentication key length increased to 42 characters
Version 7.6.1.0 Support added for S-Series
Version 7.5.1.0 Support added for C-Series
pre-Version 6.2.1.1 Introduced on E-Series
Usage Information

Use this command to configure any number of RADIUS server hosts for each server host that is configured. FTOS searches for the RADIUS hosts in the order they are configured in the software.

The global default values for timeout, retransmit, and key optional parameters are applied, unless those values are specified in the radius-server host or other commands. If you configure timeout, retransmit, or key values, you must include those keywords when entering the no radius-server host command syntax to return to the global default values.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login authentication</td>
<td>Set the database to be checked when a user logs in.</td>
</tr>
<tr>
<td>radius-server key</td>
<td>Set a authentication key for RADIUS communications.</td>
</tr>
<tr>
<td>radius-server retransmit</td>
<td>Set the number of times the RADIUS server will attempt to send information.</td>
</tr>
<tr>
<td>radius-server timeout</td>
<td>Set the time interval before the RADIUS server times out.</td>
</tr>
</tbody>
</table>

radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

Syntax

radius-server key [encryption-type] key

To delete a password, enter no radius-server key.

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Authentication key length increased to 42 characters</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

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 Configure 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, enter `no radius-server retransmit`. To return to the default setting, enter `radius-server retransmit 3`.

**Parameters**

- `retries`:
  - Enter a number of attempts that Dell Networking OS tries to locate a RADIUS server.
  - Range: zero (0) to 100.
  - Default: 3 retries.

**Defaults**

3 retries

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- `radius-server host` Configure a RADIUS host.

radius-server timeout

Configure the amount of time the RADIUS client (the switch) waits for a RADIUS host server to reply to a request.

**Syntax**

```
radius-server timeout seconds
```

To return to the default value, enter `no radius-server timeout`.

**Parameters**

- `seconds`:
  - Enter the number of seconds between an unsuccessful attempt and the FTOS times out.
  - Range: zero (0) to 1000 seconds.
  - Default: 5 seconds.

**Defaults**

5 seconds

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- `radius-server host` Configure a RADIUS host.
**TACACS+ Commands**

FTOS supports TACACS+ as an alternate method for login authentication.

- debug tacacs+
- ip tacacs source-interface
- tacacs-server host
- tacacs-server key

### debug tacacs+

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

**Syntax**

```
ip tacacs source-interface interface
```

To delete a source interface, enter **no ip tacacs source-interface**.

**Version 7.6.1.0** Introduced for S-Series

**Version 7.5.1.0** Introduced for C-Series

**pre-Version 6.2.1.1** Introduced on E-Series
Parameters

- **interface** Enter the following keywords and slot/port or number information:
  - For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16838.
  - For the Null interface, enter the keywords **null 0**.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - **C-Series** and **S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - For a SONET interface, enter the keyword **sonet** followed by the slot/port 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.
  - For VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults

- Not configured.

Command Mode

- Configuration

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for the keyword <strong>fortyGigE</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**tacacs-server host**

Specify a TACACS+ host.

Syntax

```
tacacs-server host {hostname | ipv4-address | ipv6-address} [port number] [timeout seconds] [key key]
```

Parameters

- **hostname** Enter the name of the TACACS+ server host.
- **ipv4-address | ipv6-address** Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X), of the TACACS+ server host.
- **port number** (OPTIONAL) Enter the keyword **port** followed by a number as the port to be used by the TACACS+ server.
  - Range: zero (0) to 65535
  - Default: 49
timeout seconds  (OPTIONAL) Enter the keyword timeout followed by the number of seconds
the switch waits for a reply from the TACACS+ server.
Range: 0 to 1000
Default: 10 seconds

key key  (OPTIONAL) Enter the keyword key followed by a string up to 42 characters
long as the authentication key. This authentication key must match the key
specified in the tacacs-server key command.
Configure this parameter last because leading spaces are ignored.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added or Changed Feature(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv6</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Authentication key length increased to 42 characters</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</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>Specify the login authentication method.</td>
</tr>
<tr>
<td>tacacs-server key</td>
<td>Configure 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

Parameters

<table>
<thead>
<tr>
<th>encryption-type</th>
<th>(OPTIONAL) Enter either either zero (0) or 7 as the encryption type for the key entered. The options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 0 is the default and means the key is not encrypted and stored as clear text.</td>
</tr>
<tr>
<td></td>
<td>• 7 means that the key is encrypted and hidden.</td>
</tr>
</tbody>
</table>

| 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
Port Authentication (802.1X) Commands

The 802.1X Port Authentication commands are:

- `dot1x authentication (Configuration)`
- `dot1x authentication (Interface)`
- `dot1x auth-fail-vlan`
- `dot1x auth-server`
- `dot1x guest-vlan`
- `dot1x max-eap-req`
- `dot1x port-control`
- `dot1x quiet-period`
- `dot1x reauthentication`
- `dot1x reauth-max`
- `dot1x server-timeout`
- `dot1x supplicant-timeout`
- `dot1x tx-period`
- `show dot1x interface`

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

Dell Networking OS supports RADIUS and Active Directory environments using 802.1X Port Authentication.

**Important Points to Remember**

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

- 802.1X is supported on C-Series, E-Series, and S-Series.
- 802.1X is not supported on the LAG or the channel members of a LAG.
- If no VLAN is supplied by the RADIUS server or if 802.1X authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1X authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
If 802.1X authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.

If port security is enabled on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.

If 802.1X is disabled on the port, it is returned to the configured access VLAN.

When the port is in the force authorized, force unauthorized, or shutdown state, it is placed in the configured access VLAN.

If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration will not take effect.

The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

dot1x authentication (Configuration)

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

Syntax

```
dot1x authentication
```

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

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

```
Version 7.6.1.0 Introduced on C-Series and S-Series
Version 7.4.1.0 Introduced on E-Series
```

Related Commands

```
dot1x authentication (Interface) Enable dot1x on an interface
```

dot1x authentication (Interface)

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

Syntax

```
dot1x authentication
```

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

Defaults

Disabled

Command Modes

INTERFACE

Command History

```
Version 7.6.1.0 Introduced on C-Series and S-Series
Version 7.4.1.0 Introduced on E-Series
```

Related Commands

```
dot1x authentication (Configuration) Enable dot1x globally
```

**dot1x auth-fail-vlan**

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

**Syntax**

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

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

**Parameters**

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

- **max-attempts number**
  - (OPTIONAL) Enter the keyword **max-attempts** followed number of attempts desired before authentication fails.
  - Range: 1 to 5
  - Default: 3

**Defaults**

3 attempts

**Command Modes**

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

**Command History**

Version 7.6.1.0 Introduced on C-Series, E-Series and S-Series

**Usage Information**

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

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

**Related Commands**

- **dot1x port-control** Enable port-control on an interface
- **dot1x guest-vlan** Configure a guest VLAN for non-dot1x devices
- **show dot1x interface** Display the 802.1X information on an interface

**dot1x auth-server**

Configure the authentication server to RADIUS.

**Syntax**

```
dot1x auth-server radius
```

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

Version 7.6.1.0 Introduced on C-Series and S-Series

Version 7.4.1.0 Introduced on E-Series
**dot1x guest-vlan**

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

**Syntax**

`dot1x guest-vlan vlan-id`

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

**Parameters**

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

**Defaults**

Not configured

**Command Modes**

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

**Command History**

Version 7.6.1.0 Introduced on C-Series, E-Series, and S-Series

**Usage Information**

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

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

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

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

**Related Commands**

- `dot1x auth-fail-vlan`  
  - Configure a VLAN for authentication failures
- `dot1x reauthentication`  
  - Enable periodic re-authentication
- `show dot1x interface`  
  - Display the 802.1X information on an interface

**dot1x max-eap-req**

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

**Syntax**

`dot1x max-eap-req number`

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

**Parameters**

- `number`  
  - Enter the number of times an EAP request is transmitted before a session time-out.  
  - Range: 1 to 10  
  - Default: 2

**Defaults**

2
dot1x port-control

Enable port control on an interface.

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

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

Defaults: No default behavior or values

Command Modes: INTERFACE

Command History:
- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

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

dot1x quiet-period

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

Syntax: `dot1x quiet-period seconds`

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

Parameters:
- `seconds`: Enter the number of seconds.
  - Range: 1 to 65535
  - Default: 30

Defaults: 30 seconds

Command Modes: INTERFACE

Command History:
- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series
**dot1x reauthentication**

Enable periodic re-authentication of the client.

**Syntax**

```
dot1x reauthentication [interval seconds]
```

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

**Parameters**

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

**Defaults**

3600 seconds (1 hour)

**Command Modes**

INTERFACE

**Command History**

- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

**Related Commands**

- `interface range` Configure a range of interfaces

**dot1x reauth-max**

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

**Syntax**

```
dot1x reauth-max number
```

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

**Parameters**

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

**Defaults**

2

**Command Modes**

INTERFACE

**Command History**

- Version 7.6.1.0 Introduced on C-Series and S-Series
- Version 7.4.1.0 Introduced on E-Series

**dot1x server-timeout**

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

**Syntax**

```
dot1x server-timeout seconds
```

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

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

Defaults
30 seconds

Command Modes
INTERFACE

Command History

<table>
<thead>
<tr>
<th>Command</th>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td></td>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**dot1x supplicant-timeout**

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

Syntax

`dot1x supplicant-timeout seconds`

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

Parameters

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

Defaults
30 seconds

Command Modes
INTERFACE

Command History

<table>
<thead>
<tr>
<th>Command</th>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td></td>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**dot1x tx-period**

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

Syntax

`dot1x tx-period seconds`

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

Parameters

seconds Enter the interval time, in seconds, that EAPOL PDUs are transmitted.
Range: 1 to 31536000 (1 year)
Default: 30

Defaults
30 seconds

Command Modes
INTERFACE

Command History

<table>
<thead>
<tr>
<th>Command</th>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.6.1.0</td>
<td>Introduced on C-Series and S-Series</td>
</tr>
<tr>
<td></td>
<td>7.4.1.0</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>
show dot1x interface

Display the 802.1X information on an interface.

**Syntax**

```plaintext
show dot1x interface interface
```

**Parameters**

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

**Defaults**

No default values or behavior

**Command Modes**

- EXEC
- EXEC privilege

**Command History**

Version 7.6.1.0 Introduced on C-Series, E-Series, and S-Series

**Example**

Figure 51-5. show dot1x interface command Example

```
FTOS#show dot1x int Gi 2/32
802.1x information on Gi 2/32:
-----------------------------
Dot1x Status:   Enable
Port Control:   AUTO
Port Auth Status:  UNAUTHORIZED
Re-Authentication: Disable
Untagged VLAN id: None
Guest VLAN:     Enable
Guest VLAN id:  10
Auth-Fail VLAN: Enable
Auth-Fail VLAN id: 11
Auth-Fail Max-Attempts: 3
Tx Period:     30 seconds
Quiet Period:  60 seconds
ReAuth Max:    2
Supplicant Timeout: 30 seconds
Server Timeout: 30 seconds
Re-Auth Interval: 3600 seconds
Max-EAP-Req:   2
Auth Type:     SINGLE_HOST
Auth PAE State: Initialize
Backend State: Initialize

FTOS#
```
SSH Server and SCP Commands

FTOS supports SSH Protocol versions 1.5 and 2.0. Secure Shell (SSH) is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.

- 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
Figure 51-6. crypto key generate rsa1 command example

FTOS#conf
FTOS(conf)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024>: 1024
Host key already exists. Do you want to replace. [y/n] :y
FTOS(conf)#

Usage Information
The host keys are required for key-exchange by the SSH server. If the keys are not found when the server is enabled (ip ssh server enable), the keys are automatically generated.

This command requires user interaction and will generate 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>Enable the SSH server.</td>
</tr>
<tr>
<td>show crypto</td>
<td>Display SSH host public keys</td>
</tr>
</tbody>
</table>

debug ip ssh

Enables collecting SSH debug information.

Syntax
debug ip ssh {client | server}

To disable debugging, use the no debug ip ssh {client | server} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Enter the keyword client to enable collecting debug information on the client.</td>
</tr>
<tr>
<td>server</td>
<td>Enter the keyword server to enable collecting debug information on the server.</td>
</tr>
</tbody>
</table>

Defaults

Disabled on both client and server

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

Debug information includes details for key-exchange, authentication, and established session for each connection.
**ip scp topdir**

Identify a location for files used in secure copy transfer.

**Syntax**

```
ip scp topdir directory
```

To return to the default setting, enter `no ip scp topdir` command.

**Parameters**

- **directory**
  
Enter a directory name.

**Defaults**

The internal flash (flash:) is the default directory.

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

**Usage Information**

To configure the switch as a SCP server, use the `ip ssh server` command.

**Related Commands**

- `ip ssh server` — Enable 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**

```
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 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

**Usage Information**

This command specifies the maximum number of attempts to authenticate a user on an SSH connection with the remote host for password authentication. SSH will disconnect when the number of password failures exceeds authentication-retries.
ip ssh connection-rate-limit

Syntax: ip ssh connection-rate-limit 1-10

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-10</td>
<td>Enter the number of maximum number of incoming SSH connections allowed per minute. Range: 1 to 10 per minute Default: 10 per minute</td>
</tr>
</tbody>
</table>

Defaults: 10 per minute

Command Modes: CONFIGURATION

Command History:

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced for</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>pre-6.1.1</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

ip ssh hostbased-authentication

Syntax: ip ssh hostbased-authentication enable

To disable hostbased-authentication for SSHv2 server, use the no ip ssh hostbased-authentication enable command.

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enter the keyword enable to enable hostbased-authentication for SSHv2 server.</td>
</tr>
</tbody>
</table>

Defaults: Disable by default

Command Modes: CONFIGURATION

Command History:

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced for</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>pre-6.1.1</td>
<td>E-Series</td>
</tr>
</tbody>
</table>

Usage Information:

If this command is enabled, 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 no ip ssh rsa-authentication enable is executed, host-based authentication is disabled.

Note: Administrators must specify the two files (rhosts and pub-key-file) to configure host-based authentication.
Related
Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh pub-key-file</td>
<td>Public keys of trusted hosts from a file.</td>
</tr>
<tr>
<td>ip ssh rhostsfile</td>
<td>Trusted hosts and users for rhost authentication.</td>
</tr>
</tbody>
</table>

**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

**Command History**

- Version 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

**Usage Information**

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`.

**Parameters**

```
enable
```

Enter the keyword `enable` to enable password-authentication for the SSH server.

**Defaults**

enabled

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

**Usage Information**

With password authentication enabled, users 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**

<table>
<thead>
<tr>
<th>WORD</th>
<th>Enter the file name for the host-based authentication.</th>
</tr>
</thead>
</table>

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced for</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

Figure 51-7. ip ssh pub-key-file Command Example

```
FTOS(conf)# ip ssh pub-key-file flash://knownhosts
```

**Usage Information**

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 will not appear in the running configuration since this command needs to be run just once.

The file contains the OpenSSH compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/QQP8xYhzOxn07yh4VGP4oULgkoiE7HO9G4sNV+ui+DWEc3cgYAcu5Lai1MU2ODrzhCwyDNp05tKBU3tReG1o8AO6i+S4hyEMqHzkBFNVqHzpQc+R54p2urzV0F4pRKnaXhF3Lk4D460HZRhhVrxqenPDe4nWIMPJ0ds= ashwani@poclab4
```

**Note:** For **rhostsfile** and **pub-key-file**, the administrator must FTP the file to the chassis.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh client-pub-keys</td>
<td>Display 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**

<table>
<thead>
<tr>
<th>WORD</th>
<th>Enter the file name for the host-based authentication.</th>
</tr>
</thead>
</table>

**Defaults**

No default behavior or values

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced for</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

This command specifies the file to be used for the host-based authentication. The file creates/overwrites the file flash://ADMIN_DIR/ssh/rhosts and deletes the user specified file. Even though this is a global configuration command, it will not appear in the running configuration since this command needs to be run just once.

The file contains the OpenSSH compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/QQP8xYhzOxn07yh4VGP4oULgkoiE7HO9G4sNV+ui+DWEc3cgYAcu5Lai1MU2ODrzhCwyDNp05tKBU3tReG1o8AO6i+S4hyEMqHzkBFNVqHzpQc+R54p2urzV0F4pRKnaXhF3Lk4D460HZRhhVrxqenPDe4nWIMPJ0ds= ashwani@poclab4
```

**Note:** For **rhostsfile** and **pub-key-file**, the administrator must FTP the file to the chassis.
Example Figure 51-8. 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 will not appear in the running configuration since 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
```

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Enabling RSA authentication allows the user 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)**
  
  Add 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**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If you want to log in without being prompted for a password, log in through RSA authentication. To do that, you must first add the SSHv2 RSA public keys to the list of authorized keys. This command adds the specified RSA keys to the following file:

`flash://ADMIN_DIR/ssh/authorized-keys-username` (where `username` is the user associated with this terminal).

**Note:** The `no` form of this command deletes the file `flash://ADMIN_DIR/ssh/authorized-keys-username`

**Related Commands**

- `show ip ssh rsa-authentication` Display RSA authorized keys.
- `ip ssh rsa-authentication (Config)` Enable RSA authentication.

---

ip ssh server

Configure an SSH server.

**Syntax**

`ip ssh server {enable [port port-number] [version {1 | 2}]]`

To disable SSH server functions, enter `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 of 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
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 51-9. ip ssh server port Command Example**

```
FTOS# conf
FTOS(conf)# ip ssh server port 45
FTOS(conf)# ip ssh server enable
FTOS#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ssh</code></td>
<td>Display the ssh information</td>
</tr>
</tbody>
</table>

**show crypto**

Display the public part of the SSH host-keys.

**Syntax**

```
show crypto key mypubkey {rsa | rsa1}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
<td>Enter the keyword <code>key</code> to display the host public key.</td>
</tr>
<tr>
<td><strong>mypubkey</strong></td>
<td>Enter the keyword <code>mypubkey</code> to display the host public key.</td>
</tr>
<tr>
<td><strong>rsa</strong></td>
<td>Enter the keyword <code>rsa</code> to display the host SSHv2 RSA public key.</td>
</tr>
<tr>
<td><strong>rsa1</strong></td>
<td>Enter the keyword <code>rsa1</code> to display the host SSHv1 RSA public key.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 51-10. show crypto Command Examples**

```
FTOS#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAABIAhIAEAtzKZME/e8V8smXR22EJQhCMkEOkuia=0ILVoMYU12KGFj0W5BPCsVf/
x51fYFFWu2JN0csJK7vSannMhChFZYsVx1vT36h971FJAOQloegd0ycpocFe+DNLKfJnx7SAj1akFQMWG
/g/g78ZkDT3Ydr8KkIfS14Bg/WS88740=
```

```
FTOS#show crypto key mypubkey rsa1
1024 35
13106001514808733985595325751539724965785007722064429496374808935683089610203172266
7988956754966752650063796218977992760927852236328892323055081819166009928132616408
66434577460221922951890399296634579117374224743155375050167679660273790601494434
05000001517986442569613385774919236081771341059533760063913083
```

FTOS#
show ip ssh

Display information about established SSH sessions.

Syntax

show ip ssh

Command Modes

EXEC
EXEC Privilege

Example

Figure 51-11. show ip ssh Command Example

FTOS#show ip ssh
SSH server                : enabled.
SSH server version        : v1 and v2.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA          Authentication  : disabled.
Vty Encryption Remote IP
  0 3DES  172.16.1.162
  1 3DES  172.16.1.162
  2 3DES  172.16.1.162

Related
Commands

ip ssh server Configure an SSH server.
show ip ssh client-pub-keys Display 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

No default behavior or values

Command Modes

EXEC

Command History

Version 7.6.1.0 Introduced for S-Series
Version 7.5.1.0 Introduced for C-Series
pre-Version 6.1.1.0 Introduced for E-Series
Example

Figure 51-12. show ip ssh client-pub-keys Command Example

FTOS#show ip ssh client-pub-keys
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/QQp8xYhz0Xko07yh4VGPKoUfgKoieTHO9G4aNV+ui+DW0R3c3cyAcULa11MI20DrzhCwyDNp05tKBU3tReG
08Axli6+54hyEMqHzkzBFNVqHzpQC+Rs4p2urrV0F4pRKnaXdhF3Lk4D460HZRRhVrxqeNxPdpEnWIMPJ10
ds= ashwani@poclab4
FTOS#

Usage

This command displays the contents of the file flash://ADMIN_DIR/ssh/knownhosts

Information

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh rsa-authentication</td>
<td>Display the authorized-keys for the RSA authentication.</td>
</tr>
</tbody>
</table>

Syntax

show ip ssh rsa-authentication [my-authorized-keys]

Parameters

- **my-authorized-keys**
  - Display the RSA authorized keys.

Defaults

No default behavior or values

Command Modes

- EXEC

Command History

- Version 7.6.1.0 Introduced for S-Series
- Version 7.5.1.0 Introduced for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

Example

Figure 51-13. show ip ssh rsa-authentication Command Example

FTOS#show ip ssh rsa-authentication my-authorized-keys
ssh-rsa
AAAAAB3NzaC1yc2EAAAABIwAAAIEAox/QQp8xYhz0Xko07yh4VGPKoUfgKoieTHO9G4aNV+ui+DW0R3c3cyAcULa11MI20DrzhCwyDNp05tKBU3tReG
08Axli6+54hyEMqHzkzBFNVqHzpQC+Rs4p2urrV0F4pRKnaXdhF3Lk4D460HZRRhVrxqeNxPdpEnWIMPJ10
ds= ashwani@poclab4
FTOS#

Usage

This command displays the contents of the file flash://ADMIN_DIR/ssh/authorized-keys.username.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh rsa-authentication (Config)</td>
<td>Configure the RSA authorized keys.</td>
</tr>
</tbody>
</table>
ssh

Open an SSH connection specifying the hostname, username, port number and version of the SSH client.

Dell Networking OS supports both inbound and outbound SSH sessions using IPv4 or IPv6 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

**Syntax**

```
ssh [vrf vrf-id] {hostname | ipv4 address | ipv6 address} [-l username | -p port-number | -v {1 | 2}]
```

**Parameters**

- **vrf vrf-id**
  - (OPTIONAL) Enter the keyword vrf followed by the ID number of the VRF.
  - Range: 1 to 63.

- **hostname**
  - (OPTIONAL) Enter the IP address or the hostname of the remote device.

- **vrf instance**
  - (OPTIONAL) E-Series Only: Enter the keyword vrf following by the VRF Instance name to open a SSH connection to that instance.

- **ipv4 address**
  - (OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.

- **ipv6-address prefix-length**
  - (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format.
  - Range: /0 to /128
  - **Note:** The :: notation specifies successive hexadecimal fields of zeros

- **-l username**
  - (OPTIONAL) Enter the keyword -l followed by the user name used in this SSH session.
  - Default: The user name of the user associated with the terminal.

- **-p port-number**
  - (OPTIONAL) Enter the keyword -p followed by the port number.
  - Range: 1 to 65536
  - Default: 22

- **-v {1 | 2}**
  - (OPTIONAL) Enter the keyword -v followed by the SSH version 1 or 2.
  - Default: The version from the protocol negotiation

**Defaults**

As above.

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for VRF.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.9.1.0</td>
<td>Introduced VRF</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>Version 7.5.1.0</td>
<td>Added IPv6 support; Introduced for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
Figure 51-14. ssh Command Example

FTOS#ssh 123.12.1.123 -l ashwani -p 5005 -v 2
```
# Trace List Commands

IP trace lists create an Access Control List (ACLs) to trace all traffic into the E-Series switch. This feature is useful for tracing Denial of Service (DOS) attacks.

**Note:** For other Access Control List commands, see the chapters Chapter 10, ACL VLAN Group and Chapter 9, Access Control Lists (ACL).

- clear counters ip trace-group
- deny
- deny tcp
- deny udp
- ip trace-group
- ip trace-list
- permit
- permit tcp
- permit udp
- seq
- show config
- show ip accounting trace-lists

## clear counters ip trace-group

Erase all counters maintained for trace lists.

**Syntax**

```
clear counters ip trace-group [trace-list-name]
```

**Parameters**

- `trace-list-name` *(OPTIONAL)* Enter the name of a configured trace list.

**Command Modes**

EXEC Privilege

## 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]] | log [order number]
```

To remove this filter, you have two choices:

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

**Parameters**

- `ip` Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list will deny all IP protocols.
- `ip-protocol-number` Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
deny tcp

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

Syntax

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

To remove this filter, you have two choices:

- Use the no seq sequence-number command syntax if you know the filter’s sequence number or
- Use the no deny tcp {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
(Optional) Enter a network mask in /prefix format (/x).

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.

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

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

log
(Optional) Enter the keyword log to have the information kept in a Trace-list log file.

order number
(Optional) Enter the keyword order followed by a number from 0 to 7 as the order number.
### 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` command parameter)

### port

Enter the application layer port number. Enter two port numbers if using the range logical operand.

Range: 0 to 65535.

The following list includes some common TCP port numbers:

- 23 = Telnet
- 20 and 21 = FTP
- 25 = SMTP
- 169 = SNMP

### destination

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

### count

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

### byte

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

### log

(Optional) Enter the keyword **log** to have the information kept in a Trace-list log file.

### order number

(Optional) Enter the keyword **order** followed by a number from 0 to 7 as the order number.

---

### deny udp

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

**Syntax**

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

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number or
- Use the `no deny 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**
  
(Optional) Enter a network mask in /prefix format (/x).

- **any**
  
Enter the keyword **any** to specify that all routes are subject to the filter.

- **host ip-address**
  
Enter the keyword **host** followed by the IP address to specify a host IP address.
 operator  (OPTIONAL) Enter one of the following logical 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  (OPTIONAL) Enter a network mask in /prefix format (/x).

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

 byte  (OPTIONAL) Enter the keyword byte to count only bytes

 log  (OPTIONAL) Enter the keyword log to have the information kept in a Trace-list log file.

 order  number  (OPTIONAL) Enter the keyword order followed by a number from 0 to 7 as the order number.

 Defaults  Not configured.

 Command Modes  TRACE LIST

 Related Commands  deny  Assign a trace list filter to deny IP traffic.

 deny tcp  Assign a trace list filter to deny TCP traffic.

 ip trace-group

 Assign a trace list globally to process all incoming packets to the switch.

 Syntax  

 ip trace-group  trace-list-name

 To delete an trace list configuration, use the no ip trace-group  trace-list-name command.

 Parameters  

 trace-list-name  Enter the name of a configured trace list.

 Defaults  Not enabled.

 Command Modes  CONFIGURATION

 Usage Information  You can assign one Trace list to the chassis.

 If there are unresolved next-hops and a Trace-list is enabled, there is a possibility that the traffic hitting the CPU will not be rate-limited.

 Related Commands  ip trace-list  Configure a trace list ACL.
ip trace-list

Configure a trace list, based on IP addresses or protocols, to filter all traffic on the E-Series.

**Syntax**

```
ip trace-list trace-list-name
```

To delete a trace list, use the `no ip trace-list trace-list-name` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>trace-list-name</code></td>
<td>Enter a string up to 16 characters long as the access list name.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured

**Example**

**Figure 51-15. ip trace-list Command Example**

```
FTOS(conf)#ip trace-list suzanne
FTOS(config-trace-acl)#
```

**Command Modes**

CONFIGURATION

**Usage Information**

After you create a trace list, you must apply it to the E-Series using the `ip trace-group` command in the CONFIGURATION mode.

**Related Commands**

- `ip trace-group` View the current configuration.

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]] [log]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- 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><code>ip</code></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><code>ip-protocol-number</code></td>
<td>Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header.</td>
</tr>
<tr>
<td><code>source</code></td>
<td>Enter the IP address of the network or host from which the packets were sent.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>(OPTIONAL) Enter a network mask in /prefix format (/x).</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Enter the keyword <code>any</code> to specify that all routes are subject to the filter.</td>
</tr>
<tr>
<td><code>host ip-address</code></td>
<td>Enter the keyword <code>host</code> followed by the IP address to specify a host IP address.</td>
</tr>
<tr>
<td><code>destination</code></td>
<td>Enter the IP address of the network or host to which the packets are sent.</td>
</tr>
<tr>
<td><code>count</code></td>
<td>(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.</td>
</tr>
</tbody>
</table>
## permit tcp

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

### Syntax

```
permit tcp {source mask | any | host ip-address} [operator port [port]] {destination mask | any | host ip-address} [operator port [port]] [count [byte]] | log [order number]
```

### To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- Use the `no permit tcp {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**: (OPTIONAL) Enter a network mask in /prefix format (/x).
- **any**: Enter the keyword `any` to specify that all routes are subject to the filter.
- **host ip-address**: Enter the keyword `host` followed by the IP address to specify a host IP address.
- **operator**: (OPTIONAL) Enter one of the following logical operand:
  - `eq` = equal to
  - `neq` = not equal to
  - `gt` = greater than
  - `lt` = less than
  - `range` = inclusive range of ports (you must specify two port for the `port` parameter.)
- **port port**: Enter the application layer port number. Enter two port numbers if using the range logical operand.
  - Range: 0 to 65535.
  - The following list includes some common TCP port numbers:
    - 23 = Telnet
    - 20 and 21 = FTP
    - 25 = SMTP
    - 169 = SNMP
- **destination**: Enter the IP address of the network or host to which the packets are sent.
### Defaults
Not configured.

### Command Modes
TRACE LIST

### Related Commands
- `ip trace-list` Create a trace list.
- `permit` Assign a trace list filter to forward IP packets.
- `permit udp` Assign a trace list filter to forward UDP packets.

### permit udp
Configure a filter to pass UDP packets meeting the filter criteria.

#### Syntax
```
permit udp {source mask | any | host ip-address} {operator port [port]} {destination mask | any | host ip-address} {operator port [port]} [count | byte] | log [order number]
```

To remove this filter, you have two choices:
- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number or
- 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** (OPTIONAL) Enter a network mask in /prefix format (/x).
- **any** Enter the keyword any to specify that all routes are subject to the filter.
- **host ip-address** Enter the keyword host followed by the IP address to specify a host IP address.
- **operator** (OPTIONAL) Enter one of the following logical 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.
Assign a sequence number to a deny or permit filter in a trace list while creating the filter.

**Syntax**

```
seq sequence-number [deny | permit] {ip-protocol-number | ip | tcp | udp} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator port [port]] [precedence precedence] [tos tos-value] [count [byte] | log]
```

To delete a filter, use the `no seq sequence-number` command.

**Parameters**

- **sequence-number**
  - Enter a number from 0 to 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.
- **ip-protocol-number**
  - Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
- **ip**
  - Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list will permit all IP protocols.
- **tcp**
  - Enter the keyword `tcp` to configure a TCP access list filter.
- **udp**
  - Enter the keyword `udp` to configure a UDP access list filter.
- **source**
  - Enter the IP address of the network or host from which the packets were sent.
- **mask**
  - Enter a network mask in /prefix format (/x).
- **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.
**Syntax**

```
show config
```

**Command Modes**

TRACE LIST

**Command History**

Version 7.4.1.0  Deprecated established keyword—not supported on TeraScale line cards.

**Related Commands**

- **deny**  Configure a filter to drop packets.
- **permit**  Configure a filter to forward packets.

---

**operator**

(Optional) Enter one of the following logical operands:

- `eq` = equal to
- `neq` = not equal to
- `gt` = greater than
- `lt` = less than
- `range` = inclusive range of ports (you must specify two ports for the `port` parameter.)

**port port**

(Optional) Enter the application layer port number. Enter two port numbers if using the `range` logical operand.

Range: 0 to 65535

The following list includes some common TCP port numbers:

- 23 = Telnet
- 20 and 21 = FTP
- 25 = SMTP
- 169 = SNMP

**destination**

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

**precedence precedence**

Enter the keyword `precedence` followed by a number from 0 to 7 as the precedence value.

**tos tos-value**

Enter the keyword `tos` followed by a number from 0 to 15 as the TOS value.

**count**

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

**byte**

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

**log**

(Optional) Enter the keyword `log` to have the information kept in a Trace-list log file.

**Defaults**

Not configured.

**Command Modes**

TRACE LIST

---

**show config**

View the current IP trace list configuration.
show ip accounting trace-lists

View the trace lists created on the switch and the sequence of filters.

Syntax

```
show ip accounting trace-lists [trace-list-name [linecard number]]
```

Parameters

- `trace-list-name` (OPTIONAL) Enter the name of the trace list to be displayed.
- `linecard number` (OPTIONAL) Enter the keyword `linecard` followed by the line card number to view the Trace list information on that line card. C-Series and S-Series Range: 0-7 on the C7008. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series

Example

```
Example Figure 51-17. show ip accounting trace-lists Command Example

FTOS#show ip accounting trace-list suzanne
Trace List suzanne
  seq 5 deny ip any any count (0x00 packets)
  seq 10 permit tcp 10.1.1.0 /24 any count bytes (0x00 bytes)
FTOS#
```

Secure DHCP Commands

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.

- `clear ip dhcp snooping`
- `ip dhcp relay`
- `ip dhcp snooping`
- `ip dhcp snooping database`
- `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

Syntax: clear ip dhcp snooping binding

Command Modes: EXEC Privilege

Default: None

Command History:
- Version 7.8.1.0 Introduced on C-Series and S-Series

Related Commands:
- show ip dhcp snooping Display the contents of the DHCP binding table.

ip dhcp relay

Syntax: ip dhcp relay information-option [trust-downstream]

Parameters:
- trust-downstream: Configure the system to trust Option 82 when it is received from the previous-hop router.

Command Modes: CONFIGURATION

Default: Disabled

Command History:
- Version 7.8.1.0 Introduced on C-Series and S-Series

ip dhcp snooping

Syntax: [no] ip dhcp snooping

Command Modes: CONFIGURATION

Default: Disabled

Command History:
- Version 7.8.1.0 Introduced on C-Series and S-Series

Usage Information: When enabled, no learning takes place until snooping is enabled on a VLAN. Upon 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 Enable 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**

<table>
<thead>
<tr>
<th><code>minutes</code></th>
<th>Range: 5-21600</th>
</tr>
</thead>
</table>

**Command Modes**

CONFIGURATION

**Default**

None

**Command History**

Version 7.8.1.0 Introduced on C-Series and S-Series

---

**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 7.8.1.0 Introduced on C-Series and S-Series

---

**ip dhcp snooping trust**

Configure an interface as trusted.

**Syntax**

`[no] ip dhcp snooping trust`

**Command Modes**

INTERFACE

**Default**

Untrusted

**Command History**

Version 7.8.1.0 Introduced on C-Series and S-Series

---

**ip dhcp source-address-validation**

Enable IP Source Guard.

**Syntax**

`[no] ip dhcp source-address-validation`

**Command Modes**

INTERFACE
**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 7.8.1.0 Introduced on C-Series and S-Series

**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` - Configure an interface as trusted.

---

**show ip dhcp snooping**

Display the contents of the DHCP binding table.

**Syntax**

```
show ip dhcp snooping binding
```

**Command Modes**

EXEC

EXEC Privilege

**Default**

None

**Command History**

Version 7.8.1.0 Introduced on C-Series and S-Series

**Related Commands**

- `clear ip dhcp snooping` - Clear the contents of the DHCP binding table.
Service Provider Bridging

Overview

Service Provider Bridging is composed of VLAN Stacking, Layer 2 Protocol Tunneling, and Provider Backbone Bridging as described in the Dell Networking OS Configuration Guide Service Provider Bridging chapter.

This chapter includes CLI information for Dell Networking OS Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel. L2PT is available in Dell Networking OS for the C-Series, E-Series, and S-Series.

L2PT is supported on E-Series ExaScale with Dell Networking OS 8.2.1.0 and later.

Refer to Chapter 61, VLAN Stacking or Chapter 58, Spanning Tree Protocol (STP) and Chapter 20, GARP VLAN Registration (GVRP) for further information related to those features.

Commands

The L2PT commands are:

- `debug protocol-tunnel`
- `protocol-tunnel`
- `protocol-tunnel destination-mac`
- `protocol-tunnel enable`
- `protocol-tunnel rate-limit`
- `show protocol-tunnel`

Important Points to Remember

- L2PT is enabled at the interface VLAN-Stack VLAN level. For details on Stackable VLAN (VLAN-Stacking) commands, see Chapter 61, VLAN Stacking.
- The default behavior is to disable protocol packet tunneling through the 802.1q tunnel.
- Rate-limiting is required to protect against BPDU attacks.
- A port channel (including through LACP) can be configured as a VLAN-Stack access or trunk port.
- ARP packets work as expected across the tunnel.
- FEFD works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (OSPF for example) work as expected and carry over to the other end of the VLAN-Stack VLAN.
**debug protocol-tunnel**

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

**Syntax**

```
debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]
```

To disable debugging, use the `no debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]` command.

**Parameters**

- **interface**
  - Enter one of the following interfaces and slot/port information:
    - For a Fast Ethernet interface, enter the keyword `FastEthernet` followed by the slot/port information.
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
      - **C-Series and S-Series** Range: 1-128
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword `sonet` followed by the 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.
- **in | out | both**
  - Enter the keyword `in`, `out`, or `both` to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.
- **vlan vlan-id**
  - Enter the keyword `vlan` followed by the VLAN ID.
    - Range: 1 to 4094
- **count value**
  - Enter the keyword `count` followed by the number of debug outputs.
    - Range: 1 to 100

**Defaults**

Debug Disabled

**Command Modes**

EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 8.2.1.0** Introduced on the C-Series, E-Series and E-Series ExaScale.
- **Version 7.4.1.0** Introduced

---

**protocol-tunnel**

Enable protocol tunneling per VLAN-Stack VLAN.

**Syntax**

```
protocol-tunnel stp
```

To disable protocol tunneling, use the `no protocol-tunnel stp` command.

**Parameters**

- **stp**
  - Enter the keyword `stp` to enable protocol tunneling on a spanning tree, including STP, MSTP, RSTP, and PVST.
Defaults
No default values or behavior

Command Modes
CONF-IF-VLAN

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on the C-Series, E-Series and E-Series ExaScale.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example

Figure 52-1. Protocol-tunneling Command Example

FTOS#conf
FTOS(conf)#interface vlan 2
FTOS(conf-if-vl-2)#vlan-stack compatible
FTOS(conf-if-vl-2)#member Gi1/2-3
FTOS(conf-if-vl-2)#protocol-tunnel stp
FTOS(conf-if-vl-2)#

Note: When VLAN-Stacking is enabled, no protocol packets are tunneled.

Related Commands

show protocol-tunnel Display tunneling information for all VLANs

protocol-tunnel destination-mac

Syntax
protocol-tunnel destination-mac stp address

Parameters
stp Change the default destination MAC address used for L2PT to another value.

Defaults
The default destination MAC is 01:01:e8:00:00:00.

Command Modes
CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on the C-Series and S-Series.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

When VLAN-Stacking is enabled, no protocol packets are tunneled.

Related Commands

show protocol-tunnel Display tunneling information for all VLANs

protocol-tunnel enable

Syntax
protocol-tunnel enable

To disable protocol tunneling, use the no protocol-tunnel enable command.

Defaults
Disabled
**Command Modes**

CONFIGURATION

**Command History**

- **Version 7.4.1.0** Introduced

**Usage Information**

Dell Networking OS must have the default CAM profile with the default microcode before you enable L2PT.

---

**protocol-tunnel rate-limit**

`C E S`

Enable traffic rate limiting per box.

**Syntax**

```
protocol-tunnel rate-limit rate
```

To reset the rate limit to the default, use the `no protocol-tunnel rate-limit rate` command.

**Parameters**

- `rate` Enter the rate in frames per second.
  
  - **Range:** 75 to 3000
  
  - **Default:** 75

**Defaults**

75 Frames per second

**Command Modes**

CONFIGURATION

**Command History**

- **Version 8.2.1.0** Introduced on the C-Series, E-Series Terascale, and E-Series ExaScale. Maximum rate limit on E-Series reduced from 4000 to 3000.
- **Version 7.4.1.0** Introduced

**Example**

**Figure 52-2. protocol-tunnel rate-limit Command Example**

```
FTOS#
FTOS#conf
FTOS(conf)#protocol-tunnel rate-limit 1000
FTOS(conf)#
```

**Related Commands**

- `show protocol-tunnel` Display tunneling information for all VLANs
- `show running-config` Display the current configuration.

---

**show protocol-tunnel**

`C E S`

Display protocol tunnel information for all or a specified VLAN-Stack VLAN.

**Syntax**

```
show protocol-tunnel [vlan vlan-id]
```

**Parameters**

- `vlan vlan-id` (OPTIONAL) Enter the keyword `vlan` followed by the VLAN ID to display information for the one VLAN.
  
  - **Range:** 1 to 4094

**Defaults**

No default values or behavior
**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series, E-Series and E-Series ExaScale.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

**Figure 52-3.  show protocol-tunnel Command Example**

```
FTOS#show protocol-tunnel
System Rate-Limit: 1000 Frames/second
Interface   Vlan    Protocol(s)
Gi1/2        2       STP, PVST
Gi1/3        3       STP, PVST
Po35         4       STP, PVST
FTOS#
```

**Figure 52-4.  show protocol-tunnel command example for a specific VLAN**

```
FTOS#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface   Vlan    Protocol(s)
Gi1/2        2       STP, PVST
FTOS#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Display the current configuration.</td>
</tr>
</tbody>
</table>
sFlow

Overview

sFlow commands are supported on these platforms: C E S.

Dell Networking OS 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

- Dell Networking recommends that the sFlow Collector be connected to the Dell Networking chassis through a line card port rather than the RPM Management Ethernet port.
- Dell Networking OS exports all sFlow packets to the sFlow Collector. A small sampling rate can equate to a large number of exported packets. A backoff mechanism will automatically be 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, will always be 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 PBR (Policy-Based Routing), the sFlow datagram may contain incorrect extended gateway/router information.
- sFlow does not support packing extended information for IPv6 packets. Only the first 128 bytes of the IPv6 packet is shipped in the datagram.
- The source VLAN field in the extended switch element will not be packed in case of a routed packet.
- The destination VLAN field in the extended switch element will not be 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 (see sflow extended-switch enable)
  - 1600 packets when extended-router and/or extended-gateway information packing is enabled (see Figure and sflow extended-gateway enable)
Commands

The sFlow commands are:

- `sflow collector`
- `sflow enable (Global)`
- `sflow enable (Interface)`
- `sflow extended-gateway enable`
- `sflow extended-router enable`
- `sflow extended-switch enable`
- `sflow polling-interval (Global)`
- `sflow polling-interval (Interface)`
- `sflow sample-rate (Global)`
- `sflow sample-rate (Interface)`
- `show sflow`
- `show sflow linecard`
sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

Syntax

```
sflow collector {ipv4-address | ipv6-address} agent-addr {ipv4-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number] [vrf management]
```

Parameters

- `sflow collector ipv4-address | ipv6-address` Enter the IPv4 (A.B.C.D) or IPv6 address (X:X:X::X) of the sFlow collector device.
- `agent-addr ipv4-address | ipv6-address` Enter the IPv4 (A.B.C.D) or IPv6 address (X:X:X::X) of the sFlow agent in the router.
- `number` (OPTIONAL) Enter the UDP port number (User Datagram Protocol).
  Range: 0 to 65535
  Default: 6343
- `max-datagram-size number` (OPTIONAL) Enter the keyword `max-datagram-size` followed by the size number in bytes.
  Range: 400 to 1500
  Default: 1400
- `vrf management` (OPTIONAL) Enter the keyword `vrf` followed by the keyword `management` to configure the collector device corresponding to the default VRF and the management VRF respectively.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.4.2.3</td>
<td>Support for IPv6 sFlow collectors and agents was added on the E-series TeraScale, C-Series, and S-Series.</td>
</tr>
<tr>
<td>8.4.1.1</td>
<td>Support for IPv6 sFlow collectors and agents was added on the E-series ExaScale.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduces on S-Series Stacking</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Expanded the no form of the command to mirror the syntax used to configure</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

You can configure up to two sFlow collectors (IPv4 or IPv6). 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.

IPv6 sFlow collectors and agents are supported on E-Series (ExaScale and TeraScale), C-Series, and S-Series routers.

To delete a configured collector, enter the `no sflow collector {ipv4-address | ipv6-address} agent-addr {ipv4-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number]` command.
As part of the sFlow-MIB, if the SNMP request originates from a configured collector, Dell Networking OS will return the corresponding configured agent IP in MIB requests. Dell Networking OS checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, Dell Networking OS 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

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
</tr>
<tr>
<td>Version 8.1.1.0</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
</tr>
<tr>
<td>Version 6.2.1.1</td>
</tr>
</tbody>
</table>

**Usage Information**

sFlow is disabled by default. In addition to this command, sFlow needs to be enable on individual interfaces where sFlow sampling is desired.

**Related Commands**

- `sflow enable (Interface)` — Enable 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

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.2.1.0</td>
</tr>
<tr>
<td>Version 8.1.1.0</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
</tr>
<tr>
<td>Version 6.2.1.1</td>
</tr>
</tbody>
</table>
When sFlow is enable on an interface, flow sampling is done on any traffic going out of the interface.

**Note:** Once a physical port is a member of a LAG, it will inherit the sFlow configuration from the LAG port.

### sflow extended-gateway enable

Enable packing information on an extended gateway.

**Syntax**

```
sflow extended-gateway [extended-router] [extended-switch] enable
```

To disable packing information, use the `no sflow extended-gateway [extended-router] [extended-switch] enable` command.

**Parameters**

- **extended-router**: Enter the keyword `extended-router` to collect extended router information.
- **extended-switch**: Enter the keyword `extended-switch` to collect extended switch information.
- **enable**: Enter the keyword `enable` to enable global extended information.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series

**Usage Information**

The `show sflow` command displays the configured global extended information.

Dell Networking OS 7.8.1.0 and later enhances the sFlow implementation for real time traffic analysis on the E-Series 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.

**Example**

**Figure 53-1. show sflow Command Output**

```
FTOS#show sflow
sFlow services are enabled
Global default sampling rate: 64
Global default counter polling interval: 1000
Global extended information enabled: gateway, router, switch
1 collectors configured
Collector IP addr: 20.20.20.2, Agent IP addr: 10.11.201.7, UDP port: 6343
1732336 UDP packets exported
0 UDP packets dropped
12510225 sFlow samples collected
0 sFlow samples dropped due to sub-sampling
FTOS#
```

**Related Commands**

- `show sflow` Display the sFlow configuration
sflow extended-router enable

Enable packing information on a router and switch.

Syntax

sflow extended-router [extended-switch] enable

To disable packing information, use the no sflow extended-router [extended-switch] enable command.

Parameters

- extended-switch: Enter the keyword extended-switch to collect extended switch information.
- enable: Enter the keyword enable to enable global extended information.

Defaults
Disabled

Command Modes
CONFIGURATION

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.4.1.0 Introduced on E-Series

Usage Information

Dell Networking OS 7.8.1.0 and later enhances the sFlow implementation for real time traffic analysis on the E-Series 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

- sflow extended-gateway enable: Enable packing information on an extended gateway
- sflow extended-switch enable: Enable packing information on a switch.
- show sflow: Display the sFlow configuration

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 8.2.1.0 Introduced on S-Series Stacking
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- Version 7.4.1.0 Introduced on E-Series
Dell Networking OS 7.8.1.0 and later enhances the sFlow implementation for real time traffic analysis on the E-Series 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow extended-gateway enable</td>
<td>Enable packing information on an extended gateway.</td>
</tr>
<tr>
<td>sflow extended-router enable</td>
<td>Enable packing information on a router.</td>
</tr>
<tr>
<td>show sflow</td>
<td>Display the sFlow configuration</td>
</tr>
</tbody>
</table>

**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>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: 20 seconds</td>
</tr>
</tbody>
</table>

**Defaults**

20 seconds

**Command Modes**

CONFIGURATION

**Command History**

- Version 8.2.1.0  Introduces on S-Series Stacking
- Version 8.1.1.0  Introduced on E-Series ExaScale
- Version 7.7.1.0  Introduced on S-Series
- Version 7.6.1.0  Introduced on C-Series
- Version 6.2.1.1  Introduced on E-Series

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow polling-interval (Interface)</td>
<td>Set the polling interval for an interface</td>
</tr>
</tbody>
</table>

**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.
sflow sample-rate (Global)

Change the global default sampling rate.

Syntax

```
sflow sample-rate value
```

To return to the default sampling rate, enter the `no sflow sample-rate`.

Parameters

```
value
```

Enter the sampling rate value.

- Range: C-Series and S-Series: 256 to 8388608 packets
- E-Series TeraScale and ExaScale: 2 to 8388608

Enter values in powers of 2 only, for example 4096, 8192, 16384 etc.

Default: 32768 packets

Defaults

32768

Command Modes

CONFIGURATION

Command History

- Version 8.2.1.0 Introduces on S-Series Stacking
- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
- Version 6.2.1.1 Introduced on E-Series
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.

Related Commands

sflow sample-rate (Interface) Change the Interface sampling rate.

sflow sample-rate (Interface)

Change the Interface default sampling rate.

Syntax

sflow sample-rate value

To return to the default sampling rate, enter the no sflow sample-rate.

Parameters

value Enter the sampling rate value.

Range:
- **C-Series and S-Series**: 256 to 8388608 packets
- **E-Series TeraScale and ExaScale**: 2 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduces on S-Series Stacking</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

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) Change 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 an 100/1000 Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a Loopback interface, enter the keyword loopback followed by a number from 0 to 16383.
- For a SONET interface, enter the keyword sonet followed by the 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.

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.4.6.0 Added support for the keyword fortyGigE.
Version 8.2.1.0 Introduced on S-Series Stacking
Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.7.1.0 Introduced on S-Series
Version 7.6.1.0 Introduced on C-Series
Version 6.2.1.1 Introduced on E-Series

Example

Figure 53-2. show sflow Command Example

```
FTOS#show sflow
sFlow services are enabled
Global default sampling rate: 32768
Global default counter polling interval: 20
1 collectors configured
Collector IP addr: 133.33.33.53, Agent IP addr: 133.33.33.116, UDP port: 6343
0 UDP packets exported
0 UDP packets dropped
165 sFlow samples collected
0 sFlow samples dropped due to sub-sampling  ← This count is always zero (0)

Linecard 1 Port set 0 H/W sampling rate 8192
 Gi 1/16: configured rate 8192, actual rate 8192, sub-sampling rate 1
 Gi 1/17: configured rate 16384, actual rate 16384, sub-sampling rate 2

Linecard 3 Port set 1 H/W sampling rate 16384
 Gi 3/40: configured rate 16384, actual rate 16384, sub-sampling rate 1
FTOS#
```

Usage Information

The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the figure above will always display a value of zero.

show sflow linecard

Display the sFlow information on a line card.

Syntax

```
show sflow linecard {slot number}
```
Parameters

```
slot number  (OPTIONAL) Enter a slot number to view information on the line card in that slot.
              Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
```

Command Modes

```
EXEC

EXEC Privilege
```

Command History

```
Version 8.2.1.0  Introduces on S-Series Stacking
Version 8.1.1.0  Introduced on E-Series ExaScale
Version 7.7.1.0  Introduced on S-Series
Version 7.6.1.0  Introduced on C-Series
Version 6.2.1.1  Introduced on E-Series
```

Example

```
Figure 53-3.  show sflow linecard Command Example

FTOS#show sflow linecard 1
Linecard 1
   Samples rcvd from h/w :165
   Samples dropped for sub-sampling :0
   Total UDP packets exported :0
   UDP packets exported via RPM :77
   UDP packets dropped :
FTOS#
```
SNMP and Syslog

Overview

This chapter contains commands to configure and monitor SNMP v1/v2/v3 and Syslog. Both features are supported on the C-Series, E-Series, and S-Series platforms, as indicated by the following symbols under each of the command headings: c e s

The chapter contains the following sections:

- SNMP Commands
- Syslog Commands

SNMP Commands

The SNMP commands available in Dell Networking OS 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 Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. Dell Networking OS 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. Dell Networking OS 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 LAN and WAN applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
  - SNMP Timeout — greater than 3 seconds
  - SNMP Retry count — greater than 2 seconds
- If you want to query an E-Series switch using SNMP v1/v2/v3 with an IPv6 address, configure the IPv6 address on a non-management port on the switch.
- If you want to send SNMP v1/v2/v3 traps from an E-Series using an IPv6 address, use a non-management port.
- SNMP v3 informs are not currently supported with IPv6 addresses.
- If you are using 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 VLAN.

show snmp

Display the status of SNMP network elements.

Syntax

```
show snmp
```

Command Modes

EXEC
EXEC Privilege

Command History

- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- E-Series legacy command

Example

```
Figure 54-1. 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 Get-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` Enable SNMP and set community string.
show snmp engineID

Display the identification of the local SNMP engine and all remote engines that are configured on the router.

Syntax

show snmp engineID

Command Modes

EXEC
EXEC Privilege

Command History

Version 7.6.1.0 Support added for S-Series
Version 7.5.1.0 Support added for C-Series
E-Series legacy command

Example

Figure 54-2. show snmp engineID Command

FTOS#show snmp engineID
Local SNMP engineID: 0000178B02000001E80214A8
Remote Engine ID IP-addr Port
80001F88043132333435 172.31.1.3 5009
80001F88043938373635 172.31.1.3 5008
FTOS#

Related Commands

snmp-server engineID Configure local and remote SNMP engines on the router

show snmp group

Display the group name, security model, status, and storage type of each group.

Syntax

show snmp group

Command Modes

EXEC
EXEC Privilege

Command History

Version 7.6.1.0 Support added for S-Series
Version 7.5.1.0 Support added for C-Series
E-Series legacy command

Usage Information

The following example 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 finally the row status is active.

Example

Figure 54-3. show snmp group Command Example

FTOS#show snmp group

    groupname: ngroup
    readview : nview
    notifyview: nview
    writeview: no write view specified
    row status: active
FTOS#
### show snmp user

**Syntax**
```
show snmp user
```

**Command Modes**
- EXEC
- EXEC Privilege

**Example**

Figure 54-4.  show snmp user Command Example

```
FTOS#show snmp user
User name: v1v2creadu
Engine ID: 0000178B02000001E80214A8
storage-type: nonvolatile active
Authentication Protocol: None
Privacy Protocol: None
FTOS#
```
Figure 54-5.  snmp ifmib ifalias long Command Example

 Syntax

```
snmp-server community

community-name
{ro | rw} [ipv6 ipv6-access-list-name [ipv6 ipv6-access-list-name | access-list-name | security-name name] | security-name name [ipv6 ipv6-access-list-name | access-list-name | security-name name] | access-list-name [ipv6 ipv6-access-list-name | access-list-name | security-name name]]
``` 

To remove access to a community, use the `no snmp-server community community-string {ro | rw} [security-name name [access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]]` command.

Parameters

- **community-name**: Enter a text string (up to 20 characters long) to act as a password for SNMP.
- **ro**: Enter the keyword *ro* to specify read-only permission.
- **rw**: Enter the keyword *rw* to specify read-write permission.
- **ipv6 access-list-name**: (Optional) Enter the keyword `ipv6` followed by a IPv6 ACL name (a string up to 16 characters long).
- **security-name name**: (Optional) Enter the keyword `security-name` followed by the security name as defined by the community MIB.
- **access-list-name**: (Optional) Enter a standard IPv4 access list name (a string up to 16 characters long).

Defaults

No default behavior or values

Command Modes

CONFIGURATION

Command History

- **Version 7.6.1.0**: Support added for S-Series
- **Version 7.5.1.0**: Support added for C-Series
- **pre-Version. 6.2.1.1**: Introduced on E-Series

Usage Information

The example below configures a community named `public` that is mapped to the security named `guestuser` with Read Only (ro) permissions.
Example

Figure 54-6.  snmp-server community Command Example

FTOS#config
FTOS(config)# snmp-server community public ro
FTOS(config)# snmp-server community guest ro security-name guestuser
FTOS(config)#

The **security-name** parameter maps the community string to an SNMPv3 user/security name as defined by the community MIB.

If a community string is configured without a **security-name** (for example, `snmp-server community public ro`), the community is mapped to a default security-name/group:

- `v1v2creadu / v1v2creadg` — maps to a community with `ro` permissions
- `v1v2cwriteu / v1v2cwriteg` — maps to a community with `rw` permissions

This command is indexed by the **community-name** parameter.

If the `snmp-server community` command is not configured, you cannot query SNMP data. Only Standard IPv4 ACL and IPv6 ACL is supported in the optional `access-list-name`.

The command options `ipv6`, `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. The following example demonstrates the creation of a standard IPv4 ACL called “snmp-ro-acl” and then assigning it to the SNMP community “guest”:

Example

Figure 54-7.  snmp-server community Command Example

FTOS(config)# ip access-list standard snmp-ro-acl
FTOS(config-standard-nacl)#seq 5 permit host 10.10.10.224
FTOS(config-standard-nacl)#seq 10 deny any count
!
FTOS(config)#snmp-server community guest ro snmp-ro-acl
FTOS(config)#

Note: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP, ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valid for SNMP.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list standard</code></td>
</tr>
<tr>
<td><code>ipv6 access-list</code></td>
</tr>
<tr>
<td><code>show running-config snmp</code></td>
</tr>
</tbody>
</table>

**snmp-server contact**

Configure contact information for troubleshooting this SNMP node.

**Syntax**

```
snmp-server contact text
```

**Parameters**

- `text`  
Enter an alphanumeric text string, up to 55 characters long.
snmp-server enable traps

Enable and configure 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

- **notification-type**
  - `bgp` — Notification of changes in BGP process
  - `envmon` — For Dell Force10, device notifications when an environmental threshold is exceeded
  - `snmp` — Notification of RFC 1157 traps.
  - `stp` — Notification of state change in Spanning Tree protocol (RFC 1493)
  - `vrrp` — Notification of state change in a VRRP group
  - `xstp` — Notification of state change in MSTP (802.1s), RSTP (802.1w), and PVST+
  - `vlt` — Notification of state change in VLT process

- **notification-option**
  - For the `envmon` notification-type, enter one of the following optional parameters:
    - `fan`
    - `supply`
    - `temperature`
  - For the `snmp` notification-type, enter one of the following optional parameters:
    - `authentication`
    - `coldstart`
    - `linkdown`
    - `linkup`

Defaults

Not enabled.

Command Modes

- **CONFIGURATION**

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.5</td>
<td>New format for VRRP traps was introduced on the C-Series. New STP, RSTP, and PVST+ traps for root and topology changes were added on the C-Series.</td>
</tr>
<tr>
<td>8.4.1.3</td>
<td>New format for VRRP traps was introduced on the E-Series ExaScale. New STP, RSTP, and PVST+ traps for root and topology changes were added on the E-Series ExaScale.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Support was added for VRRP traps.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series; Added support for STP and xSTP traps.</td>
</tr>
</tbody>
</table>
Dell Networking OS supports up to 16 SNMP trap receivers.

If this command is not configured, 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` - Enable SNMP and set the community string.

**snmp-server engineID**

**Syntax**

```
snmp-server engineID [local engineID] [remote ip-address vrf vrf-id udp-port port-number engineID]
```

To return to the default, use the `no snmp-server engineID [local engineID] [remote ip-address vrf vrf-name udp-port port-number engineID]` command

**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.
  - The first 4 octets are set to the private enterprise number.
  - The remaining 8 octets are the MAC address of the chassis.

- **vrf vrf-name**
  - (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.

- **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 8.4.6.0 Added support for VRF.
- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- E-Series legacy command

**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 an MD5 (Message Digest Algorithm) or SHA (Secure Hash Algorithm) 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**
  Display SNMP engine and all remote engines that are configured on the router
- **show running-config snmp**
  Display 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 | ipv6 access-list-name | access-list-name ipv6 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 | ipv6 access-list-name | access-list-name ipv6 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.
  - `vlv2creadg` — maps to a community/security-name with `ro` permissions
  - `l1v2cwriteg` — 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series legacy command</td>
</tr>
</tbody>
</table>

Usage Information

The following example specifies the group named harig as a version 3 user requiring both authentication and encryption and read access limited to the read named rview.

```
FTOS#conf
FTOS(conf)# snmp-server group harig 3 priv read rview
FTOS#
```

- **Note:** For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP, ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valid for SNMP.

**Example**

**Figure 54-8. 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.

**Related Commands**

- `show snmp group` Display the group name, security model, view status, and storage type of each group.
- `show running-config snmp` Display the SNMP running configuration

### snmp-server host

Configure the recipient of an SNMP trap operation.

**Syntax**

```
snmp-server host ip-address | ipv6-address [vrf vrf-name 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 | ipv6-address [vrf vrf-name 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).
- `ipv6-address` Enter the keyword `host` followed by the IPv6 address of the host in the `X::X::X::X` format.
  - The `::` notation specifies successive hexadecimal fields of zero
- `vrf vrf-name` Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
**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.

**udp-port**

**port-number** (OPTIONAL) Enter the keywords **udp-port** followed by the port number of the remote host to use.
Range: 0 to 65535.
Default: 162

**notification-type** (OPTIONAL) Enter one of the following keywords for the type of trap to be sent to the host:
- **bgp** - BGP state change
- **envmon** - Environment monitor trap
- **snmp** - SNMP notification (RFC 1157)
- **stp** - Spanning Tree protocol notification (RFC 1493)
- **vrrp** - State change in a VRRP group
- **xstp** - State change in MSTP (802.1s), RSTP (802.1w), and PVST+
Default: All trap types are sent to host.

**Defaults**
As shown

**Command Modes**
CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Support Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Support was added for VRRP traps.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series; Added support for STP and xSTP notification types.</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.

### Configuring Informs

To send an inform, follow the step below.

1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group for this user with access rights.
4. Enable traps.
5. Configure a host to receive informs.

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server enable traps</code></td>
<td>Enable SNMP traps.</td>
</tr>
<tr>
<td><code>snmp-server community</code></td>
<td>Configure 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, enter `no snmp-server location`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>text</code></td>
<td>Enter an alpha-numeric text string, up to 55 characters long.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.
### 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**

- `byte-count`: Enter one of the following values 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.

**Defaults**

8

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>E-Series</td>
<td>Legacy command</td>
</tr>
</tbody>
</table>

### 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, enter `no snmp trap-source`.

**Parameter**

- `interface`: Enter the following keywords and slot/port or number information:
  - For an 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
  - For a SONET interface, enter the keyword `sonet` followed by the 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.

**Defaults**

The IP address assigned to the management interface is the default.

**Command Modes**

CONFIGURATION
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`  Set the community string.

---

## snmp-server user

Configure a new user to an SNMP group.

### Syntax

```
snmp-server user name {group_name remote ip-address vrf vrf-name udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]
```

To remove a user from the SNMP group, use the `no snmp-server user name {group_name remote ip-address vrf vrf-name udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access-list-name | ipv6 access-list-name | access-list-name ipv6 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.
  - vl2vcreadu — maps to a community with ro permissions
  - lv2v2creadu — 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.
- **vrf vrf-name**: Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- **udp-port port-number**: Enter the keyword `udp-port` followed by the UDP (User Datagram Protocol) port number on the remote device. Range: 0 to 65535. Default: 162

- **1 | 2c | 3**: (OPTIONAL) Enter the security model version number (1, 2c, or 3).
  - 1 is the least secure version
  - 3 is the most secure of the security modes.
  - 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
  Default: 1

- **encrypted**: (OPTIONAL) Enter the keyword `encrypted` to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
- **auth**: (OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
**Defaults**
As above

**Command Modes**
CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>E-Series</td>
<td>E-Series legacy command</td>
</tr>
</tbody>
</table>

**Usage Information**

- **Note:** For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP, ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valid for SNMP.

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. The following command is an example of how to specify the command with an encrypted string:

**Examples**

- **Figure 54-9. snmp-server user Command Example**

  FTOS# snmp-server user privuser v3group v3 encrypted auth md5 9fc53d9d908118b2804fe80e3ba8763d priv des56 d0452401a8c3ce42804fe80e3ba8763d

---

**md5 | sha**

(OPTIONAL) Enter the keyword `md5` or `sha` to designate the authentication level.

- **md5** — Message Digest Algorithm
- **sha** — Secure Hash Algorithm

**auth-password**

(OPTIONAL) Enter a text string (up to 20 characters long) password that will enable the agent to receive packets from the host.

Minimum: 8 characters long

**priv des56**

(Optional) Enter the keyword `priv des56` to initiate a privacy authentication level setting using the CBC-DES privacy authentication algorithm (`des56`).

**priv password**

(Optional) Enter a text string (up to 20 characters long) password that will enable the host to encrypt the contents of the message it sends to the agent.

Minimum: 8 characters long

**access-list-name**

(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).

**ipv6**

```
access-list-name
```

(Optional) Enter the keyword `ipv6` followed by the IPv6 access list name (a string up to 16 characters long)

**access-list-name**

(Optional) Enter both an IPv4 and IPv6 access list name.
The following command is an example of how to enter a plain-text password as the string `authpasswd` for user `authuser` of group `v3group`.

```
FTOS(conf)# snmp-server user authuser v3group v3 auth md5 authpasswd
```

The following command configures a remote user named `n3user` with a `v3` security model and a security level of `authNOPriv`.

```
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><code>show snmp user</code></td>
<td>Display 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><code>view-name</code></td>
<td>Enter the name of the view (not to exceed 20 characters).</td>
</tr>
<tr>
<td><code>oid-tree</code></td>
<td>Enter the OID sub tree for the view (not to exceed 20 characters).</td>
</tr>
<tr>
<td><code>included</code></td>
<td>(OPTIONAL) Enter the keyword <code>included</code> to include the MIB family in the view.</td>
</tr>
<tr>
<td><code>excluded</code></td>
<td>(OPTIONAL) Enter the keyword <code>excluded</code> to exclude the MIB family in the view.</td>
</tr>
</tbody>
</table>

### Defaults

No default behavior or values

### Command Modes

- **CONFIGURATION**

### Command History

- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- E-Series legacy command
The \textit{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. The following example configures a view named \texttt{rview} that allows access to all objects under 1.3.6.1:

\begin{verbatim}
FTOS# conf
FTOS#(conf) snmp-server view rview 1.3.6.1 included
\end{verbatim}

**Usage Information**

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{show running-config snmp}</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, enter \texttt{no snmp trap link-status}.

**Defaults**

Enabled.

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

If the interface is expected to flap during normal usage, you could disable this command.

### Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches:

- clear logging
- default logging buffered
- default logging console
- default logging monitor
- default logging trap
- logging
- logging buffered
- logging console
- logging facility
- logging history
- logging history size
- logging monitor
- logging on
• logging source-interface
• logging synchronous
• logging trap
• show logging
• show logging driverlog stack-unit (S-Series)
• terminal monitor

**clear logging**

This command clears messages in the logging buffer.

**Syntax**
clear logging

**Defaults**
None.

**Command Modes**
EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series legacy command</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>Display logging settings and system messages in the internal buffer.</td>
</tr>
</tbody>
</table>

**default logging buffered**

This command returns to the default setting for messages logged to the internal buffer.

**Syntax**
default logging buffered

**Defaults**
size = 40960; level = 7 or debugging

**Command Modes**
CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series legacy command</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging buffered</td>
<td>Set the logging buffered parameters.</td>
</tr>
</tbody>
</table>

**default logging console**

This command returns to the default settings for messages logged to the console.

**Syntax**
default logging console

**Defaults**
level = 7 or debugging
default logging monitor

Return to the default settings for messages logged to the terminal.

**Syntax**

```
default logging monitor
```

**Defaults**

level = 7 or debugging

---

**default logging trap**

Return to the default settings for logging messages to the Syslog servers.

**Syntax**

```
default logging trap
```

**Defaults**

level = 6 or informational

---

**Related Commands**

- **logging console**
  
  Set the logging console parameters.

- **logging monitor**
  
  Set the logging monitor parameters.

- **terminal monitor**
  
  Send system messages to the terminal/monitor.

- **logging trap**
  
  Limit 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 both IPv4 and/or IPv6 can be configured.

**Syntax**

logging {ipv4-address | ipv6-address | hostname} [vrf vrf-name]

To disable logging, enter `no logging`.

**Parameters**

- `ipv4-address`: Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) address.
- `ipv6-address`: (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF. Range: 1 to 63.
- `hostname`: Enter the name of a host already configured and recognized by the switch.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- `logging on` Enables the logging asynchronously to logging buffer, console, Syslog server, and terminal lines.
- `logging trap` Enables logging to the Syslog server based on severity.

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, enter `default logging buffered`. To disable logging stored to an internal buffer, enter `no logging buffered`.

**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
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging</td>
<td>Clear the logging buffer.</td>
</tr>
<tr>
<td>default logging</td>
<td>Returns the logging buffered parameters to the default setting.</td>
</tr>
<tr>
<td>buffered</td>
<td></td>
</tr>
<tr>
<td>show logging</td>
<td>Display the logging setting and system messages in the internal buffer.</td>
</tr>
</tbody>
</table>

logging console

Specify which messages are logged to the console.

Syntax

```
logging console [level]
```

To return to the default values, enter `default logging console`. To disable logging to the console, enter `no logging console`.

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.
```

Defaults 7 or debugging

Command Modes CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series legacy command</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging</td>
<td>Clear logging buffer.</td>
</tr>
<tr>
<td>default logging</td>
<td>Returns the logging console parameters to the default setting.</td>
</tr>
<tr>
<td>buffered</td>
<td></td>
</tr>
<tr>
<td>show logging</td>
<td>Display logging settings and system messages in the internal buffer.</td>
</tr>
</tbody>
</table>

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, enter `no logging facility`. 
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**

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
</tbody>
</table>

E-Series legacy command

Related Commands

- **logging**  
  Enable logging to a Syslog server.
- **logging on**  
  Enables logging.

---

**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, enter **no logging history**.
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**

- `show logging history` Display information logged to the history buffer.

---

**logging history size**

Specify the number of messages stored in the FTOS logging history table.

**Syntax**

```
logging history size size
```

To return to the default values, enter `no logging history size`.

**Parameters**

- `size` Indicate a value as the number of messages to be stored.

  - Range: 0 to 500.
  - Default: 1 message.

**Defaults**

1 message

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
</tbody>
</table>

**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**

- `show logging history` Display information logged to the history buffer.
logging monitor

Specify which messages are logged to Telnet applications.

**Syntax**

```
logging monitor [level]
```

To disable logging to terminal connections, enter `no logging monitor`.

**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**

- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- E-Series legacy command

**Related Commands**

- `default logging monitor` Returns the logging monitor parameters to the default setting.

logging on

Specify that debug or error messages are asynchronously logged to multiple destinations, such as logging buffer, Syslog server, or terminal lines.

**Syntax**

```
logging on
```

To disable logging to logging buffer, Syslog server and terminal lines, enter `no logging on`.

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

- Version 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- E-Series legacy command

**Usage Information**

When you enter `no logging on`, messages are logged only to the console.

**Related Commands**

- `logging` Enable logging to Syslog server.
- `logging buffered` Set the logging buffered parameters.
- `logging console` Set the logging console parameters.
- `logging monitor` Set the logging parameters for the terminal connections.
logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

**Syntax**

```
logging source-interface interface
```

To disable this command and return to the default setting, enter `no logging source-interface`.

**Parameters**

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For an 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
    - For Loopback interfaces, enter the keyword `loopback` followed by a number from zero (0) to 16383.
    - For the management interface on the RPM, 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:
      - **C-Series and S-Series** Range: 1-128
      - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
    - For a SONET interface, enter the keyword `sonet` followed by the slot/port 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.
    - For a VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
</tbody>
</table>

**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` — Enable 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Enter the keyword <code>all</code> to ensure that all levels are printed asynchronously.</td>
</tr>
<tr>
<td><strong>level level</strong></td>
<td>Enter the keyword <code>level</code> 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</td>
</tr>
<tr>
<td><strong>limit number-of-buffers</strong></td>
<td>Enter the keyword <code>limit</code> followed by the number of buffers to be queued for the terminal after which new messages are dropped. Range: 20 to 300. Default: 20</td>
</tr>
</tbody>
</table>

**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 7.6.1.0  Support added for S-Series
- Version 7.5.1.0  Support added for C-Series
- E-Series legacy command

**Usage Information**

When `logging synchronous` is enabled, 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 the message severity.

**Syntax**

```
logging trap [level]
```

To return to the default values, enter `default logging trap`. To disable logging, enter `no logging trap`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>level</strong></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 6.</td>
</tr>
</tbody>
</table>
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. Slots *7* and *8* represent RPMs.

**Command Modes**

- EXEC
- EXEC Privilege
show logging driverlog stack-unit (S-Series)

Display the driver log for the specified stack member.

Syntax

```
show logging driverlog stack-unit unit#
```

Parameters

- **stack-unit unit#**
  - Enter the keyword `stack-unit` followed by the stack member ID of the switch for which you want to display the driver log.
  - Range: 0 to 1

Defaults

No default values or behavior

---

**Figure 54-11.  show logging Command Example (Partial)**

```
FTOS#show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 5604 Messages Logged, Size (524288 bytes)
  Trap logging: level informational
Oct 8 09:25:37: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor 223.80.255.254 closed. Hold time expired
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.1.3 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.13 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.1.42 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.14 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.15 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.4.1.3 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.6 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.12 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.15 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.3 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.12.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Session closed by neighbor 1.1.10.2 (Hold time expired)
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor 1.1.11.2 closed. Neighbor recycled
```

**Figure 54-12.  show logging history Command Example**

```
FTOS#show logging history
Syslog History Table: 1 maximum table entries, saving level Warnings or higher
SNMP notifications not Enabled
%RPM:0:0 %CHMGR-2-LINECARDDOWN - Line card 3 down - IPC timeout
FTOS#
```
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**

```plaintext
terminal monitor
```

To return to default settings, enter `terminal no monitor`.

**Defaults**

Disabled.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- `logging monitor`: Set the logging parameters on the monitor/terminal.
SONET

Overview

Dell Networking OS supports RFC 2558 “Definitions of Managed Objects for the SONET/SDH Interface” and RFC 2615 “PPP-over-SONET/SDH” only on the E-Series platform, as indicated by this character under each command heading in this chapter: [E]

Commands

This chapter contains the commands to configure Packet Over SONET/SDH (POS/SDH) interfaces and features, including Point-to-Point Protocol (PPP) encapsulation.

- ais-shut
- alarm-report
- clock source
- debug ppp
- delay triggers
- down-when-looped
- encapsulation
- flag
- framing
- interface sonet
- keepalive
- loopback
- ppp authentication
- ppp chap hostname
- ppp chap password
- ppp chap rem-hostname
- ppp chap rem-password
- ppp next-hop
- ppp pap hostname
- ppp pap password
- ppp pap rem-hostname
- ppp pap rem-password
- scramble-atm
- show controllers
• show interfaces
• sonet-port-recover detection-interval
• speed

ais-shut

Enable an alarm indication signal (AIS) when the SONET interface is shutdown.

Syntax

ais-shut

To disable the AIS, enter no ais-shut.

Defaults

Disabled.

Command Modes

INTERFACE

alarm-report

Specify which POS/SDH alarms to report to the remote SNMP server.

Syntax

alarm-report {lais | lrdi | pais | plop | prdi | sd-ber | sf-ber | slof | slos}

To disable an alarm, use the no alarm-report {lais | lrdi | pais | plop | prdi | sd-ber | sf-ber | slof | slos} command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lais</td>
<td>Enter the keyword lais to report line alarm indication signal.</td>
</tr>
<tr>
<td>lrdi</td>
<td>Enter the keyword lrdi to report line remote defect indicator.</td>
</tr>
<tr>
<td>pais</td>
<td>Enter the keyword pais to report path alarm indication signal.</td>
</tr>
<tr>
<td>plop</td>
<td>Enter the keyword plop to report path loss of pointer.</td>
</tr>
<tr>
<td>prdi</td>
<td>Enter the keyword prdi to report the path remote defect indication.</td>
</tr>
<tr>
<td>sd-ber</td>
<td>Enter the keyword sd-ber to report signal degradation BER errors.</td>
</tr>
<tr>
<td>sf-ber</td>
<td>Enter the keyword sf-ber to report signal failure BER errors.</td>
</tr>
<tr>
<td>slof</td>
<td>Enter the keyword slof to report section loss of frame.</td>
</tr>
<tr>
<td>slos</td>
<td>Enter the keyword slos to report section loss of signal.</td>
</tr>
</tbody>
</table>

Defaults

Disabled—no alarm reporting for all alarms

Command Modes

INTERFACE

Usage Information

Alarm reporting is available with this command. SNMP traps are available; however, syslogs are not generated. To display active alarms and defects, use the show controllers command. The table below defines the alarms that can be enabled by this command. If enabled for reporting, the alarms will generate reports on a trap receiver.
Table 55-1. Alarm Definitions

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bais</td>
<td>Line Alarm Indication Signal</td>
</tr>
<tr>
<td>lrdi</td>
<td>Line Remote Defect Indication</td>
</tr>
<tr>
<td>pais</td>
<td>Path Alarm Indication Signal</td>
</tr>
<tr>
<td>plop</td>
<td>Path loss of Pointer</td>
</tr>
<tr>
<td>prdi</td>
<td>Path Remote Defect Indication</td>
</tr>
<tr>
<td>sd-ber</td>
<td>LBIP BER in excess of Signal Degradation threshold. The default SD alarm value is 10^-6, this value can not be changed.</td>
</tr>
<tr>
<td>sf-ber</td>
<td>LBIP BER in excess of Signal Failure threshold. The default SF alarm value is 10^-3, this value can not be changed.</td>
</tr>
<tr>
<td>slof</td>
<td>Section Loss of Frame</td>
</tr>
<tr>
<td>slos</td>
<td>Section Loss of Signal</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show controllers</td>
<td>Display alarms and defects</td>
</tr>
</tbody>
</table>

clock source

Configure the clock source for each POS/SDH interface.

Syntax

clock source \{internal | line\}

To return to the default setting, enter no clock source.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>Enter the keyword internal to use the internal clock from the interface.</td>
</tr>
<tr>
<td>line</td>
<td>Enter the keyword line to use the recovered clock from the interface. This is the default.</td>
</tr>
</tbody>
</table>

Defaults  line

Command Modes  INTERFACE

dep ppp

Display traffic and information in a Point-to-Point Protocol (PPP) network.

Syntax

dep ppp [authentication | error | negotiation | packet] interface sonet slot/port

To disable debugging, enter no debug dep.
If you enter `debug ppp` without parameters, all parameters are enabled.

### delay triggers

Delay triggering the line or path alarms with a 100ms delay.

#### Syntax

```
delay triggers {line [lrdi | sd-ber | sf-ber] | path [pais | prdi]}
```

To disable delay trigger (the default), enter `no delay triggers {line [lrdi | sd-ber | sf-ber] | path [pais | prdi]}` command.

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>line</strong></td>
<td>Enter the keyword <code>line</code> to delay the specified line alarm.</td>
</tr>
<tr>
<td><strong>lrdi</strong></td>
<td>(OPTIONAL) Enter the keyword <code>lrdi</code> to specify line remote defect indicator.</td>
</tr>
<tr>
<td><strong>sd-ber</strong></td>
<td>(OPTIONAL) Enter the keyword <code>sd-ber</code> to specify signal degradation BER errors.</td>
</tr>
<tr>
<td><strong>sf-ber</strong></td>
<td>(OPTIONAL) Enter the keyword <code>sf-ber</code> to specify signal failure BER errors.</td>
</tr>
<tr>
<td><strong>path</strong></td>
<td>Enter the keyword <code>path</code> to delay the specified path alarm.</td>
</tr>
<tr>
<td><strong>pais</strong></td>
<td>(OPTIONAL) Enter the keyword <code>pais</code> to specify path alarm indication signal.</td>
</tr>
<tr>
<td><strong>prdi</strong></td>
<td>(OPTIONAL) Enter the keyword <code>prdi</code> to specify the path remote defect indication.</td>
</tr>
</tbody>
</table>

#### Defaults

Disabled

#### Command Modes

INTERFACE

#### Command History

Version 7.4.2.0 Added path option

#### Usage Information

By default, certain alarms (LOS, LOF, LAIS, PLOP) bring the line protocol down immediately. Use this command, with the `line` option, to delay that trigger event by 100ms.

By default, path alarms (AIS, RDI, LOP) do not cause (or trigger) the interface line protocol to go down. This command, with the `path` option, can be used to trigger this action with a delay of 100ms.
down-when-looped

Set the interface to send a system message when it detects a loopback condition and goes down.

Syntax down-when-looped

To disable notification, enter no down-when-looped.

Defaults Enabled

Command Modes INTERFACE

encap

Configure encapsulation for a PPP interface.

Syntax encap ppp

To remove encapsulation, enter no encap.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp</td>
<td>Enter the keyword ppp for Point-to-Point Protocol encapsulation.</td>
</tr>
</tbody>
</table>

Defaults Not configured.

Command Modes INTERFACE

Usage Information

When you enter the no encap command, you administratively shutdown the interface and configuration information (such as IP address) is deleted from the interface. A SONET interface without encapsulation is always operationally down.

When you enable encapsulation on the interface, PPP negotiation begins after you enable the interface (no shutdown command). You can enable authentication and other related commands once negotiation is completed.

Note: Encapsulation must be configured before the interface is enabled for traffic.

flag

Set the overhead bytes in the frame header to ensure interoperability between different vendor equipment.

Syntax flag {c2 | j0} value

To return to the default value, use no flag {c2 | j0} command.
framing

Set the type of framing used on a POS/SDH interface.

Syntax

framing \{sdh | sonet\}

To return to the default, enter no framing.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdh</td>
<td>Enter the keyword sdh to specify Synchronous Digital Hierarchy (SDH) framing. Default: Sonet</td>
</tr>
<tr>
<td>sonet</td>
<td>Enter the keyword sonet to specify SONET framing. Default: Sonet</td>
</tr>
</tbody>
</table>

Defaults

sonet

Command Modes

INTERFACE

Usage Information

Framing should be changed only when the interfaces are shutdown.

hardware monitor mac action-on-error port-shutdown

Shut down and bring back up the port (flap).

Syntax

hardware monitor mac action-on-error port-shutdown

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 7.7.1.0 Introduced command
interface sonet

Enter the INTERFACE mode to configure a POS/SDH interface.

Syntax

```
interface sonet slot/port
```

Parameters

```
slot/port
```
Enter the slot/port information.

Defaults

Not configured

Command Modes

CONFIGURATION

Example

```
Figure 55-1. interface sonet Command Example

FTOS(conf)#interface sonet 8/2
FTOS(conf-if-so-8/2)#
```

Usage Information

You cannot delete POS/SDH interfaces. By default, POS/SDH interfaces are disabled (shutdown). Use the `encap` command to enable encapsulation on the interface.

Related Commands

```
encap
```
Configure PPP encapsulation.

keepalive

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

Syntax

```
keepalive [seconds]
```

Parameters

```
seconds
```
(Optional) For POS/SDH interfaces with encapsulation enabled, enter the number of seconds between keepalive packets.

Range: 0 to 32767

Default: 10 seconds

Defaults

Enabled.

Command Modes

INTERFACE

Usage Information

When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

loopback

Troubleshoot a POS/SDH interface by looping back traffic through the interface or the line.
loopback \{internal | line\}

To delete a loopback setting, use the no loopback \{internal | line\} command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>Enter the keyword internal to test the physical interface by sending incoming traffic back through the interface.</td>
</tr>
<tr>
<td>line</td>
<td>Enter the keyword line to test connectivity to the network by sending incoming traffic back to the network.</td>
</tr>
</tbody>
</table>

| Defaults   | Not configured. |

| Command Modes | INTERFACE |

Usage Information
Use the show config command in the INTERFACE mode to determine if the loopback command was configured.

Related Commands
show config Display the interface configuration.

ppp authentication

Enable Challenge-Handshake Authentication Protocol (CHAP) and/or Password Authentication Protocol (PAP) authentication on the interface.

Syntax ppp authentication \{chap | chap pap | pap | pap chap\}

To remove all PPP authentication, enter no ppp authenticate.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chap</td>
<td>Enter the keyword chap to enable CHAP authentication only.</td>
</tr>
<tr>
<td>chap pap</td>
<td>Enter the keywords chap pap to enable CHAP on one side and PAP on the other.</td>
</tr>
<tr>
<td>pap</td>
<td>Enter the keyword pap to enable PAP authentication only.</td>
</tr>
<tr>
<td>pap chap</td>
<td>Enter the keywords pap chap to enable PAP on one side and CHAP on the other side.</td>
</tr>
</tbody>
</table>

| Defaults   | Not configured. |

| Command Modes | INTERFACE |

Usage Information
Once you configure this command, the remote device must prove its identity before the FTOS sends traffic.

The two authentication types differ slightly:

- With CHAP authentication, the E-Series sends a challenge to the remote device, which must encrypt the response with a shared value and return it to the E-Series with a username. The E-Series checks the local database for a match on the shared value and username.
- With PAP authentication, the remote device must send a username/password set which the FTOS checks against the local database. PAP passwords are sent as “clear text” and could be intercepted and used.
After you enable PPP authentication, you must configure remote hostnames and passwords to initiate authentication on the E-Series.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp chap hostname</code></td>
<td>Configure a hostname for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp chap password</code></td>
<td>Configure a password for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp chap rem-hostname</code></td>
<td>Configure a remote hostname for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp chap rem-password</code></td>
<td>Configure a remote password for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp pap hostname</code></td>
<td>Configure a hostname for PAP authentication.</td>
</tr>
<tr>
<td><code>ppp pap password</code></td>
<td>Configure a password for PAP authentication.</td>
</tr>
<tr>
<td><code>ppp pap rem-hostname</code></td>
<td>Configure a remote hostname for PAP authentication.</td>
</tr>
<tr>
<td><code>ppp pap rem-password</code></td>
<td>Configure a remote password for PAP authentication.</td>
</tr>
</tbody>
</table>

**ppp chap hostname**

Configure a hostname to be used in the CHAP authentication process.

**Syntax**

```
ppp chap hostname name
```

To remove the CHAP hostname, enter `no ppp chap hostname`.

**Parameters**

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

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Usage Information**

For peers to successfully negotiate authentication on both sides of the link, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp authentication</code></td>
<td>Enable CHAP or PAP or both authentication.</td>
</tr>
<tr>
<td><code>ppp chap password</code></td>
<td>Configure a password for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp chap rem-hostname</code></td>
<td>Configure a remote hostname for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp chap rem-password</code></td>
<td>Configure a remote password for CHAP authentication.</td>
</tr>
</tbody>
</table>

**ppp chap password**

Configure a password to be used in the CHAP authentication process.

**Syntax**

```
ppp chap password password
```

To remove the CHAP password, enter `no ppp chap password`.

**Parameters**

- `password` Enter a character string up to 32 characters long.

**Defaults**

Not configured.

**Command Modes**

INTERFACE
For peers to successfully negotiate authentication on both sides of the link, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp authentication</code></td>
<td>Enable CHAP or PAP or both authentication.</td>
</tr>
<tr>
<td><code>ppp chap hostname</code></td>
<td>Configure a hostname for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp chap rem-hostname</code></td>
<td>Configure a remote hostname for CHAP authentication.</td>
</tr>
<tr>
<td><code>ppp chap rem-password</code></td>
<td>Configure a remote password for CHAP authentication.</td>
</tr>
</tbody>
</table>

**ppp chap rem-hostname**

Configure a remote hostname to be used in the CHAP authentication process.

**Syntax**

```
ppp chap rem-hostname name
```

To remove the remote hostname, enter `no ppp chap rem-hostname`.

**Parameters**

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

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Usage Information**

For peers to successfully negotiate authentication on both sides of the link, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ppp chap rem-password</code></td>
<td>Configure a remote password for CHAP authentication.</td>
</tr>
</tbody>
</table>

**ppp chap rem-password**

Configure a remote password for CHAP authentication.

**Syntax**

```
ppp chap rem-password password
```

To remove a password, enter `no ppp chap rem-password`.

**Parameters**

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

**Defaults**

Not configure.

**Command Modes**

INTERFACE

**Usage Information**

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp authentication</td>
<td>Enable CHAP or PAP or both authentication.</td>
</tr>
<tr>
<td>ppp chap rem-hostname</td>
<td>Configure a remote host name for CHAP authentication.</td>
</tr>
<tr>
<td>ppp chap hostname</td>
<td>Configure a hostname for CHAP authentication.</td>
</tr>
<tr>
<td>ppp chap password</td>
<td>Configure a password for CHAP authentication.</td>
</tr>
</tbody>
</table>

### ppp next-hop

Assign an IP address as the next hop for this interface.

#### Syntax

```
ppp next-hop ip-address
```

To delete a next hop address, enter `no ppp next-hop`.

#### 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

#### Usage Information

This IP address must match the peer’s IP address or the link is not established. A peer will configure this IP address.

### ppp pap hostname

Configure a host name for PAP authentication.

#### Syntax

```
ppp pap hostname name
```

To delete a host name, enter `no ppp pap hostname`.

#### Parameters

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

#### Defaults

Not configured.

#### Command Modes

INTERFACE

#### Usage Information

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.
ppp pap password

Configure a password for PAP authentication.

Syntax

```
ppp pap password password
```

To delete a password, enter `no ppp pap password`.

Parameters

- `password` Enter a character string up to 32 characters long.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.

Related Commands

- `ppp authentication` Enable CHAP or PAP or both authentication.
- `ppp pap hostname` Configure a hostname for PAP authentication.
- `ppp pap rem-hostname` Configure a remote hostname for PAP authentication.
- `ppp pap rem-password` Configure a remote password for PAP authentication.

ppp pap rem-hostname

Configure a remote PAP hostname.

Syntax

```
ppp pap rem-hostname hostname
```

To delete a remote PAP host name, enter `no ppp pap rem-hostname`.

Parameters

- `hostname` Enter a character string up to 32 characters long.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.

Related Commands

- `ppp authentication` Enable CHAP or PAP or both authentication.
- `ppp pap rem-password` Configure remote password for PAP authentication.
- `ppp pap hostname` Configure a hostname for PAP authentication.
- `ppp pap password` Configure a password for PAP authentication.

ppp pap rem-password

Configure a remote PAP password.
**Syntax**

```plaintext
ppp pap rem-password password
```

To delete a remote PAP password, enter `no ppp pap rem-password`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>Enter a character string up to 32 characters long.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Usage Information**

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.

**Related Commands**

- `ppp authentication` Enable CHAP or PAP or both authentication.
- `ppp pap rem-hostname` Configure a remote hostname for PAP authentication.
- `ppp pap hostname` Configure a hostname for PAP authentication.
- `ppp pap password` Configure a password for PAP authentication.

---

**scramble-atm**

Enable POS/SDH payload scrambling on the interface.

**Syntax**

```plaintext
scramble-atm
```

To disable scrambling, enter `no scramble-atm`.

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Usage Information**

You must either enable payload scrambling or disable scambling on both ends of the link.

---

**show controllers**

Display troubleshooting information, such as the clock source, SONET alarms and error rates, and registers values.

**Syntax**

```plaintext
show controllers interface
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Enter the one of the following interface keywords and slot/port information:</td>
</tr>
<tr>
<td></td>
<td>- For a SONET interface, enter the keyword <code>sonet</code> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>- For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

EXEC Privilege
Example  

Figure 55-2.  show controllers sonet Command Example

```
FTOS#show controllers sonet
Interface is SONET 1/2

SECTION
  LOF = 0    LOS = 0                           BIP(B1)  = 0

LINE
  AIS = 0    RDI = 0               FEBE = 0    BIP(B2) = 0

PATH
  AIS = 0    RDI = 0    LOP = 0    FEBE = 0    BIP(B3) = 0

Active Defects: NONE

Enabled Alarms are listed here (default is none)
Active Alarms: NONE

Alarm reporting enabled for:  SLOS SLOF B1-TCA LAIS LRDI B2-TCA PAIS PRDI PLOP B3-TCA SD SF

Framing is SDH, AIS-shut is enabled
Scramble-ATM is enabled, Down-when-looped is enabled
Loopback is disabled, Clock source is internal, Speed is Oc48
CRC is 32-bits, Flag C2 is 0x16, Flag J0 is 0xcc, Flag S1S0 is 0x2
FTOS#
```

Example  

Figure 55-3.  show controllers tengigabitethernet Command Example

```
FTOS#show controllers te 4/1
Interface is TenGigabitEthernet 4/1

SECTION
  LOF = 0    LOS = 0                           BIP(B1)  = 13

LINE
  AIS = 0    RDI = 1               FEBE = 7633    BIP(B2) = 19264

PATH
  AIS = 0    RDI = 0    LOP = 0    FEBE = 8554    BIP(B3) = 15685

Active Defects: LRDI

Active Alarms: LRDI

Alarm reporting enabled for:  SLOS SLOF B1-TCA LAIS LRDI B2-TCA PAIS PRDI PLOP B3-TCA SD SF

Framing is SONET, AIS-shut is enabled
Scramble-ATM is enabled, Down-when-looped is enabled
Loopback is disabled, Clock source is line, Speed is Oc192
CRC is 32-bits, Flag C2 is 0x1a, Flag J0 is 0xcc, Flag S1S0 is 0x0
FTOS#
```

Table 55-2. Lines in show controllers interface Command Example

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface is...</td>
<td>Displays the interface type and the slot and port number information.</td>
</tr>
<tr>
<td>SECTION</td>
<td>Displays the section loss of frame (LOF) error. This error is detected when</td>
</tr>
<tr>
<td>LOF</td>
<td>a severely error framing (SEF) defect on the incoming interface signal persist for 3 milliseconds</td>
</tr>
</tbody>
</table>
show interfaces

Display detailed information on the Sonet or 10-Gigabit Ethernet interfaces.

**Syntax**

`show interfaces interface`

---

**Table 55-2. Lines in show controllers interface Command Example (continued)**

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOS</td>
<td>Displays the loss of signal (LOS) error. This error is detected when an all-zeros pattern on the incoming interface signal lasts 19 plus or minus 3 microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.</td>
</tr>
<tr>
<td>BIP(B1)</td>
<td>Displays the bit interleaved parity error for the B1 byte. For B1, the report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate section-level errors.</td>
</tr>
<tr>
<td>LINE AIS</td>
<td>Displays the alarm indication signal. This signal is sent by the section terminating equipment (STE) to alert the downstream line terminating equipment (LTE) that a LOS or LOF defect has been detected on the incoming interface section. Path alarm indication signal is sent by the LTE to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.</td>
</tr>
<tr>
<td>RDI</td>
<td>Displays remote defect indication. This indication is reported by the downstream LTE when it detects LOF, LOS, or AIS conditions.</td>
</tr>
<tr>
<td>BIP(B2)</td>
<td>Displays the bit interleaved parity error for the B2 byte. For B2, the report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate line-level errors.</td>
</tr>
<tr>
<td>PATH AIS</td>
<td>Displays the alarm indication signal. This signal is sent by the section terminating equipment (STE) to alert the downstream line terminating equipment (LTE) that a LOS or LOF defect has been detected on the incoming SONET section. Path alarm indication signal is sent by the LTE to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.</td>
</tr>
<tr>
<td>RDI</td>
<td>Displays remote defect indication. This indication is reported by the downstream LTE when it detects LOF, LOS, or AIS conditions.</td>
</tr>
<tr>
<td>BIP(B3)</td>
<td>Displays the bit interleaved parity error for the B3 byte. For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate path-level errors.</td>
</tr>
<tr>
<td>Active Defects:</td>
<td>Lists the current interface defects.</td>
</tr>
<tr>
<td>Active Alarms</td>
<td>List the current interface alarms as enforced the interface Alarm Hierarchy.</td>
</tr>
<tr>
<td>Alarm reporting enabled for:</td>
<td>List the alarms enabled. Enabled alarms generate trap reports.</td>
</tr>
</tbody>
</table>
### Parameters

*interface*

Enter the one of the following interface keywords and slot/port information:

- For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.

### Command Modes

**EXEC**

**EXEC Privilege**

### Example

**Figure 55-4. show interfaces sonet with PPP Encapsulation Command Example (EtherScale)**

```
FTOS>show interfaces sonet 2/0
SONET 2/0 is up, line protocol is up
Hardware is SONET, address is 00:01:e8:00:03:ff
Encapsulation PPP, Framing is SONET, AIS-shut is enabled
Scramble-ATM is enabled, Down-when-looped is enabled
Loopback is disabled, Clock source is internal, Speed is 0c48
CRC is 32-bits, Flag C2 is 0x16, Flag J0 is 0xcc, Flag S1S0 is 0x0
Keepalive Set (10 Sec)
LCP State: OPENED
IPCP State: OPENED
Internet address is 6.1.5.2/30
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2488 Mbit
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of "show interfaces" counters 17:08:10
Queueing strategy: fifo
91425052815 packets input, 6188485730919 bytes
Input 91425040617 IP Packets, 0 Vlans 0 MPLS
Received 0 input symbol errors, 0 runts, 0 giants, 0 throttles
0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
55176128354 packets output, 3677188351652 bytes, 474 underruns
Output 173858 Multicasts, 0 Broadcasts, 55175954550 Unicasts
55176116090 IP Packets, 0 Vlans, 0 MPLS
0 throttles, 474 discarded
Rate info (interval 299 minutes):
Input 1604.04Mbits/sec, 2583270 packets/sec
Output 1169.30Mbits/sec, 1913510 packets/sec
Time since last interface status change: 17:10:40

FTOS>
```

### Table 55-3. Fields in the show interfaces sonet with PPP Encapsulation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sonet 2/0...</td>
<td>Displays the interface’s type, slot/port and physical 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>Encapsulation is...</td>
<td>Displays the encapsulation method, the framing, and if the ais-shut command is enabled.</td>
</tr>
<tr>
<td>Scramble-ATM is enabled</td>
<td>States whether the scramble-atm and the down-when-looped commands are enabled.</td>
</tr>
<tr>
<td>Loopback is...</td>
<td>States whether the loopback, clock source, and speed, and flag commands are configured. This information is displayed over 2 lines.</td>
</tr>
<tr>
<td>Keepalive Set</td>
<td>Displays the number of seconds between keepalive messages.</td>
</tr>
<tr>
<td>LCP State:</td>
<td>States if LCP was successfully negotiated.</td>
</tr>
</tbody>
</table>
### Table 55-3. Fields in the show interfaces sonet with PPP Encapsulation (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPCP State:</td>
<td>States if IPCP was successfully negotiated.</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>Peer address</td>
<td>Displays the PPP peer’s IP address.</td>
</tr>
<tr>
<td>MTU 1554...</td>
<td>Displays link and IP MTU.</td>
</tr>
<tr>
<td>LineSpeed</td>
<td>Displays 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 <code>show interfaces</code> counters were cleared.</td>
</tr>
<tr>
<td>Queuing strategy.</td>
<td>States the packet queuing strategy. FIFO means first in first out.</td>
</tr>
<tr>
<td>0 packets...</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 2 lines. Any PPP packet less than 64 bytes in length will be padded out to 64 bytes upon reception. This padding will be counted by the ingress byte counter.</td>
</tr>
<tr>
<td>Received 0...</td>
<td>Displays the type and number of error or other specific packets received.</td>
</tr>
<tr>
<td>Output 0...</td>
<td>Displays the type and number of packets sent out the interface.</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>

**Related Commands**

- `show interfaces switchport` Displays Layer 2 information about the interfaces.
- `show ip interface` Displays Layer 3 information about the interfaces.

---

### sonet-port-recover detection-interval

**Syntax**

```plaintext
sonet-port-recover detection-interval interval
```

**Parameters**

- `interval` Interval for SONET port recovery (in seconds(15-600))

**Defaults**

- 60 seconds

**Command Modes**

- INTERFACE

**Privilege Level**

- 15 sys-hidden

**Recovery interval to automatically clear a condition that could cause a SONET port to hang, and stop sending and receiving data.**
When enabled, Dell Networking OS continuously polls status registers on SONET line cards. A port hang is declared when backpressure is detected on the port, and the port is brought down and then back up to clear the condition.

To keep a port in shutdown use the `hardware monitor mac action-on-error port-shutdown` command.

**speed**

Set the speed of the SONET interface.

**Syntax**

`speed {155 | 622 | 2488}`

To return to the default value, enter `no speed`.

**Parameters**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>155</td>
<td>Enter 155 to set the interface as OC3.</td>
</tr>
<tr>
<td>622</td>
<td>Enter 622 to set the interface as OC12.</td>
</tr>
<tr>
<td>2488</td>
<td>Enter 2488 to set the interface as OC48.</td>
</tr>
</tbody>
</table>

**Defaults**

2488

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for 2488 (OC48)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.4.1.0</td>
<td></td>
</tr>
</tbody>
</table>
S-Series Stacking Commands

Overview

All commands in this chapter are specific to the S-Series platform, as indicated by the \( S \) character that appears below each command heading. The commands are always available and operational, whether or not the S-Series has a stacking module inserted. You can use the commands to pre-configure a switch, so that the configuration settings are invoked when the switch is attached to other S-Series units.

For details on using the S-Series stacking feature, see the chapter “Stacking S-Series Switches” in the *Dell Networking OS Configuration Guide*.

\( \text{Note: } \) S-Series Stacking is not supported on the S60 system

Commands

The commands in this chapter are used for managing the stacking of S-Series systems:

- redundancy disable-auto-reboot
- redundancy force-failover stack-unit
- reset stack-unit
- show redundancy
- show system stack-ports
- stack-unit priority
- stack-unit provision
- stack-unit renumber
- upgrade system stack-unit (S-Series stack member)

redundancy disable-auto-reboot

\( S \) Prevent the S-Series stack management unit and standby unit from rebooting if they fails.

**Syntax**

`redundancy disable-auto-reboot [stack-unit | all]`

To return to the default, enter `no redundancy disable-auto-reboot stack-unit`.

**Defaults**

Disabled (the failed switch is automatically rebooted).
### Command Modes
<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGURATION</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added the <strong>all</strong> option</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

### Usage Information

Enabling this command keeps the failed switch in the failed state. It will not reboot until it is manually rebooted. When enabled, it is not displayed in the running-config. When disabled, it is displayed in the running-config.

### Related Commands

- **show redundancy**
  Display the current redundancy status.

---

#### redundancy force-failover stack-unit

**Syntax**

```plaintext
redundancy force-failover stack-unit
```

**Defaults**

Not enabled

**Command Modes**

EXEC Privilege

---

#### reset stack-unit

**Syntax**

```plaintext
reset stack-unit 0-7 hard
```

**Parameters**

- **0-7**
  Enter the stack member unit identifier of the stack member to reset.
- **hard**
  Reset the stack unit if the unit is in a problem state.

**Default**

none

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Added hard reset option.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Augmented to run on the standby unit in order to reset the standby unit directly.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Resetting the management unit is not allowed, and an error message will be displayed if you try to do so. Resetting is a soft reboot, including flushing the forwarding tables.

Starting with Dell Networking OS 7.8.1.0, you can run this command directly on the stack standby unit (standby master) to reset the standby. You cannot reset any other unit from the standby unit.
Example

Figure 56-1. Using the reset stack-unit Command on the Stack Standby Unit

FTOS#show system brief
Stack MAC : 00:01:e8:51:4e:f8

<table>
<thead>
<tr>
<th>Unit</th>
<th>UnitType</th>
<th>Status</th>
<th>ReqTyp</th>
<th>CurTyp</th>
<th>Version</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Member</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
<tr>
<td>1</td>
<td>Member</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
<tr>
<td>2</td>
<td>Member</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
<tr>
<td>3</td>
<td>Member</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
<tr>
<td>4</td>
<td>Standby</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
<tr>
<td>5</td>
<td>Member</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
<tr>
<td>6</td>
<td>Mgmt</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
<tr>
<td>7</td>
<td>Member</td>
<td>online</td>
<td>S50N</td>
<td>S50N</td>
<td>4.7.7.117</td>
<td>52</td>
</tr>
</tbody>
</table>

FTOS(standby)#reset ? <<Standby management unit
stack-unit <Unit number>
FTOS(standby)#reset stack-unit 7
<0-7> Unit number id
% Error: Reset of master unit is not allowed. <<Resetting master not allowed
FTOS(standby)#reset stack-unit 0
% Error: Reset of stack units from standby is not allowed. <<no reset of other member
FTOS(standby)#
FTOS(standby)#reset stack-unit 4 <<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: Gi 4/1-48
FTOS(standby)#rebooting
U-Boot 1.1.4 (Mar 6 2008 - 00:00:04)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Reboot Dell Networking OS.</td>
</tr>
<tr>
<td>upgrade (S-Series management unit)</td>
<td>Reset the designated S-Series 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 7.7.1.0 Introduced on S-Series
Example

Example Figure 56-2. show redundancy Command Output

FTOS#show redundancy
-- S-Series Redundancy Configuration --
----------------------------------------------
Auto reboot : Enabled
-- Stack-unit Status --
----------------------------------------------
Mgmt ID: 0
Stack-unit ID: 0
Stack-unit Redundancy Role: Primary
Stack-unit State: Active
Stack-unit SW Version: 7.7.1.0
Link to Peer: Up
-- PEER Stack-unit Status --
----------------------------------------------
Stack-unit State: Standby
Peer stack-unit ID: 1
Stack-unit SW Version: 7.7.1.0
-- 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: --
----------------------------------------------
Line Card Config: succeeded Mar 07 1996 00:27:39
Start-up Config: succeeded Mar 07 1996 00:27:39
Runtime Event Log: succeeded Mar 07 1996 00:27:39
Running Config: succeeded Mar 07 1996 00:27:39
ACL Mgr: succeeded Mar 07 1996 00:27:39

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy disable-auto-reboot</td>
<td>Prevent 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 S-Series 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 status to display the command output without the Connection field.</td>
</tr>
<tr>
<td>topology</td>
<td>(OPTIONAL) Enter the keyword topology to limit the table to just the Interface and Connection fields.</td>
</tr>
</tbody>
</table>

Defaults

No default behavior
**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>
</tr>
</thead>
<tbody>
<tr>
<td>0/49</td>
<td>1/49</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>0/50</td>
<td>0/49</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>0/51</td>
<td>2/49</td>
<td>24</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>1/49</td>
<td>0/49</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>1/50</td>
<td>2/51</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>2/49</td>
<td>0/51</td>
<td>24</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>2/51</td>
<td>1/50</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>2/52</td>
<td></td>
<td>12</td>
<td>up</td>
<td>down</td>
</tr>
</tbody>
</table>

FTOS#

**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>
</tr>
</thead>
<tbody>
<tr>
<td>0/49</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>0/50</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>0/51</td>
<td>24</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>1/49</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>1/50</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>2/49</td>
<td>24</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>2/51</td>
<td>12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>2/52</td>
<td>12</td>
<td>up</td>
<td>down</td>
</tr>
</tbody>
</table>

FTOS#

**show system stack-ports topology Command Example**

FTOS# show system stack-ports topology
Topology: Ring

<table>
<thead>
<tr>
<th>Interface</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/49</td>
<td>1/49</td>
</tr>
<tr>
<td>0/50</td>
<td></td>
</tr>
<tr>
<td>0/51</td>
<td>2/49</td>
</tr>
<tr>
<td>1/49</td>
<td>0/49</td>
</tr>
<tr>
<td>1/50</td>
<td>2/51</td>
</tr>
<tr>
<td>2/49</td>
<td>0/51</td>
</tr>
<tr>
<td>2/51</td>
<td>1/50</td>
</tr>
<tr>
<td>2/52</td>
<td></td>
</tr>
</tbody>
</table>

FTOS#

**show interfaces description Command Example Fields**

<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>
</tbody>
</table>
stack-unit priority

Configure the ability of an S-Series switch to become the management unit of a stack.

Syntax

```
stack-unit 0-7 priority 1-14
```

Parameters

- `0-7` Enter the stack member unit identifier, from 0 to 7, 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 0 the lowest priority and 14 the highest. The switch with the highest priority value will be chosen to become the management unit if the active management unit fails or on the next reload.

Defaults

1

Command Modes

CONFIGURATION

Command History

Version 7.7.1.0 Introduced on S-Series

Related Commands

- `reset stack-unit` - Reset the designated S-Series stack member.
- `show hardware stack-unit` - Display the data plane or management plane input and output statistics of the designated component of the designated stack member.
- `show system (S-Series)` - Display the current status of all stack members or a specific member.
- `upgrade (S-Series management unit)` - Upgrade the bootflash image or system image of the S-Series management unit.
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 0-7 provision {S25N|S25P|S25V|S50N|S50V}
```

Parameters

- **0-7**: Enter a stack member identifier, from 0 to 7, of the switch that you want to add to the stack.
- **S25N|S25P|S25V|S50N|S50V**: Enter the S-Series model identifier of the switch to be added as a stack member. This identifier is also referred to as the provision type.

Defaults

When this value is not set, a switch joining the stack is given the next available sequential stack member identifier.

Command Modes

CONFIGURATION

Command History

- **Version 7.7.1.0**: Introduced on S-Series

Related Commands

- **reload**: Reboot Dell Networking OS.
- **show system (S-Series)**: Display the current status of all stack members or a specific member.

Change the stack member ID of any stack member or a stand-alone S-Series.

Syntax

```
stack-unit 0-7 renumber 0-7
```

Parameters

- **0-7**: The first instance of this value is the stack member unit identifier, from 0 to 7, of the switch that you want to add to the stack. The second instance of this value is the desired new unit identifier number.

Defaults

none

Command Modes

EXEC Privilege

Command History

- **Version 7.7.1.0**: Introduced on S-Series

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 will reset and come up with the new unit number.
### upgrade system stack-unit (S-Series stack member)

Copy the boot image or Dell Networking OS from the management unit to one or more stack members.

**Syntax**

```
upgrade {boot | system} stack-unit {all | 0-7}
```

**Parameters**

- **boot**
  - Enter this keyword to copy the boot image from the management unit to the designated stack members.

- **system**
  - Enter this keyword to copy the Dell Networking OS image from the management unit to the designated stack members.

- **all**
  - Enter this keyword to copy the designated image to all stack members.

- **0-7**
  - Enter the unit ID of the stack member to which to copy the designated image.

**Defaults**

No configuration or default values

**Command Modes**

EXEC

**Command History**

Version 7.7.1.0 Introduced on S-Series

**Usage Information**

You must reload Dell Networking OS after using the `upgrade` command.

**Related Commands**

- `reload`
  - Reboot Dell Networking OS.

- `reset stack-unit`
  - Reset the designated S-Series stack member.

- `show system (S-Series)`
  - Display the current status of all stack members or a specific member.

- `show version`
  - Display the current Dell Networking OS version information on the system.

- `upgrade (S-Series management unit)`
  - Upgrade the bootflash image or system image of the S-Series management unit.
Storm Control

Overview

The Dell Networking OS Storm Control feature allows users to limit or suppress traffic during a traffic storm (Broadcast/Unknown Unicast Rate Limiting, or Multicast on the C-Series and S-Series).

Support for particular Dell Networking platforms (C-Series, E-Series, or S-Series) is indicated by the characters that appear below each command heading:

- C-Series: C
- E-Series: E
- S-Series: S

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

- Interface commands can only be applied on physical interfaces (VLANs and LAG interfaces are not supported).
- An INTERFACE-level command only support storm control configuration on ingress.
- An INTERFACE-level command overrides any CONFIGURATION-level ingress command for that physical interface, if both are configured.
- The CONFIGURATION-level storm control commands can be applied at ingress or egress and are supported on all physical interfaces.
- When storm control is applied on an interface, the percentage of storm control applied is calculated based on the advertised rate of the line card. It is not based on the speed setting for the line card.
Do not apply per-VLAN QoS on an interface that has storm control enabled (either on an interface or globally).

When broadcast storm control is enabled on an interface or globally on ingress, and DSCP marking for a DSCP value 1 is configured for the data traffic, the traffic will go to queue 1 instead of queue 0.

Similarly, if unicast storm control is enabled on an interface or globally on ingress, and DSCP marking for a DSCP value 2 is configured for the data traffic, the traffic will go to queue 2 instead of queue 0.

**Note:** Bi-directional traffic (unknown unicast and broadcast), along with egress storm control, causes the configured traffic rates to be split between the involved ports. The percentage of traffic that each port receives after the split is not predictable. These ports can be in the same/different port pipes, or the same/different line cards.

### 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 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the 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.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - Fast Ethernet is not supported.

**Defaults**

No default behavior or values

**Command Modes**

EXEC

EXEC Privilege

**Command History**

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **Version 6.5.1.0** Introduced on E-Series

**Example**

**Figure 57-1. show storm-control broadcast Command Example (E-Series)**

```
FTOS#show storm-control broadcast gigabitethernet 11/11
Broadcast storm control configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Direction</th>
<th>Percentage</th>
<th>Wred Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 11/11</td>
<td>Ingress</td>
<td>5.6</td>
<td></td>
</tr>
<tr>
<td>Gi 11/11</td>
<td>Egress</td>
<td>5.6</td>
<td>-</td>
</tr>
</tbody>
</table>
FTOS#
```
Example

Figure 57-2. show storm-control broadcast Command Example (C-Series)

FTOS#show storm-control broadcast gigabitethernet 3/24

Broadcast storm control configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Direction</th>
<th>Packets/Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 3/24</td>
<td>Ingress</td>
<td>1000</td>
</tr>
</tbody>
</table>

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 Fast Ethernet, enter the keyword `Fastethernet` followed by the slot/port information.
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the 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.

Defaults

No default behavior or values

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 8.4.6.0  
  Added support for the keyword `fortyGigE`.
- Version 7.6.1.0  
  Introduced on C-Series and S-Series

Example

Figure 57-3. show storm-control multicast Command Example

FTOS#show storm-control multicast gigabitethernet 1/0

Multicast storm control configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Direction</th>
<th>Packets/Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 1/0</td>
<td>Ingress</td>
<td>5</td>
</tr>
</tbody>
</table>

FTOS#
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 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the 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.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - Fast Ethernet is not supported.

Defaults

No default behavior or values

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 8.4.6.0**  
  Added support for the keyword `fortyGigE`.
- **Version 7.6.1.0**  
  Introduced on S-Series
- **Version 7.5.10**  
  Introduced on C-Series
- **Version 6.5.1.0**  
  Introduced on E-Series

Example

**E-Series**

```
FTOS#show storm-control unknown-unicast gigabitethernet 11/1

Unknown-unicast storm control configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Direction</th>
<th>Percentage</th>
<th>Wred Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 11/1</td>
<td>Ingress</td>
<td>5.9</td>
<td>-</td>
</tr>
<tr>
<td>Gi 11/1</td>
<td>Egress</td>
<td>5.7</td>
<td>w8</td>
</tr>
</tbody>
</table>

FTOS#
```

**C-Series**

```
FTOS#show storm-control unknown-unicast gigabitethernet 3/0

Unknown-unicast storm control configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Direction</th>
<th>Packets/Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 3/0</td>
<td>Ingress</td>
<td>1000</td>
</tr>
</tbody>
</table>

FTOS#
```
storm-control broadcast (Configuration)

Configure the percentage of broadcast traffic allowed in or out of the network.

Syntax

```
storm-control broadcast [percentage decimal_value in | out] [wred-profile name]
[packets_per_second in]
```

To disable broadcast rate-limiting, use the `storm-control broadcast [percentage decimal_value in | out] [wred-profile name]] [packets_per_second in]` command.

Parameters

- **percentage decimal_value in | out**
  - **E-Series Only**: Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%.
  - Percentage: 0 to 100
  - 0% blocks all related traffic
  - 100% allows all traffic into the interface
  - Decimal Range: 0.1 to 0.9

- **wred-profile name**
  - **E-Series Only**: (Optionally) Enter the keyword `wred-profile` followed by the profile name to designate a wred-profile.

- **packets_per_second in**
  - **C-Series and S-Series Only**: Enter the packets per second of broadcast traffic allowed into the network.
  - Range: 0 to 33554431

Defaults

No default behavior or values

Command Modes

`CONFIGURATION (conf)`

Command History

- **Version 7.6.1.0**: Introduced on S-Series
- **Version 7.5.1.0**: Introduced on C-Series
- **Version 7.4.1.0**: E-Series Only: Added percentage decimal value option
- **Version 6.5.1.0**: Introduced on E-Series

Usage Information

Broadcast storm control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

storm-control broadcast (Interface)

Configure the percentage of broadcast traffic allowed on an interface (ingress only).

Syntax

```
storm-control broadcast [percentage decimal_value in] [wred-profile name]
[packets_per_second in]
```

To disable broadcast storm control on the interface, use the `no storm-control broadcast [percentage decimal_value in] [wred-profile name]] [packets_per_second in]` command.
Storm Control

### storm-control multicast (Configuration)

Configure the packets per second (pps) of multicast traffic allowed in to the C-Series and S-Series networks only.

**Syntax**

`storm-control multicast packets_per_second in`

To disable storm-control for multicast traffic into the network, use the `no storm-control multicast packets_per_second in` command.

**Parameters**

- **packets_per_second in**

  - **C-Series and S-Series Only**: Enter the packets per second of multicast traffic allowed into the network followed by the keyword `in`. Range: 0 to 33554431

**Defaults**

No default behavior or values

**Command Modes**

- `CONFIGURATION (conf)`

**Command History**

- **Version 7.6.1.0** Introduced on C-Series and S-Series only

**Usage Information**

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 percentage of multicast traffic allowed on an C-Series or S-Series interface (ingress only) network only.

Syntax

```
storm-control multicast packets_per_second in
```

To disable multicast storm control on the interface, use the `no storm-control multicast packets_per_second in` command.

Parameters

- `packets_per_second in` C-Series and S-Series Only: Enter the packets per second of broadcast traffic allowed into the network.
  - Range: 0 to 33554431

Defaults

No default behavior or values

Command Modes

```
INTERFACE (conf-if-interface-slot/port)
```

Command History

- **Version 7.6.1.0** Introduced on C-Series and S-Series

storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed in or out of the network.

Syntax

```
storm-control unknown-unicast [percentage decimal_value [in | out]] [wred-profile name] [packets_per_second in]
```

To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast [percentage decimal_value [in | out]] [wred-profile name] [packets_per_second in]` command.

Parameters

- `percentage decimal_value [in | out]` E-Series Only: Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%.
  - Percentage: 0 to 100
  - 0 % blocks all related traffic
  - 100% allows all traffic into the interface
  - Decimal Range: 0.1 to 0.9

- `wred-profile name` E-Series Only: (Optionally) Enter the keyword `wred-profile` followed by the profile name to designate a wred-profile.

- `packets_per_second in` C-Series and S-Series Only: Enter the packets per second of broadcast traffic allowed into the network.
  - Range: 0 to 33554431

Defaults

No default behavior or values

Command Modes

```
CONFIGURATION
```

Command History

- **Version 7.6.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
Usage Information

Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

storm-control unknown-unicast (Interface)

Configure percentage of unknown-unicast traffic allowed on an interface (ingress only).

Syntax

```
storm-control unknown-unicast [percentage decimal_value in] | [wred-profile name]
[packets_per_second in]
```

To disable unknown-unicast storm control on the interface, use the no storm-control unknown-unicast [percentage decimal_value in] | [wred-profile name] [packets_per_second in] command.

Parameters

- `percentage decimal_value in` E-Series Only: Enter the percentage of broadcast traffic allowed into the network. Optionally, you can designate a decimal value percentage, for example, 55.5%.
  - Percentage: 0 to 100
  - 0% blocks all related traffic
  - 100% allows all traffic into the interface
  - Decimal Range: 0.1 to 0.9

- `wred-profile name` E-Series Only: (Optionally) Enter the keyword `wred-profile` followed by the profile name to designate a wred-profile.

- `packets_per_second in` C-Series and S-Series Only: Enter the packets per second of broadcast traffic allowed into the network.
  - Range: 0 to 33554431

Defaults

No default behavior or values

Command Modes

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

Command History

```
| Version 7.6.1.0 | Introduced on S-Series |
| Version 7.5.1.0 | Introduced on C-Series |
| Version 7.4.1.0 | E-Series Only: Added percentage decimal value option |
| Version 6.5.1.0 | Introduced on E-Series |
```
Spanning Tree Protocol (STP)

Overview

The commands in this chapter configure and monitor the IEEE 802.1d Spanning Tree protocol (STP) and are supported on all three Dell Networking switch/routing platforms, as indicated by the C, E, and S characters under the command headings:

Commands

- bpdu-destination-mac-address
- bridge-priority
- debug spanning-tree
- description
- disable
- forward-delay
- hello-time
- max-age
- protocol spanning-tree
- show config
- show spanning-tree 0
- spanning-tree 0
bpdu-destination-mac-address

Use the Provider Bridge Group address in Spanning Tree or GVRP PDUs.

Syntax

bpdu-destination-mac-address [stp | gvrp] provider-bridge-group

Parameters

- **stp**: Force STP, RSTP, and MSTP to use the Provider Bridge Group address as the destination MAC address in its BPDUs.
- **gvrp**: Forces GVRP to use the Provider Bridge GVRP Address as the destination MAC address in its PDUs.

Defaults

The destination MAC address for BPDUs is the Bridge Group Address.

Command Modes

CONFIGURATION

Command History

Version 8.2.1.0 Introduced on C-Series and S-Series.

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, enter **no bridge-priority**.

Parameters

- **priority-value**: Enter a number as the bridge priority value.
  Range: 0 to 65535.
  Default: 32768.

  - **primary**: Enter the keyword **primary** to designate the bridge as the root bridge.

  - **secondary**: Enter the keyword **secondary** to designate the bridge as a secondary root bridge.

Defaults

**priority-value** = 32768

Command Modes

SPANNING TREE (The prompt is “config-stp”).

Command History

- Version 7.7.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

debug spanning-tree

Enable debugging of Spanning Tree Protocol and view information on the protocol.

Syntax

ddebug spanning-tree [stp-id [all | bpdru interface | config | events | exceptions | general | root] | protocol]

To disable debugging, enter **no debug spanning-tree**.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>stp-id</strong></td>
<td>Enter zero (0). The switch supports one Spanning Tree group with a group ID of 0.</td>
</tr>
<tr>
<td><strong>protocol</strong></td>
<td>Enter the keyword for the type of STP to debug, either <strong>mstp</strong>, <strong>pvst</strong>, or <strong>rstp</strong>.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>all</strong> to debug all spanning tree operations.</td>
</tr>
<tr>
<td><strong>bpdu</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>bpdu</strong> to debug Bridge Protocol Data Units.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>(OPTIONAL) Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For the Management interface, enter the keyword <strong>ManagementEthernet</strong> followed by the slot/port information. The slot range is 0 and the port range is 0-1.</td>
</tr>
<tr>
<td></td>
<td>• For a Port Channel interface, enter the keyword <strong>port-channel</strong> followed by a number:</td>
</tr>
<tr>
<td></td>
<td>C-Series and S-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</td>
</tr>
<tr>
<td></td>
<td>• For a SONET interface, enter the keyword <strong>sonet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <strong>TenGigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <strong>fortyGigE</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For VLAN, enter the keyword <strong>vlan</strong> followed by a number from 1 to 4094.</td>
</tr>
<tr>
<td><strong>config</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>config</strong> to debug configuration information.</td>
</tr>
<tr>
<td><strong>events</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>events</strong> to debug STP events.</td>
</tr>
<tr>
<td><strong>general</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>general</strong> to debug general STP operations.</td>
</tr>
<tr>
<td><strong>root</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>root</strong> to debug STP root transactions.</td>
</tr>
</tbody>
</table>

### Command Modes

**EXEC Privilege**

### Command History

- **Version 8.4.6.0** Added support for the keyword **fortyGigE**.
- **Version 7.7.1.0** Introduced on S-Series
- **Version 7.5.1.0** Introduced on C-Series
- **pre-Version 6.2.1.1** Introduced on E-Series

### 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

- **protocol spanning-tree** Enter SPANNING TREE mode on the switch.

---

### description

Enter a description of the Spanning Tree

**Syntax**

```
description {description}
```

To remove the description from the Spanning Tree, use the **no description {description}** command.
### disable

**Syntax**

```plaintext
disable
```

Disable Spanning Tree Protocol globally on the switch.

**Parameters**

- **Defaults**
  - No default behavior or values

- **Command Modes**
  - SPANNING TREE

**Command History**

- **Version 7.7.1.0**
  - Introduced on S-Series

- **Version 7.5.1.0**
  - Introduced on C-Series

- **pre-Version 6.2.1.1**
  - Introduced on E-Series

**Related Commands**

- protocol spanning-tree

### forward-delay

The amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

**Syntax**

```plaintext
forward-delay seconds
```

To return to the default setting, enter `no forward-delay`.

**Parameters**

- **seconds**
  - Enter the number of seconds the FTOS waits before transitioning STP to the forwarding state.
  - Range: 4 to 30
  - Default: 15 seconds.

**Defaults**

- 15 seconds

**Command Modes**

- SPANNING TREE
### hello-time

Set the time interval between generation of Spanning Tree Bridge Protocol Data Units (BPDUs).

**Syntax**

```
hello-time seconds
```

To return to the default value, enter `no hello-time`.

**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**

- SPANNING TREE

### 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, enter `no max-age`.

**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
### protocol spanning-tree

Enter the SPANNING TREE mode to enable and configure the Spanning Tree group.

**Syntax**

```
protocol spanning-tree stp-id
```

To disable the Spanning Tree group, enter `no protocol spanning-tree stp-id` command.

**Parameters**

- **stp-id**: Enter zero (0). FTOS supports one Spanning Tree group, group 0.

**Defaults**

Not configured.

**Command Modes**

- **CONFIGURATION**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
<td></td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

**Figure 58-1. protocol spanning-tree Command Example**

```
FTOS(conf)#protocol spanning-tree 0
FTOS(config-stp)#
```

**Usage Information**

STP is not enabled when you enter the SPANNING TREE mode. To enable STP globally on the switch, enter `no disable` from the SPANNING TREE mode.

**Related Commands**

- **disable**: Disable Spanning Tree group 0. To enable Spanning Tree group 0, enter `no disable`.

### show config

Display the current configuration for the mode. Only non-default values are displayed.

**Syntax**

```
show config
```

**Command Modes**

- **SPANNING TREE**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>Introduced on S-Series</td>
<td></td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
<td></td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
<td></td>
</tr>
</tbody>
</table>
Example Figure 58-2. show config Command for the SPANNING TREE Mode

   FTOS(config-stp)#show config
   protocol spanning-tree 0
   no disable
   FTOS(config-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` (OPTIONAL) 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 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a SONET interface, enter the keyword `sonet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - C-Series and S-Series Range: 1-128
    - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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 8.4.6.0 Added support for the keyword `fortyGigE`.
- Version 8.5.1.0 Support for the optional `guard` keyword was added on the E-Series ExaScale.
- Version 8.4.2.1 Support for the optional `guard` keyword was added on the C-Series, S-Series, and E-Series TeraScale.
- Version 7.7.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series
Example

Figure 58-3.  show spanning-tree 0 Command Example

FTOS#show spann 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
  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 GigabitEthernet 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 (GigabitEthernet 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
  Number of transitions to forwarding state 1
  BPDU: sent:18, received 0
  The port is not in the portfast mode

Port 27 (GigabitEthernet 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
  Number of transitions to forwarding state 1
  BPDU: sent:18, received 0
  The port is not in the portfast mode

Port 28 (GigabitEthernet 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
  Number of transitions to forwarding state 1
  BPDU: sent:31, received 0
  The port is not in the portfast mode

FTOS#

Table 58-1.  show spanning-tree 0 Command Information

<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>“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 58-1. show spanning-tree 0 Command Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Times”</td>
<td>List the number of seconds since the last:</td>
</tr>
<tr>
<td></td>
<td>• hello time</td>
</tr>
<tr>
<td></td>
<td>• topology change</td>
</tr>
<tr>
<td></td>
<td>• notification</td>
</tr>
<tr>
<td></td>
<td>• aging</td>
</tr>
<tr>
<td>“Port 1...”</td>
<td>Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).</td>
</tr>
<tr>
<td>“Port path...”</td>
<td>Displays the path cost, priority, and identifier for the interface.</td>
</tr>
<tr>
<td>“Designated root...”</td>
<td>Displays the priority and MAC address of the root bridge of the STG that the interface belongs.</td>
</tr>
<tr>
<td>“Designated port...”</td>
<td>Displays the designated port ID</td>
</tr>
</tbody>
</table>

Figure 58-4. 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
Interface          Designated
  Name          PortID Prio Cost Sts Cost   Bridge ID             PortID
----------------- ------ ---- ---- --- -----    -----------------     -----
  Gi 1/1          8.26     8    4 FWD     0    32768 0001.e800.0a56  8.26
  Gi 1/2          8.27     8    4 FWD     0    32768 0001.e800.0a56  8.27
  Gi 1/3          8.28     8    4 FWD     0    32768 0001.e800.0a56  8.28
FTOS#
```

Figure 58-5. show spanning-tree 0 guard Command Example

```
FTOS#show spanning-tree 0 guard
Interface
  Name     Instance  Sts     Guard type
  --------- -------- -------- ------------
  Gi 0/1    0        INCON(Root) Rootguard
  Gi 0/2    0        LIS      Loopguard
  Gi 0/3    0        EDS (Shut) Bpduguard
```

Table 58-2. show spanning-tree 0 guard Command Example Information

<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>
<tr>
<td>Guard Type</td>
<td>Type of STP guard configured (Root, Loop, or BPDU guard)</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 | {loopguard | rootguard} | portfast [bpdu-guard | shutdown-on-violation]] | priority priority}
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>stp-id</strong></td>
<td>Enter the keyword <code>stp-id</code> followed by the STP instance ID. Range: 0</td>
</tr>
</tbody>
</table>
| **cost cost** | Enter the keyword `cost` followed by a number as the cost. Range: 1 to 65535  
Defaults:  
- 100 Mb/s Ethernet interface = 19  
- 1-Gigabit Ethernet interface = 4  
- 10-Gigabit Ethernet interface = 2  
- 40-Gigabit interface = 1  
- Port Channel interface with 100 Mb/s Ethernet = 18  
- Port Channel interface with 1-Gigabit Ethernet = 3  
- Port Channel interface with 10-Gigabit Ethernet = 1  
- Port Channel interface with 40-Gigabit Ethernet = 1 |
| **loopguard** | Enter the keyword `loopguard` to enable STP loop guard on a port or port-channel interface. |
| **rootguard** | Enter the keyword `rootguard` to enable STP root guard on a port or port-channel interface. |
| **portfast** | Enter the keyword `portfast` to enable Portfast to move the interface into forwarding mode immediately after the root fails.  
Enter the optional keyword `bpdu-guard` 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. |
| **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 8.5.1.0**  
  Introduced the `loopguard` and `rootguard` options on the E-Series ExaScale.

- **Version 8.4.2.1**  
  Introduced the `loopguard` and `rootguard` options on the E-Series TeraScale, C-Series, and S-Series.

- **Version 8.2.1.0**  
  Introduced `shutdown-on-violation` option.

- **Version 7.7.1.0**  
  Introduced on S-Series.

- **Version 7.5.1.0**  
 Introduced on C-Series.

- **Version 6.2.1.1**  
  Introduced.
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 **shutdown-on-violation** is not enabled, BPDUs will still be sent to the RPM CPU.

STP loop guard and root guard are 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.

STP 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.

Do not enable Portfast BPDU guard and loop guard at the same time on a port. Enabling both features may result 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.

To display the type of STP guard (Portfast BPDU, root, or loop guard) enabled on a port, enter the **show spanning-tree 0** command.
Time and Network Time Protocol (NTP)

Overview

The commands in this chapter configure time values on the system, either using Dell Networking OS, or 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 details, see the “Network Time Protocol” section of the Management chapter in the Dell Networking OS Configuration Guide.

The commands in this chapter are generally supported on the C-Series, E-Series, and S-Series, with some exceptions, as noted in the Command History fields and by these symbols under the command headings: C E S

Commands

• calendar set
• clock read-calendar
• clock set
• clock summer-time date
• clock summer-time recurring
• clock timezone
• clock update-calendar
• debug ntp
• ntp authenticate
• ntp authentication-key
• ntp broadcast client
• ntp disable
• ntp multicast client
• ntp server
• ntp source
• ntp trusted-key
• ntp update-calendar
• show calendar
• show clock
• show ntp associations
• show ntp status
calendar set

Set the time and date for the switch hardware clock.

**Syntax**
calendar set time month day year

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, for example, 17:15:00 is 5:15 pm.</td>
</tr>
<tr>
<td>month</td>
<td>Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.</td>
</tr>
<tr>
<td>day</td>
<td>Enter the number of the day. Range: 1 to 31. You can enter the name of a month to change the order of the display to time day month year.</td>
</tr>
<tr>
<td>year</td>
<td>Enter a four-digit number as the year. Range: 1993 to 2035.</td>
</tr>
</tbody>
</table>

**Command Modes**
EXEC Privilege

**Command History**
<table>
<thead>
<tr>
<th>Version</th>
<th>Feature/Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

**Figure 59-1. calendar set Command Example**

```
FTOS#calendar set 08:55:00 june 18 2006
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 Set the software clock based on the hardware clock.
clock set Set the software clock.
clock update-calendar Set the hardware clock based on the software clock.
show clock Display clock settings.

clock read-calendar

Set the software clock on the switch from the information set in hardware clock (calendar).

**Syntax**
clock read-calendar
In the switch, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the FTOS automatically updates the software clock after system bootup.

You cannot delete this command (that is, there is not a “no” version of this command).

**clock set**

Set the software clock in the switch.

**Syntax**

```
clock set time month day year
```

**Parameters**

- **time**
  - Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.

- **month**
  - Enter the name of one of the 12 months, in English.
  - You can enter the number of a day and change the order of the display to `time day month`.

- **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**
  - Enter a four-digit number as the year.
  - Range: 1993 to 2035.

**Defaults**

Not configured

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
Figure 59-2. clock set Command Example

FTOS#clock set 16:20:00 19 may 2001
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 that you use an outside time source, such as NTP, to ensure accurate time on the switch.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp update-calendar</td>
<td>Set the switch using the NTP settings.</td>
</tr>
</tbody>
</table>

### clock summer-time date

**Syntax**

```
clock summer-time time-zone date start-month start-day start-year start-time end-month end-day end-year end-time [offset]
```

**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.
- **start-day**: Enter the number of the day. Range: 1 to 31.
- **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-month**: Enter the name of one of the 12 months in English.
- **end-day**: Enter the number of the day. Range: 1 to 31.
- **end-year**: Enter a four-digit number as the year. Range: 1993 to 2035.
- **end-time**: Enter the time in hours:minutes. For the hour variable, use the 24-hour format, example, 17:15 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
clock summer-time recurring

Set the software clock to convert to daylight savings 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-day end-month end-time [offset]]
```

To delete a daylight savings time zone configuration, enter `no clock summer-time`.

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 savings 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 savings time.
  - `first`: Enter this keyword to start daylight savings time in the first week of the month.
  - `last`: Enter this keyword to start daylight savings time in the last week of the month.

- **start-day**: Enter the name of the day that you want daylight saving time to begin. Use English three letter abbreviations, for example, Sun, Sat, Mon, etc.
  - Range: Sun – Sat

- **start-month**: Enter the name of one of the 12 months in English.

- **start-time**: Enter the time in hours:minutes. For the hour variable, use the 24-hour format, example, 17:15 is 5:15 pm.

- **end-week**: Enter the one of the following as the week that daylight savings ends:
  - `week-number`: enter a number from 1-4 as the number of the week to end daylight savings time.
  - `first`: enter the keyword first to end daylight savings time in the first week of the month.
  - `last`: enter the keyword last to end daylight savings 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.
clock timezone

Configure a timezone for the switch.

Syntax

```
clock timezone timezone-name offset
```

To delete a timezone configuration, enter `no clock timezone`.

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 7.6.1.0**: Support added for S-Series
- **Version 7.5.1.0**: Support added for C-Series
- **Version 7.4.1.0**: Updated the `start-day` and `end-day` options to allow for using the three-letter abbreviation of the weekday name.
- **pre-Version 6.1.1.0**: Introduced for E-Series

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

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 Set the hardware clock.

debug ntp

Display Network Time Protocol (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

- adjust: Enter the keyword adjust to display information on NTP clock adjustments.
- all: Enter the keyword all to display information on all NTP transactions.
- authentication: Enter the keyword authentication to display information on NTP authentication transactions.
- events: Enter the keyword events to display information on NTP events.
- loopfilter: Enter the keyword loopfilter to display information on NTP local clock frequency.
- packets: Enter the keyword packets to display information on NTP packets.
- select: Enter the keyword select to display information on the NTP clock selection.
- sync: Enter the keyword sync to display information on the NTP clock synchronization.

Command Modes

EXEC Privilege

Command History

Version 7.6.1.0 Support added for S-Series
Version 7.5.1.0 Support added for C-Series
pre-Version 6.1.1.0 Introduced for E-Series
ntp authenticate

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

Syntax

```
nntp authenticate
```

To disable NTP authentication, enter `no ntp authenticate`.

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version 7.6.1.0</th>
<th>Support added for S-Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

Usage Information

You also must configure an authentication key for NTP traffic using the `ntp authentication-key` command.

Related Commands

- `ntp authentication-key` Configure authentication key for NTP traffic.
- `ntp trusted-key` Configure a key to authenticate

ntp authentication-key

Specify a key for authenticating the NTP server.

Syntax

```
nntp authentication-key number md5 [0 | 7] key
```

Parameters

- `number` Specify a number for the authentication key.
  - Range: 1 to 4294967295.
  - The 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 8.2.1.0 | Added options `[0 | 7]` for entering authentication key. |
|----------------|--------------------------------------------------------|
| Version 7.6.1.0 | Support added for S-Series |
| Version 7.5.1.0 | Support added for C-Series |
| pre-Version 6.1.1.0 | Introduced for E-Series |
After configuring the `ntp authentication-key` command, configure the `ntp trusted-key` command to complete NTP authentication.

Dell Networking OS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous Dell Networking OS versions; beginning in version 8.2.1.0, Dell Networking OS 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 Dell Networking OS 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ntp authenticate</code></td>
<td>Enables NTP authentication.</td>
</tr>
<tr>
<td><code>ntp trusted-key</code></td>
<td>Configure a trusted key.</td>
</tr>
</tbody>
</table>

### ntp broadcast client

Set up the interface to receive NTP broadcasts from an NTP server.

**Syntax**

```
ntp broadcast client
```

To disable broadcast, enter `no ntp broadcast client`.

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

### ntp disable

Prevent an interface from receiving NTP packets.

**Syntax**

```
ntp disable
```

To re-enable NTP on an interface, enter `no ntp disable`.

**Defaults**

Disabled (that is, if an NTP host is configured, all interfaces receive NTP packets)

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Added/Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
**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 either an IPv4 address in dotted decimal format or an IPv6 address in X::X::X::X format. If you do not enter a multicast address, the address 224.0.1.1 is configured if the interface address is IPv4 or ff05::101 is configured if the interface address is IPv6.

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv6 multicast addresses.</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**ntp server**

Configure an NTP time-serving host.

**Syntax**

```
ntp server [vrf vrf-name] {hostname | ipv4-address | ipv6-address} [key keyid] [prefer] [version number]
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword vrf followed by the name of the VRF. Range: 1 to 63.
- `ipv4-address | ipv6-address` Enter an IPv4 address (A.B.C.D) or IPv6 address (X::X::X::X).
- `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.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added IPv6 support.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
You can configure multiple time serving hosts (up to 250). From these time serving hosts, the FTOS will choose one NTP host with which to synchronize. Use the show ntp associations to determine which server was selected.

Since a large number of polls to NTP hosts can impact network performance, Dell Force10 recommends that you limit the number of hosts configured.

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ntp associations</td>
</tr>
</tbody>
</table>

**ntp source**

Specify an interface’s IP address to be included in the NTP packets.

**Syntax**

```
nntp source interface
```

To delete the configuration, enter `no ntp source`.

**Parameters**

**interface**

Enter the following keywords and slot/port or number information:

- For an 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port 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:
  - **C-Series** and **S-Series** Range: 1-128
  - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale
- For SONET interface types, enter the keyword `sonet` followed by the 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.
- For VLAN interface, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <code>fortyGigE</code>.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter a number as the trusted key ID. Range: 1 to 4294967295.</td>
</tr>
</tbody>
</table>

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**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` Set an authentication key for NTP.
- `ntp authenticate` Enable 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**

```
ntp update-calendar [minutes]
```

To return to default setting, enter `no ntp update-calendar`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>minutes</code></td>
<td>(OPTIONAL) Enter the number of minutes between updates from NTP to the hardware clock. Range: 1 to 1440. Default: 60 minutes.</td>
</tr>
</tbody>
</table>

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>
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 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

Example

```
Figure 59-3.  show calendar Command Example

FTOS#show calendar
16:33:30 UTC Tue Jun 26 2001
FTOS#
```

Related Commands

- `show clock`  Display the time and date from the switch software clock.

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 7.6.1.0 Support added for S-Series
- Version 7.5.1.0 Support added for C-Series
- pre-Version 6.1.1.0 Introduced for E-Series

Example

```
Figure 59-4.  show clock Command Example

FTOS#show clock
11:05:56.949 UTC Thu Oct 25 2001
FTOS#
```
Example

Figure 59-5.  show clock detail Command Example

FTOS#show clock detail
12:18:10.691 UTC Wed Jan 7 2009
Time source is RTC hardware
Summer time starts 02:00:00 UTC Sun Mar 8 2009
Summer time ends 02:00:00 ABC Sun Nov 1 2009
FTOS#

Related

Commands

clock summer-time recurring    Display the time and date from the switch hardware clock.
show calendar                   Display the time and date from the switch hardware clock.

show ntp associations

Display the NTP master and peers.

Syntax

show ntp associations

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.6.1.0  Support added for S-Series
Version 7.5.1.0  Support added for C-Series
pre-Version 6.1.1.0  Introduced for E-Series

Example

Figure 59-6.  show ntp associations Command Example

FTOS#show ntp associations
remote ref clock st when poll reach delay offset disp
-----------------------------------------------
10.10.120.5 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16 377 -0.08 -1499.9 104.16
172.31.1.33 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
192.200.0.2 0.0.0.0 16 - 256 0 0.00 0.000 16000.0
* master (synced), # master (unsynced), + selected, - candidate
FTOS#
show ntp status

Display the current NTP status.

**Syntax**

```
show ntp status
```

**Command Modes**

EXEC

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Support added for C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced for E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS#sh ntp status
Clock is synchronized, stratum 2, reference is 100.10.10.10
frequency is -32.000 ppm, stability is 15.156 ppm, precision is 4294967290
reference time is BC242FD5.C7C5C000 (10:15:49.780 UTC Mon Jan 10 2000)
clock offset is clock offset msec, root delay is 0.01656 sec
root dispersion is 0.39694 sec, peer dispersion is peer dispersion msec
peer mode is client
FTOS#
```
Table 59-2. show ntp status Command Example Information

<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 Hertz)</td>
</tr>
<tr>
<td></td>
<td>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 | Display information on 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 NIC teaming, automatic recovery from a failed link.

Uplink Failure Detection is supported on platform: S (S50 only).

Commands

- 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

S50 only

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}

Parameters

interface interface

- Specifies one or more downstream interfaces.
- For interface, enter one of the following interface types:
  - Fast Ethernet: fastethernet {slot/port | slot/port-range}
  - 1-Gigabit Ethernet: gigabitethernet {slot/port | slot/port-range}
  - 10-Gigabit Ethernet: tengigabitethernet {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:
- gigabitethernet 1/1-2,5,9,11-12
- port-channel 1-3,5
- A comma is required to separate each port and port-range entry.

uplink-state-group group-id

- Re-enables all UFD-disabled downstream interfaces in the group.
- Valid group-id values are 1 to 16.

Defaults

A downstream interface in an uplink-state group that has been disabled by UFD is disabled and in a UFD-disabled error state.

Command Modes

CONFIGURATION

Command History

Version 8.4.2.3 Introduced on the S-Series S50.

Related Commands

downstream

- Assign a port or port-channel to the uplink-state group as a downstream interface.

uplink-state-group

- Create an uplink-state group and enabling the tracking of upstream links.
**debug uplink-state-group**

S50 only

Enable debug messages for events related to a specified uplink-state group or all groups.

**Syntax**

```
display uplink-state-group [group-id]
```  

**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 8.4.2.3 Introduced on the S-Series S50.

**Usage Information**

To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.

**Related Commands**

- `clear ufd-disable` Re-enable downstream interfaces that are in a UFD-disabled error state.

---

**description**

S50 only

Enter a text description of an uplink-state group.

**Syntax**

```
description text
```  

**Parameters**


**Defaults**

None

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

Version 8.4.2.3 Introduced on the S-Series S50.

**Related Commands**

- `uplink-state-group` Create an uplink-state group and enabling the tracking of upstream links.

**Example**

**Figure 60-1. description Command Example**

```
FTOS(conf-uplink-state-group-16)# description test
FTOS(conf-uplink-state-group-16)##
```
downstream

**S** S50 only

Assign a port or port-channel to the uplink-state group as a downstream interface.

**Syntax**

```
downstream interface
```

**Parameters**

<table>
<thead>
<tr>
<th>interface</th>
<th>Enter one of the following interface types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Ethernet: `fastethernet {slot/port</td>
<td>slot/port-range}`</td>
</tr>
<tr>
<td>1-Gigabit Ethernet: `gigabitethernet {slot/port</td>
<td>slot/port-range}`</td>
</tr>
<tr>
<td>10-Gigabit Ethernet: `tengigabitethernet {slot/port</td>
<td>slot/port-range}`</td>
</tr>
<tr>
<td>Port channel: `port-channel {1-512</td>
<td>port-channel-range}`</td>
</tr>
</tbody>
</table>

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:

- `gigabitethernet 1/1-2,5,9,11-12`
- `port-channel 1-3,5`

A comma is required to separate each port and port-range entry.

**Defaults**

None

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on the S-Series S50.</th>
</tr>
</thead>
</table>

**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. Each interface assigned to an uplink-state group must be configured 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.

To delete an uplink-state group, enter the `no downstream interface` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>upstream</code></td>
<td>Assign 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>Create an uplink-state group and enabling the tracking of upstream links.</td>
</tr>
</tbody>
</table>

**downstream auto-recover**

**S** S50 only

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
```

**Defaults**

The auto-recovery of UFD-disabled downstream ports is enabled.

**Command Modes**

UPLINK-STATE-GROUP
To disable auto-recovery on downstream links, enter the `no downstream auto-recover` command.

**Related Commands**

- **downstream** Assign a port or port-channel to the uplink-state group as a downstream interface.

- **uplink-state-group** Create an uplink-state group and enabling the tracking of upstream links.

---

**downstream disable links**

**S50 only**

Configure the number of downstream links in the uplink-state group that will be disabled if one upstream link in an uplink-state group goes down.

**Syntax**

```
downstream disable links {number | all}
```

**Parameters**

- **number** Enter the number of downstream links to be brought down by UFD.
  
  Range: 1 to 1024.

- **all** Brings down all downstream links in the group.

**Defaults**

No downstream links are disabled when an upstream link in an uplink-state group goes down.

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

Version 8.4.2.3 Introduced on the S-Series S50.

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 when one upstream interface in an uplink-state group goes down.

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.

To revert to the default setting, enter the `no downstream disable links` command.

**Related Commands**

- **downstream** Assign a port or port-channel to the uplink-state group as a downstream interface.

- **uplink-state-group** Create an uplink-state group and enabling the tracking of upstream links.
**enable**

S S50 only

Re-enable upstream-link tracking for an uplink-state group after it has been disabled.

**Syntax**

```plaintext
enable
```

**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 8.4.2.3 Introduced on the S-Series S50.

**Usage Information**

To disable upstream-link tracking without deleting the uplink-state group, enter the `no enable` command.

**Related Commands**

- `uplink-state-group`: Create an uplink-state group and enabling the tracking of upstream links.

**show running-config uplink-state-group**

S S50 only

Display the current configuration of one or more uplink-state groups.

**Syntax**

```plaintext
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

**Command History**

Version 8.4.2.3 Introduced on the S-Series S50.

**Example**

**Figure 60-2. show running-config uplink-state-group Command Example**

```
FTOS#show running-config uplink-state-group
!
no enable
uplink state track 1
downstream GigabitEthernet 0/2,4,6,11-19
upstream TengigabitEthernet 0/48, 52
upstream PortChannel 1
!
uplink state track 2
downstream GigabitEthernet 0/1,3,5,7-10
upstream TengigabitEthernet 0/56,60
```
show uplink-state-group

S50 only
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 8.4.2.3: Introduced on the S-Series S50.
Example

Figure 60-3.  show uplink-state-group Command Examples

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 : Gi 0/46(Up) Gi 0/47(Up)
Downstream Interfaces : Te 13/0(Up) Te 13/1(Up) Te 13/5(Up) Te 13/6(Up)

Uplink State Group : 5 Status: Enabled, Down
Upstream Interfaces : Gi 0/0(Dwn) Gi 0/3(Dwn) Gi 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 : Gi 0/41(Dwn) Po 8(Dwn)
Downstream Interfaces : Gi 0/40(Dwn)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Display the current configuration of one or more uplink-state groups.</td>
</tr>
<tr>
<td>uplink-state-group</td>
<td>Create an uplink-state group and enabling the tracking of upstream links.</td>
</tr>
</tbody>
</table>
Create an uplink-state group and enabling the tracking of upstream links on a switch/router.

Syntax

```
uplink-state-group group-id
```

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

Command History

- Version 8.4.2.3 Introduced on the S-Series S50.

Usage Information

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.

To delete an uplink-state group, enter the **no uplink-state-group group-id** command.

To disable upstream-link tracking without deleting the uplink-state group, enter the **no enable** command in uplink-state-group configuration mode.

Related Commands

- **show running-config**
  - Display the current configuration of one or more uplink-state groups.

- **show uplink-state-group**
  - Display status information on a specified uplink-state group or all groups.

Example

```
FTOS(conf)#uplink-state-group 16
FTOS(conf)#
02:23:17: %RPM0-P:CP %IFMGR-5-ASTATE_UP: Changed uplink state group Admin state to up: Group 16
```
upstream

S S50 only

Assign a port or port-channel to the uplink-state group as an upstream interface.

Syntax

upstream interface

Parameters

- **interface**
  - Enter one of the following interface types:
    - Fast Ethernet: `fastethernet {slot/port | slot/port-range}`
    - 1-Gigabit Ethernet: `gigabitethernet {slot/port | slot/port-range}`
    - 10-Gigabit Ethernet: `tengigabitethernet {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:
    - `gigabitethernet 1/1-2,5,11-12`
    - `port-channel 1-3,5`
  - A comma is required to separate each port and port-range entry.

 Defaults

None

Command Modes

UPLINK-STATE-GROUP

Command History

- **Version 8.4.2.3**
  - Introduced on the S-Series S50.

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. Each interface assigned to an uplink-state group must be configured 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.

To delete an uplink-state group, enter the no upstream interface command.

Related Commands

- **downstream**
  - Assign a port or port-channel to the uplink-state group as a downstream interface.

- **uplink-state-group**
  - Create an uplink-state group and enabling the tracking of upstream links.

Example

**Figure 60-5. upstream Command Example**

```
FTOS(conf-uplink-state-group-16)# upstream gigabitethernet 1/10-15
FTOS(conf-uplink-state-group-16)#
```
VLAN Stacking

Overview

With the VLAN-Stacking feature (also called Stackable VLANs and QinQ), available on all Dell Networking platforms (C-Series, E-Series, and S-Series) that are supported by this version of Dell Networking OS, you can “stack” VLANs into one tunnel and switch them through the network transparently.

VLAN Stacking is supported on E-Series ExaScale with Dell Networking OS 8.2.1.0 and later.

Commands

The commands included 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 on basic VLAN commands, see Virtual LAN (VLAN) Commands in the chapter Layer 2.

Important Points to Remember

- If Spanning Tree Protocol (STP) is not enabled across the Stackable VLAN network, STP 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 protocol tunneling is enabled.

Note: For details on protocol tunneling on the E-Series, see Chapter 52, Service Provider Bridging.
- 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 SNMP management over a Stackable VLAN enabled VLAN containing only Stackable VLAN trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
- It is recommended that you do not use the same MAC address, on different customer VLANs, on the same Stackable VLAN.
- Interfaces configured using Stackable VLAN access or Stackable VLAN trunk commands will not switch traffic for the default VLAN. These interfaces will switch traffic only when they are added to a non-default VLAN.
- Starting with Dell Networking OS 7.8.1 for C-Series and S-Series (Dell Networking OS 7.7.1 for E-Series, 8.2.1.0 for E-Series ExaScale), 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. See portmode hybrid.

**dei enable**

Make packets eligible for dropping based on their DEI value.

**Syntax**

```
dei enable
```

**Defaults**

Packets are colored green; no packets are dropped.

**Command Mode**

CONFIGURATION

**Command History**

Version 8.3.1.0 Introduced on C-Series and S-Series.

**dei honor**

Honor the incoming DEI value by mapping it to an Dell Networking OS drop precedence. You may enter the command once for 0 and once for 1.

**Syntax**

```
dei honor {0 | 1} {green | red | yellow}
```

**Parameters**

- `0 | 1`: Enter the bit value you want to map to a color.
- `green | red | yellow`: 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**

Version 8.3.1.0 Introduced on C-Series and S-Series.
### vlan-stacking

You must first enable DEI for this configuration to take effect.

### dei mark

Set the DEI value on egress according to the color currently assigned to the packet.

**Syntax**

```
dei mark {green | yellow} {0 | 1}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>green</td>
<td>yellow</td>
</tr>
<tr>
<td>• Green</td>
<td>High priority packets that are the least preferred to be dropped.</td>
</tr>
<tr>
<td>• Yellow</td>
<td>Lower priority packets that are treated as best-effort.</td>
</tr>
</tbody>
</table>

**Defaults**

All the packets on egress will be marked with DEI 0.

**Command Mode**

INTERFACE

**Command History**

Version 8.3.1.0 Introduced on C-Series and S-Series.

**Usage Information**

You must first enable DEI for this configuration to take effect.

### 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**

- **interface**
  
  Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **C-Series and S-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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 Mode

**CONF-IF-VLAN**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for C-Series and S-Series</td>
</tr>
</tbody>
</table>

### Usage Information

You must enable the Stackable VLAN (using the `vlan-stack compatible` command) on the VLAN prior to adding a member to the VLAN.

### Related Commands

- `vlan-stack compatible` - Enable Stackable VLAN on a VLAN.

### show interface dei-honor

**Display the **dei honor** configuration.**

**Syntax**

```plaintext
show interface dei-honor [interface slot/port | linecard number port-set number]
```

**Parameters**

- `interface slot/port` - Enter the interface type followed by the line card slot and port number. Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - **C-Series** Range: 1-128
    - **E-Series** Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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 the VLAN ID. The VLAN ID range is from 1 to 4094.

- `linecard number port-set number` - Enter **linecard** followed by the line card slot number, then enter **port-set** followed by the port-pipe number.

**Command Mode**

**EXEC Privilege**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword <strong>fortyGigE</strong>.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on C-Series and S-Series.</td>
</tr>
</tbody>
</table>

### Example

```
FTOS#show interface dei-honor

Default Drop precedence: Green
Interface                CFI/DEI | Drop precedence
------------------------|--------|----------------
G1 0/1                  | 0      | Green          
G1 0/1                  | 1      | Yellow         
G1 8/9                  | 1      | Red            
G1 8/40                 | 0      | Yellow         
```
show interface dei-mark

Display the dei mark configuration.

Syntax

```
show interface dei-mark [interface slot/port | linecard number port-set number]
```

Parameters

- **interface slot/port**: Enter the interface type followed by the line card slot and port number. Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
  - For a Port Channel interface, enter the keyword **port-channel** followed by a number:
    - **C-Series**: Range: 1-128
    - **E-Series**: Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
  - 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 the VLAN ID. The VLAN ID range is from 1 to 4094.

- **linecard number**: Enter **linecard** followed by the line card slot number, then enter **port-set** followed by the port-pipe number.

Command Mode

EXEC Privilege

Command History

- **Version 8.4.6.0**: Added support for the keyword **fortyGigE**.
- **Version 8.3.1.0**: Introduced on C-Series and S-Series.

Example

```
FTOS#show interface dei-mark

Default CFI/DEI Marking: 0

Interface           Drop precedence CFI/DEI
------------------------------------------
Gi 0/1               Green               0
Gi 0/1               Yellow              1
Gi 8/9               Yellow              0
Gi 8/40              Yellow              0
```

Related Commands

- dei honor

**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, enter **no vlan-stack access**.
Defaults
Not configured.

Command Modes
INTERFACE

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for C-Series and S-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

Usage Information
Prior to enabling this command, you must enter the switchport command to place the interface in Layer 2 mode.

To remove the access port designation, the port must be removed (using 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, enter no vlan-stack compatible.

Defaults
Not configured.

Command Modes
CONF-IF-VLAN

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for C-Series and S-Series</td>
</tr>
</tbody>
</table>

E-Series original Command

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 the EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.

Figure 61-1.  show vlan Command Example with Stackable VLANs

FTOS#show vlan
Codes: * - Default VLAN, G - GVRP VLANs

<table>
<thead>
<tr>
<th>NUM</th>
<th>Status</th>
<th>Q Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Inactive</td>
<td>M Gi 13/13</td>
</tr>
<tr>
<td>2</td>
<td>Active</td>
<td>M Gi 13/0-2</td>
</tr>
<tr>
<td>3</td>
<td>Active</td>
<td>M Po1(Gi 13/14-15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M Gi 13/18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M Gi 13/3</td>
</tr>
<tr>
<td>4</td>
<td>Active</td>
<td>M Po1(Gi 13/14-15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M Gi 13/18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M Gi 13/4</td>
</tr>
<tr>
<td>5</td>
<td>Active</td>
<td>M Po1(Gi 13/14-15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M Gi 13/18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M Gi 13/5</td>
</tr>
</tbody>
</table>

FTOS#
**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: 0-7

- **sp-tag-dot1p value**
  - Enter the keyword followed by the service provider dot1p value.
  - Range: 0-7

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

Version 8.3.1.0 Introduced on C-Series and S-Series.

---

**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, Dell Networking OS assigns the value 0x9100.

**Syntax**

```
vlan-stack protocol-type number
```

**Parameters**

- **number**
  - Enter the hexadecimal number as the Stackable VLAN tag.
  - On the E-Series: Dell Networking OS accepts the Most Significant Byte (MSB) and then appends zeros for the Least Significant Byte (LSB).
  - On the C-Series and S-Series: You may specify both bytes of the 2-byte S-Tag TPID.
  - E-Series Range: 0-FF
  - C-Series and S-Series Range: 0-FFFF
  - Default: 9100

**Defaults**

0x9100

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.0</td>
<td>Introduced on E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on E-Series ExaScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for C-Series and S-Series</td>
</tr>
<tr>
<td></td>
<td>E-Series original Command</td>
</tr>
</tbody>
</table>

---
Usage Information

See the Dell Networking OS Configuration Guide for specific interoperability limitations regarding the S-Tag TPID.

On E-Series TeraScale, the two characters you enter in the CLI for `number` become the MSB, as shown in Table 61-1.

<table>
<thead>
<tr>
<th>number</th>
<th>Resulting TPID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x0100</td>
</tr>
<tr>
<td>10</td>
<td>0x1000</td>
</tr>
<tr>
<td>More than two characters.</td>
<td>Configuration rejected.</td>
</tr>
</tbody>
</table>

On E-Series ExaScale, C-Series, and S-Series, four characters you enter in the CLI for `number` are interpreted as follows:

<table>
<thead>
<tr>
<th>number</th>
<th>Resulting TPID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x0001</td>
</tr>
<tr>
<td>10</td>
<td>0x0010</td>
</tr>
<tr>
<td>81</td>
<td>0x0081</td>
</tr>
<tr>
<td>8100</td>
<td>0x8100</td>
</tr>
</tbody>
</table>

Related Commands

`portmode hybrid` Set a port (physical ports only) to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.

`vlan-stack trunk` Specify a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

**Vlan-stack trunk**

Specify a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

**Syntax**

`vlan-stack trunk`

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series ExaScale</td>
<td></td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Functionality augmented for C-Series and S-Series to enable multi-purpose use of the port. See Usage Information, below.</td>
<td></td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Functionality augmented for E-Series to enable multi-purpose use of the port. See Usage Information, below.</td>
<td></td>
</tr>
</tbody>
</table>
Prior to using this command, you must execute the `switchport` command to place the interface in Layer 2 mode.

To remove the trunk port designation, the port must first be removed (using the `no member interface` command) from all Stackable VLAN-enabled VLANs.

Starting with Dell Networking OS 7.7.1.0 for E-Series, the VLAN-Stack trunk port can transparently tunnel, in a service provider environment, customer-originated xSTP control protocol PDUs. See Chapter 52, Service Provider Bridging.

Starting with Dell Networking OS 7.8.1.0 for C-Series and S-Series (Dell Networking OS 7.7.1 for E-Series), 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. See `portmode hybrid`.

In Example 1 below, a VLAN-Stack trunk port is configured and then also made part of a single-tagged VLAN.

In Example 2 below, the Tag Protocol Identifier (TPID) is set to 8848. The “Gi 3/10” port is configured to act as a VLAN-Stack access port, while the “TenGi 8/0” port will act 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 executing the `portmode hybrid` command. See `portmode hybrid` in Interfaces.)
Example 1  Figure 61-2. Adding a Stackable VLAN Trunk Port to a Tagged VLAN

```conf
FTOS(conf-if-gi-0/42)#switchport
FTOS(conf-if-gi-0/42)#vlan-stack trunk
FTOS(conf-if-gi-0/42)#show config
!
interface GigabitEthernet 0/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
FTOS(conf-if-gi-0/42)#interface vlan 100
FTOS(conf-if-vl-100)#vlan-stack compatible
FTOS(conf-if-vl-100-stack)#member gigabitethernet 0/42
FTOS(conf-if-vl-100-stack)#show config
!
interface Vlan 100
  no ip address
  vlan-stack compatible
  member GigabitEthernet 0/42
  shutdown
FTOS(conf-if-vl-100-stack)#interface vlan 20
FTOS(conf-if-vl-20)#tagged gigabitethernet 0/42
FTOS(conf-if-vl-20)#show config
!
interface Vlan 20
  no ip address
  tagged GigabitEthernet 0/42
  shutdown
FTOS(conf-if-vl-20-stack)#do show vlan
```

<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>T Gi 0/42</td>
</tr>
<tr>
<td>20</td>
<td>Active</td>
<td></td>
<td>M Gi 0/42</td>
</tr>
<tr>
<td>100</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 2  Figure 61-3. Adding a Stackable VLAN Trunk Port to Tagged and Untagged VLANs

```conf
FTOS(config)#vlan-stack protocol-type 88A8
FTOS(config)#interface gigabitethernet 3/10
FTOS(config-if-gi-3/10)#no shutdown
FTOS(config-if-gi-3/10)#vlan-stack access
FTOS(config-if-gi-3/10)#exit
FTOS(config)#interface tenGigabitethernet 8/0
FTOS(config-if-te-10/0)#no shutdown
FTOS(config-if-te-10/0)#portmode hybrid
FTOS(config-if-te-10/0)#switchport
FTOS(config-if-te-10/0)#vlan-stack trunk
FTOS(config-if-te-10/0)#exit
FTOS(config)#interface vlan 10
FTOS(config-if-vlan)#vlan-stack compatible
FTOS(config-if-vlan)#member Gi 7/0, Gi 3/10, TenGi 8/0
FTOS(config-if-vlan)#exit
FTOS(config)#interface vlan 30
FTOS(config-if-vlan)#untagged TenGi 8/0
FTOS(config-if-vlan)#exit
FTOS(config)#interface vlan 40
FTOS(config-if-vlan)#tagged TenGi 8/0
FTOS(config-if-vlan)#exit
FTOS(config)#
```
Virtual Routing and Forwarding (VRF)

Overview

Virtual Routing and Forwarding (VRF) allows multiple instances of a routing table to co-exist on the same router at the same time.

Virtual Routing and Forwarding (VRF) is supported on the E-Series TeraScale and ExaScale platforms. This is noted in the Command History fields and by the symbol under the command headings: ❯

Commands

- cam-profile (E-Series Exascale only)
- cam-profile ipv4-vrf (E-Series Terascale only)
- cam-profile ipv4-v6-vrf (E-Series Terascale only)
- ip vrf
- ip vrf forwarding
- ip vrf-vlan-block
- show ip vrf
- show run vrf
- start-vlan-id

**cam-profile**

(E-Series Exascale only) Set the VRF CAM size. The default CAM size is 40M which supports both IPv4 and IPv6. You can also configure 10M CAM which supports only IPv4.

**Syntax**

```
cam-profile name [10M-CAM]
```

**Parameters**

- `name`: Enter the name for the VRF CAM profile. Maximum: 16 characters.
- `10M-CAM`: Set the CAM size to 10M.

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series Exascale.</td>
</tr>
</tbody>
</table>
Example

FTOS(conf)#cam-profile test
FTOS(conf-cam-prof-test)#microcode vrf
FTOS(conf-cam-prof-test)#enable
CAM profile 'abc' is currently enabled.
Do you want to disable it and continue? [yes/no]: y
System configuration has been modified. Save? [yes/no]: y
Nov 3 21:57:27: %RPM0-P:CP %FILEMGR-5-FILESAVED: Copied running-config to
Synchronizing data to peer RPM
!!!!!
Proceed with reload [confirm yes/no]: y

Reload the system after setting the CAM Profile.

FTOS# show cam-profile

-- Chassis CAM Profile --
CamSize : 40-Meg
Profile Name : test
Microcode Name : VRF
L2FIB : 15K entries
Learn : 1K entries
L2ACL : 5K entries
System Flow : 102 entries
Qos : 500 entries
Frrp : 102 entries
L2pt : 266 entries
IPv4FIB : 256K entries
IPv4ACL : 16K entries
IPv4Flow : 24K entries
Mcast Fib/Acl : 9K entries
Pbr : 1K entries
Qos : 10K entries
System Flow : 4K entries
EgL2ACL : 2K entries
EgIpv4ACL : 4K entries
Mpls : 60K entries
IPv6FIB : 12K entries
IPv6ACL : 6K entries
IPv6Flow : 6K entries
Mcast Fib/Acl : 3K entries
Pbr : 0K entries
Qos : 1K entries
System Flow : 2K entries
EgIPv6ACL : 1K entries
GenEgACL : 0.5K entries
IPv4FHOP : 4K entries
IPv6FHOP : 4K entries
IPv4/IPv6NHOP : 12K entries

Usage Information

After you set the CAM size on an Exascale platform, you must select and enable VRF microcode, and
load the system to activate the CAM profile (see the example above).

Related Commands

cam-profile ipv4-v6-vrf Set the VRF CAM profile for IPv4 and IPv6 on the
E-Series Terascale.
cam-profile ipv4-vrf

(E-Series Terascale only) Set the VRF CAM profile for IPv4 only.

Syntax

```
cam-profile ipv4-vrf microcode ipv4-vrf
```

Command Modes

CONFIGURATION

Command History

Version 8.2.1.0 Introduced on the E-Series Terascale.

Example

```
FTOS(conf)#cam-profile ipv4-vrf microcode ipv4-vrf
Must reload the system after setting the CAM Profile.
FTOS(conf)#do reload
-- Chassis CAM Profile --

CamSize : 18-Meg
Profile Name : ipv4-vrf   : ipv4-vrf
L2FIB : 32K entries : 32K entries
L2ACL : 3K entries : 3K entries
IPv4FIB : 160K entries : 160K entries
IPv4ACL : 2K entries : 2K entries
IPv4Flow : 12K entries : 12K entries
EqL2ACL : 1K entries : 1K entries
EqIPv4ACL : 12K entries : 12K entries
Reserved : 2K entries : 2K entries
IPv6FIB : 0 entries : 0 entries
IPv6ACL : 0 entries : 0 entries
IPv6Flow : 0 entries : 0 entries
EqIPv6ACL : 0 entries : 0 entries
MicroCode Name : Ipv4-Vrf   : Ipv4-Vrf

-- Line card 1 - per Port Pipe --

CamSize : 18-Meg
Profile Name : ipv4-vrf   : ipv4-vrf
L2FIB : 32K entries : 32K entries
L2ACL : 3K entries : 3K entries
IPv4FIB : 160K entries : 160K entries
IPv4ACL : 2K entries : 2K entries
IPv4Flow : 12K entries : 12K entries
EqL2ACL : 1K entries : 1K entries
EqIPv4ACL : 12K entries : 12K entries
Reserved : 2K entries : 2K entries
IPv6FIB : 0 entries : 0 entries
IPv6ACL : 0 entries : 0 entries
IPv6Flow : 0 entries : 0 entries
EqIPv6ACL : 0 entries : 0 entries
MicroCode Name : Ipv4-Vrf   : Ipv4-Vrf

FTOS(conf)#
```

Usage Information

Reload the system after entering this command to activate the CAM profile.

Do not use this command in EXEC Privilege mode.

Related Commands

```
cam-profile ipv4-v6-vrf
Set the VRF CAM profile for IPv4 and IPv6 on the E-Series Terascale.
```
cam-profile ipv4-v6-vrf

(E-Series Terascale only) Set the VRF CAM profile for IPv4 and IPv6.

Syntax
cam-profile ipv4-v6-vrf microcode ipv4-v6-vrf

Command Modes
CONFIGURATION

Command History
Version 8.2.1.0  Introduced on the E-Series Terascale.

Example
FTOS(conf)#cam-profile ipv4-v6-vrf microcode ipv4-v6-vrf
FTOS(conf)#do reload
FTOS(conf)#do show cam-profile

-- Chassis CAM Profile --

CamSize          : 18-Meg
Profile Name     : ipv4-v6-vrf      : ipv4-v6-vrf
L2FIB            : 32K entries      : 32K entries
L2ACL            : 3K entries       : 3K entries
IPv4FIB          : 64K entries      : 64K entries
IPv4ACL          : 1K entries       : 1K entries
IPv4Flow         : 12K entries      : 12K entries
EqL2ACL          : 1K entries       : 1K entries
EqIPv4ACL        : 11K entries      : 11K entries
Reserved         : 2K entries       : 2K entries
IPv6FIB          : 18K entries      : 18K entries
IPv6ACL          : 4K entries       : 4K entries
IPv6Flow         : 3K entries       : 3K entries
EqIPv6ACL        : 1K entries       : 1K entries
MicroCode Name   : Ipv4-V6-Vrf      : Ipv4-V6-Vrf

-- Line card 1 - per Port Pipe --

CamSize          : 18-Meg
Profile Name     : ipv4-v6-vrf      : ipv4-v6-vrf
L2FIB            : 32K entries      : 32K entries
L2ACL            : 3K entries       : 3K entries
IPv4FIB          : 64K entries      : 64K entries
IPv4ACL          : 1K entries       : 1K entries
IPv4Flow         : 12K entries      : 12K entries
EqL2ACL          : 1K entries       : 1K entries
EqIPv4ACL        : 11K entries      : 11K entries
Reserved         : 2K entries       : 2K entries
IPv6FIB          : 18K entries      : 18K entries
IPv6ACL          : 4K entries       : 4K entries
IPv6Flow         : 3K entries       : 3K entries
EqIPv6ACL        : 1K entries       : 1K entries
MicroCode Name   : Ipv4-V6-Vrf      : Ipv4-V6-Vrf

Usage Information
Reload the systems after entering this command to activate the CAM profile.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cam-profile ipv4-vrf</td>
<td>Set the VRF CAM profile for IPv4 only.</td>
</tr>
</tbody>
</table>
cam-profile ipv4-vrf

(E-Series Exascale only) Set the VRF CAM profile for IPv4 only.

**Syntax**
cam-profile ipv4-vrf microcode ipv4-vrf

**Command Modes**
CONFIGURATION

**Command History**

| Version 8.2.1.0 | Introduced on the E-Series |

**Example**

```
FTOS(conf)# cam-profile ipv4-vrf microcode ipv4-vrf
Must reload the system after setting the CAM Profile.
```

```
FTOS(conf)# do reload
-- Chassis CAM Profile --
CamSize : 18-Meg
<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Current Settings</th>
<th>Next Boot</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-vrf</td>
<td>ipv4-vrf</td>
<td></td>
</tr>
<tr>
<td>L2FIB</td>
<td>32K entries</td>
<td>32K entries</td>
</tr>
<tr>
<td>IPv4FIB</td>
<td>16K entries</td>
<td>16K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>L2ACL</td>
<td>3K entries</td>
<td>3K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>3K entries</td>
<td>3K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
</tbody>
</table>

```

```
FTOS(conf)#

```

-- line card 1 - per Port Pipe --
CamSize : 18-Meg
<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Current Settings</th>
<th>Next Boot</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-vrf</td>
<td>ipv4-vrf</td>
<td></td>
</tr>
<tr>
<td>L2FIB</td>
<td>32K entries</td>
<td>32K entries</td>
</tr>
<tr>
<td>IPv4FIB</td>
<td>16K entries</td>
<td>16K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>L2ACL</td>
<td>3K entries</td>
<td>3K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>3K entries</td>
<td>3K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>IPv4ACL</td>
<td>2K entries</td>
<td>2K entries</td>
</tr>
<tr>
<td>IPv4Flow</td>
<td>12K entries</td>
<td>12K entries</td>
</tr>
<tr>
<td>EqL2ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
<tr>
<td>EqIPv4ACL</td>
<td>1K entries</td>
<td>1K entries</td>
</tr>
</tbody>
</table>

```

```
FTOS(conf)#
```

**Usage Information**
Reload the system after entering this command to activate this CAM profile.

Do not use this command in EXEC Privilege mode.

**Related Commands**
cam-profile ipv4-v6-vrf Set the VRF CAM Profile for IPv4 and IPv6.
Create a non-default VRF instance by specifying the VRF name and ID.

**Note:** Starting in Dell Networking OS 8.4.2.1, when VRF microcode is loaded on an E-Series ExaScale or TeraScale router, the `ip vrf {default-vlan | vrf-name}` command is deprecated, and is replaced by the `ip vrf vrf-name vrf-id` command.

**Syntax**

```
ip vrf vrf-name vrf-id
```

To remove a VRF, enter `no ip vrf vrf-name`.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf-name</td>
<td>Enter the name of the VRF instance. Maximum: 32 characters.</td>
</tr>
<tr>
<td>vrf-id</td>
<td>Enter the VRF ID number. VRF ID range: 1 to 14 and 0 (default VRF)</td>
</tr>
</tbody>
</table>

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>The `ip vrf {default-vlan</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS(conf)#ip vrf East
FTOS(conf-vr-East)#exit
FTOS(conf)#ip vrf default-vrf
FTOS(conf-vr-default-vrf)#
```

**Usage Information**

VRF is enabled by default. The default VRF 0 is automatically configured when a router with VRF loaded in CAM boots up.

Dell Networking OS supports up to 15 VRF instances on an E-Series router: 1 to 14 and the default VRF 0.
ip vrf forwarding

Assign this interface to the VLAN specified.

Syntax

```
ip vrf forwarding vrf-name
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf-name</td>
<td>Enter the name of the VRF instance to which this interface will belong. If no name is entered, default-vrf is assigned.</td>
</tr>
</tbody>
</table>

Command Modes

```
INTERFACE
```

Command History

Version 8.2.1.0 Introduced on the E-Series

Usage Information

There must be no prior Layer 3 configuration on the interface when configuring VRF.

VRF must be enabled prior to implementing this command.

Starting in release 8.4.1.0, you can configure an IP subnet or address on a physical or VLAN interface that overlaps the same IP subnet or address configured on another interface only if the interfaces are assigned to different VRFs. If two interfaces are assigned to the same VRF, you cannot configure overlapping IP subnets or the same IP address on them.

Example

```
FTOS(conf-if-gi-1/1)#int gi 1/10
FTOS(conf-if-gi-1/10)#show config
!
interface GigabitEthernet 1/10
  no ip address
  shutdown
FTOS(conf-if-gi-1/10)#ip vrf ?
FTOS(conf-if-gi-1/10)#ip vrf forwarding East
FTOS(conf-if-gi-1/10)#show config
!
interface GigabitEthernet 1/10
  ip vrf forwarding East
  no ip address
  shutdown
FTOS(conf-if-gi-1/10)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip vrf</td>
<td>Set the name of the VRF instance the VRF, or specify the default-vrf.</td>
</tr>
<tr>
<td>ip vrf-vlan-block</td>
<td>Configure the total number of VLANs that can be configured per VRF.</td>
</tr>
<tr>
<td>start-vlan-id</td>
<td>Set the starting VLAN ID for a VRF instance.</td>
</tr>
</tbody>
</table>
ip vrf-vlan-block

Configure the total number of VLANs that can be configured per VRF.

Note: Starting in Dell Networking OS 8.4.2.1, when VRF microcode is loaded on an E-Series ExaScale or TeraScale router, the **ip vrf-vlan-block number** command is deprecated.

**Syntax**

```
ip vrf-vlan-block number
```

To remove the VLAN block configuration, enter **no vrf-vlan-block**.

**Parameters**

- **number**
  
  Total number of VLANs allotted for VRF instances.
  
  Expressed in power of 2 (2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096)

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.4.2.1</td>
<td>The <strong>ip vrf-vlan-block number</strong> command is deprecated.</td>
</tr>
<tr>
<td>Version 8.2.1.0</td>
<td>Introduced on the E-Series</td>
</tr>
</tbody>
</table>

**Example**

```
FTOS#conf
FTOS(conf)#ip vrf-vlan-block 1024
FTOS(conf)#
```

Enter the number as a power of 2.

**Usage Information**

The total block number of VLANs applies to every configured VRF process. You cannot set different blocks for different VRF processes.

All VLAN member ports must be removed from the VLAN before the VLAN is deleted from a VRF instance.

**Related Commands**

- **start-vlan-id**
  
  Set the starting VLAN ID for a VRF instance.
**show ip vrf**

Display the interfaces assigned to VRF instances.

**Syntax**

```
show ip vrf [vrf-name]
```

**Parameters**

- `vrf-name` Enter the name of a non-default VRF instance. To display information on all VRF instances (including the default VRF 0), do not enter a value.

**Command Modes**

EXEC

**Command History**

- **Version 8.2.1.0** Introduced on the E-Series

**Example**

```
FTOS#show ip vrf
VRF-Name                         VRF-ID Interfaces
default-vrf                      0      So 0/0 So 0/1 So 0/2 So 0/3 Gi 1/0 Gi 1/1
Gi 1/2 Gi 1/3 Gi 1/4 Gi 1/6 Gi 1/7 Gi 1/8 Gi 1/9 Gi 1/11 Gi 1/12 Gi 1/13 Gi 1/14
Gi 1/15 Gi 1/16 Gi 1/17 Gi 1/18 Gi 1/19 Gi 1/20 Gi 1/21 Gi 1/22 Gi 1/23 Gi 1/24 Gi
1/25 Gi 1/26 Gi 1/27 Gi 1/28 Gi 1/29 Gi 1/30 Gi 1/31 Gi 1/32 Gi 1/33 Gi 1/34 Gi 1/35
Gi 1/36 Gi 1/37 Gi 1/38 Gi 1/39 Gi 1/40 Gi 1/41 Gi 1/42 Gi 1/43 Gi 1/44 Gi 1/45
Gi 1/46 Gi 1/47 Ma 0/0 Ma 1/0 Nu 0 Vl 1 Vl 100 Vl 111 Vl 112
East                            1      Gi 1/10
North                            2      Gi 1/5
West                             3
```

**show run vrf**

View information about the current running VRF instances.

**Syntax**

```
show run vrf [vrf-name]
```

**Parameters**

- `vrf-name` Enter the name of the VRF instance you want to view.

**Command Modes**

EXEC

**Command History**

- **Version 8.2.1.0** Introduced on the E-Series

**Example**

```
FTOS#show run vrf
!
ip vrf default-vrf
  start-vlan-id 32
!
ip vrf East
  start-vlan-id 1
!
ip vrf North
!
ip vrf West
  start-vlan-id 96
FTOS#
```
## start-vlan-id

Set the starting VLAN ID for a VRF instance.

**Note:** Starting in Dell Networking OS 8.4.2.1, when VRF microcode is loaded on an E-Series ExaScale or TeraScale router, the `start vlan-id vlan-start-id` command is deprecated.

### Syntax

```
start-vlan-id vlan-start-id
```

### Parameters

- `vlan-start-id` The starting VLAN ID number for this VRF instance.
  - The system takes this number and adds up the number of VLANs assigned in `ip-vrf-vlan-block` to set the start and end range for the VRF VLANs.

### Command Modes

- **CONFIGURATION-VRF**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.2.1</td>
<td>The <code>start vrf-vlan-id vlan-start-id</code> command is deprecated.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series</td>
</tr>
</tbody>
</table>

### Example

```
FTOS(conf)#ip vrf default-vrf
FTOS(conf-vr-default-vrf)#start-vlan-id 32
FTOS(conf-vr-default-vrf)#

FTOS(conf-vr-default-vrf)#ip vrf East
FTOS(conf-vr-East)#start-vlan-id 1
FTOS(conf-vr-East)#ip vrf West

FTOS(conf-vr-West)#start-vlan-id 96
FTOS(conf-vr-West)#
```

### Usage Information

If a given VLAN is not in the range of any VRF, no VRF command can be configured for that VLAN.

All VLAN member ports must be removed from the VLAN before the VLAN is deleted from a VRF instance. This also applies when moving a VLAN from one VRF to another: delete all member ports, then delete the VLAN prior to adding it to another VRF.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip vrf forwarding</code></td>
<td>Assign this interface to the VLAN specified.</td>
</tr>
<tr>
<td><code>ip vrf-vlan-block</code></td>
<td>Configure the total number of VLANs that can be configured per VRF.</td>
</tr>
<tr>
<td><code>show run vrf</code></td>
<td>View information about the current running VRF instances.</td>
</tr>
</tbody>
</table>
Virtual Link Trunking (VLT)

Virtual link trunking (VLT) is supported on the C-Series platform. VLT allows physical links between two chassis to appear as a single virtual link to the network core. VLT eliminates the requirement for Spanning Tree protocols by allowing link aggregation group (LAG) terminations on two separate distribution or core switches, and by supporting a loop-free topology. VLT provides Layer 2 multi-pathing, creating redundancy through increased bandwidth and enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

**Note:** When you launch the VLT link, the VLT peer-ship is not established if any of the following is TRUE:

- The VLT System-MAC configured on both the VLT peers do not match.
- The VLT Unit-Id configured on both the VLT peers are identical.
- The VLT System-MAC or Unit-Id is configured only on one of the VLT peers.
- The VLT domain ID is not the same on both peers.

If the VLT peer-ship is already established, changing the System-MAC or Unit-Id does not cause VLT peer-ship to go down.

Also, if the VLT peer-ship is already established and the VLT Unit-Id or System-MAC are configured on both peers, then changing the CLI configurations on the VLT Unit-Id or System-MAC is rejected if any of the following become TRUE:

- After making the CLI configuration change, the VLT Unit-Id becomes identical on both peers.
- After making the CLI configuration change, the VLT System-MAC do not match on both peers.

When the VLT peer-ship is already established, you can remove the VLT Unit-Id or System-MAC configuration from either or both peers. However, removing configuration settings can cause the VLT ports to go down if you configure the Unit-Id or System-MAC on only one of the VLT peers.

**back-up destination**

Configure the IPv4 address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

**Syntax**

```
back-up destination {ipv4-address [interval seconds]}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>Enter the IPv4 address of the backup destination.</td>
</tr>
<tr>
<td>interval</td>
<td>Enter the keyword <code>interval</code> to specify the time interval to send hello</td>
</tr>
<tr>
<td>seconds</td>
<td>messages. The range is from 1 to 5 seconds. The default is 1 second.</td>
</tr>
</tbody>
</table>
back-up-secondary destination

Configure the secondary IPv4 address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

Syntax

back-up-secondary destination {ipv4-address [interval seconds]}

Parameters

ipv4-address Enter the IPv4 address of the secondary backup destination.
interval seconds Enter the keyword interval to specify the time interval to send hello messages. The range is from 1 to 5 seconds. The default is 1 second.

Defaults

1 Second

Command Modes

VLT DOMAINS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version 8.4.6.0 Introduced on the C-Series.

clear vlt statistics

Clear the statistics on VLT operations.

Syntax

clear vlt statistics [arp | domain | igmp-snoop | mac | multicast | ndp]

Parameters

domain Clear the VLT statistics for the domain.
multicast Display the VLT statistics for multicast.
mac Clear the VLT statistics for the MAC address.
arp Clear the VLT statistics for ARP.
igmp-snoop Clear the VLT statistics for IGMP snooping.
ndp Clear the VLT statistics for NDP.
Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Example

```
VLT ARP Statistics
------------------
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:19
ARP Reg Request rcd:10
```

Related Commands

- `show vlt statistics` Displays statistics on VLT operations.

delay-restore Configure the delay in bringing up VLT ports after reload or peer-link restoration between the VLT peer switches.

**Syntax**

delay-restore

**Parameters**

- `delay-restore` Enter the amount of time, in seconds, to delay bringing up the VLT ports after the VLT device is reloaded or after the peer-link is restored between VLT peer switches. The range from 1 to 1200. The default is 90 seconds.

**Defaults**

Not Configured.

**Command Modes**

VLT DOMAIN

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To delay the system from bringing up the VLT port for a brief period to allow IGMP Snooping and Layer 3 routing protocols to converge, use the delay-restore parameter. Use this feature:

- after a VLT device is reloaded.
- if the Peer VLT device was up at the time the VLTi link failed to the time when it was restored.

**Related Commands**

- `show vlt statistics` Displays statistics on VLT operations.
**lacp ungroup member-independent**

Prevent possible loop during the boot up of a VLT peer switch or a device that accesses the VLT domain.

**Syntax**

```
lacp ungroup member-independent {vlt | port-channel}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port-channel</code></td>
<td>Force all LACP port-channel members to become switchport.</td>
</tr>
<tr>
<td><code>vlt</code></td>
<td>Force all VLT LACP members to become switchports.</td>
</tr>
</tbody>
</table>

**Defaults**

Not Configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

- **Version 8.4.6.0**
  
  Introduced on the C-Series.

**Usage Information**

LACP on the VLT ports (on a VLT switch or access device), which are members of the virtual link trunk, is not brought up until the VLT domain is recognized on the access device.

To ungroup the VLT and port-channel configurations, use the no lacp ungroup member-independent command on a VLT port channel, depending on whether the port channel is VLT or non-VLT.

**Example**

```text
Dell Networking OS (conf)#lacp ungroup member-independent ?
port-channel LACP port-channel members become switchports
vlt All VLT LACP members become switchports
```

**multicast peer-routing timeout**

Configure the time for a VLT node to retain synced multicast routes or synced multicast outgoing interface (OIF) after a VLT peer node failure.

**Syntax**

```
multicast peer-routing timeout value
```

To restore the default value, use the **no multicast peer-routing timeout** command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Enter the timeout value in seconds. The range is from 1 to 1200. The default is 150.</td>
</tr>
</tbody>
</table>

**Command Modes**

VLT DOMAIN (conf-vlt-domain)

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.
The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**peer-link port-channel**

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

**Syntax**

```plaintext
peer-link port-channel port-channel-number {peer-down-vlan vlan id}
```

**Parameters**

- `port-channel-number`: Enter the port-channel number that acts as the interconnect trunk.
- `peer-down-vlan`: Enter the keyword `peer-down-vlan` then a VLAN ID to configure the VLAN that the VLT peer link uses when the VLT peer is down.

**Defaults**

- Not Configured.

**Command Modes**

- VLT DOMAIN

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

- To configure the VLAN from where the VLT peer forwards packets received over the VLTi from an adjacent VLT peer that is down, use the `peer-down-vlan` parameter.

**peer-routing**

Enable L3 VLT peer-routing.

**Syntax**

```plaintext
peer-routing
```

**Defaults**

- Disabled.

**Command Modes**

- VLT DOMAIN (conf-vlt-domain)

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
peer-routing-timeout

Configure the delay after which peer routing is disabled when the peer is unavailable.

**Syntax**

```
peer-routing-timeout value
```

To restore the default value, use the `no peer-routing-timeout` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Enter the timeout value in seconds. The range is from 1 to 65535. The default value is 0 (no timeout).</td>
</tr>
</tbody>
</table>

**Command Modes**

VLT DOMAIN (conf-vlt-domain)

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

When the timer expires, the software checks to see if the VLT peer is now available. If the VLT peer is not available, peer-routing is disabled on that peer.

primary-priority

Assign the priority for master election among VLT peers.

**Syntax**

```
[no] primary-priority
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>To configure the primary role on a VLT peer, enter a lower value than the priority value of the remote peer. The range is from 1 to 65535.</td>
</tr>
</tbody>
</table>

**Default**

32768

**Command Modes**

VLT DOMAIN (conf-vlt-domain)

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

After you configure the VLT domain on each peer switch on both sides of the interconnect trunk, by default, the Dell Networking OS software elects a primary and secondary VLT peer device. To reconfigure the primary role of VLT peer switches, use the `priority` command.
show vlt brief

Displays summarized status information about VLT domains currently configured on the switch.

Syntax

show vlt brief

Defaults

Not Configured.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version 8.4.6.0 Introduced on the C-Series.

Usage Information

The version shown in the show vlt brief output command displays the VLT version number which is different from the Dell Networking OS version number. VLT version numbers are begin with odd numbers such as 3 or 5.

Example (Brief)

Dell Networking OS (conf) #show vlt brief
VLT Domain Brief
-----------------------------
Domain ID: 10
Role: Primary
Role Priority: 32768
ICL Link Status: Up
Heart Beat Status: Not Established
VLT Peer Status: Up
Version: 5 (1)
Local System MAC address: 00:01:e8:8b:14:3c
Remote System MAC address: 00:01:e8:8b:15:20
Remote System Version: 5 (1)
Delay-Restore timer: 90 seconds

show vlt backup-link

Displays information on the backup link operation.

Syntax

show vlt backup-link

Defaults

Not Configured.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version 8.4.6.0 Introduced on the C-Series.
show vlt counters  

Displays the counter information.

Syntax  
show vlt counters [arp | igmp-snoop | interface | mac | ndp]

Parameters  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Enter the keyword arp to display the ARP counter information for the VLT.</td>
</tr>
<tr>
<td>igmp-snoop</td>
<td>Enter the keywords igmp-snoop to display the igmp-snooping counter information for the VLT.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter the keyword interface to display the interface counter information for the VLT.</td>
</tr>
<tr>
<td>mac</td>
<td>Enter the keyword mac to display the MAC address counter information for the VLT.</td>
</tr>
<tr>
<td>ndp</td>
<td>Enter the keyword ndp to display the VLT counter information for NDP.</td>
</tr>
</tbody>
</table>

Defaults  
Not Configured.

Command Modes  
EXEC

Command History  
This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version 8.4.6.0  Introduced on the C-Series.

Usage Information  
If you do not add a parameter such as arp or mac, the output displays all of the counters.

Example  

FTOS_VLTpeer1# show vlt backup-link

VLT Backup Link
-----------------
Destination: 10.11.200.18
Peer HeartBeat status: Up
HeartBeat Timer Interval: 1
HeartBeat Timeout: 3
UDP Port: 34998
HeartBeat Messages Sent: 1026
HeartBeat Messages Received: 1025
Example (igmp-snoop)

FTOS# show vlt counter igmp-snoop
Total IGMP VLT counters
---------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count : 5

Example (igmp-snoop interface port-channel)

FTOS# show vlt counter igmp-snoop interface port-channel 2
VLT Port-ID: 2 IGMP Counter
---------------------
IGMP MRouter Vlans count : 0
IGMP Mcast Groups count : 5

FTOS# show vlt counter igmp-snoop interface port-channel 100
VLT Port-ID: 100 IGMP Counter
---------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count : 0

Example (NDP and Non-VLT ARP)

FTOS# show vlt counters
Total VLT Counters
---------------------
L2 Total MAC-Address Count: 2
Total Arp Entries Learnt : 0
Total Arp Entries Synced : 0
Total Non-VLT Arp entries Learnt: 0
Total Non-VLT Arp Entries Synced 0
IGMP MRouter Vlans count :
IGMP Mcast Groups count :
Total VLT Ndp Entries Learnt : 2
Total VLT Ndp Entries Synced : 0
Total Non-VLT Ndp Entries Learnt : 0
Total Non-VLT Ndp Entries Synced : 0

show vlt detail

Displays detailed status information about VLT domains currently configured on the switch.

Syntax

show vlt detail

Defaults

Not Configured.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version 8.4.6.0 Introduced on the C-Series.

Example

FTOS# FTOS(conf-if-vl-100)# show vlt detail
Local LAG Id Peer LAG Id Local Status Peer Status Active VLANs
---------------------- ---------------------- ----------------------
10 10 UP UP 100, 200, 300, 400,
show vlt inconsistency

Display run-time inconsistencies in the incoming interface (IIF) for spanned multicast routes.

Syntax

```
show vlt inconsistency ip mroute
```

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant

The following is a list of the Dell Networking OS version history for this command.

```
Version 8.4.6.0   Introduced on the C-Series.
```

Example

```
FTOS#show vlt inconsistency ip mroute
Spanned Multicast Routing IIF Inconsistency
  Multicast Route | LocalIIF | PeerIIF
  ----------------|---------|---------
(22.22.22.200, 225.1.1.2) | VLAN 5  | VLAN 6
(*, 225.1.1.2)     | VLAN 15 | te 0/5

FTOS#
```

show vlt mismatch

Display mismatches in VLT parameters.

Syntax

```
show vlt mismatch
```

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant

The following is a list of the Dell Networking OS version history for this command.

```
Version 8.4.6.0   Introduced on the C-Series.
```
show vlt role

Displays the VLT peer status, role of the local VLT switch, VLT system MAC address and system priority, and the MAC address and priority of the local VLT device.

Syntax

```
show vlt role
```

Defaults

Not Configured.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on the C-Series.</th>
</tr>
</thead>
</table>

Example

```
FTOS_VLTpeer1# show vlt role

VLT Role
----------
VLT Role: Primary
System MAC address: 00:01:e8:8a:df:bc
System Role Priority: 32768
Local System MAC address: 00:01:e8:8a:df:bc
Local System Role Priority: 32768

FTOS_VLTpeer2# show vlt role

VLT Role
----------
VLT Role: Secondary
System MAC address: 00:01:e8:8a:df:bc
System Role Priority: 32768
Local System MAC address: 00:01:e8:8a:df:e6
Local System Role Priority: 32768
```
show vlt statistics

Displays statistics on VLT operations.

Syntax

show vlt statistics [arp | domain | igmp-snoop | mac | multicast | ndp]

Parameters

- **domain**: Display the VLT statistics for the domain.
- **multicast**: Display the VLT statistics for multicast.
- **mac**: Display the VLT statistics for the MAC address.
- **arp**: Display the VLT statistics for ARP.
- **igmp-snoop**: Display the VLT statistics for IGMP snooping.
- **ndp**: Display the VLT statistics for NDP.

Defaults

Not Configured.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

- **Version 8.4.6.0** Introduced on the C-Series.

Related Commands

- clear vlt statistics: Clears the statistics on VLT operations.

Example

Note: The following example shows the statistics for all of the VLT parameters. If you enter a specific keyword, such as `mac`, only the statistics for that VLT parameter displays.
show vlt statistics igmp-snoop

Displays the informational packets and IGMP control PDUs that are exchanged between VLT peer nodes.
show vlt statistics igmp-snoop

Syntax

show vlt statistics igmp-snoop

Defaults

Not Configured.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Example

FTOS_VLTpeer1#show vlt statistics igmp-snoop

VLT Igmp-Snooping Statistics
-----------------------------
IGMP Info Pkts sent: 4
IGMP Info Pkts Rcvd: 1
IGMP Reg Request sent: 1
IGMP Reg Request rcvd: 2
IGMP Reg Response sent: 1
IGMP Reg Response rcvd: 1
IGMP PDU Tunnel Pkt sent: 5
IGMP PDU Tunnel Pkt rcvd: 10
IGMP Tunnel PDUs sent: 10
IGMP Tunnel PDUs rcvd: 19

system-mac

Syntax

system-mac mac-address

Parameters

mac-address Enter the system MAC address for the VLT domain.

Defaults

Not Configured.

Command Modes

VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Usage Information
When you create a VLT domain on a switch, Dell Networking OS automatically creates a VLT-system MAC address used for internal system operations.

To reconfigure the default MAC address for the domain by entering a new MAC address in the format nn:nn:nn:nn:nn:nn, use the `system-mac` command.

You must also reconfigure the same MAC address on the VLT peer switch.

unit-id
Explicitly configure the default unit ID of a VLT peer switch.

Syntax
```
unit-id [0 | 1]
```

Parameters

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Configure the default unit ID of a VLT peer switch. Enter 0 for the first peer or enter 1 for the second peer.</td>
</tr>
</tbody>
</table>

Defaults
Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.

Command Modes
VLT DOMAIN

Command History
This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information
When you create a VLT domain on a switch, Dell Networking OS automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. Use the `unit-id` command to explicitly configure the unit ID of a VLT peer. Configure a different unit ID (0 or 1) on each peer switch.

To minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots, use this command.

vlt domain
Enable VLT on a switch, configure a VLT domain, and enter VLT-domain configuration mode.

Syntax
```
vlt domain domain-id
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-id</td>
<td>Enter the Domain ID number. Configure the same domain ID on the peer switch. The range of domain IDs is from 1 to 1000.</td>
</tr>
</tbody>
</table>

Defaults
Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.
## Command Modes

**CONFIGURATION**

### Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

The VLT domain ID must be the same between the two VLT devices. If the domain ID is not the same, a syslog message is generated and VLT does not launch.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlt brief</td>
<td>Uses the show vlt brief command to display the delay-restore value.</td>
</tr>
</tbody>
</table>

## vlt-peer-lag port-channel

Associate the port channel to the corresponding port channel in the VLT peer for the VLT connection to an attached device.

### Syntax

`vlt-peer-lag port-channel id-number`

### Parameters

- **id-number**: Enter the respective vlt port-channel number of the peer device.

### Defaults

Not configured.

### Command Modes

**INTERFACE PORT-CHANNEL**

### Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) is available on platforms: C E S
IPv6 VRRP (VRRP version 3) is available on platforms: C E S

Overview

This chapter has the following sections:

• IPv4 VRRP Commands on page 19
• IPv6 VRRP Commands on page 34

IPv4 VRRP Commands

The IPv4 VRRP commands are:

• advertise-interval
• authentication-type
• clear counters vrrp
• debug vrrp
• description
• disable
• hold-time
• preempt
• priority
• show config
• show vrrp
• track
• virtual-address
• vrrp-group
Virtual Router Redundancy Protocol (VRRP)

**advertise-interval**

Set the time interval between VRRP advertisements.

**Syntax**

```
advertise-interval time
```

**Parameters**

- `time` Enter a number of in seconds for IPv4 or centiseconds for IPv6.
  - IPv4 Default: 1 second.
  - IPv6 Default: 100 centiseconds

**Defaults**

1 second for IPv4 and 100 centiseconds for IPv6

**Command Modes**

INTERFACE-VRRP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.2.0</td>
<td>Introduced for IPv6 on E-Series TeraScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Dell Force10 recommends that you keep the default setting for this command. If you do change the time interval between VRRP advertisements on one router, you must change it on all routers.

---

**authentication-type**

Enable authentication of VRRP data exchanges.

**Syntax**

```
authentication-type simple [encryption-type] password
```

**Parameters**

- `simple` Enter the keyword `simple` to specify simple authentication.
- `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 character string up to 8 characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.

**Defaults**

Not configured.

**Command Modes**

VRRP

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

The password is displayed in the `show config` output if the encryption-type is unencrypted or clear text. If you choose to encrypt the password, the `show config` displays an encrypted text string.
clear counters vrrp

Clear the counters recorded for IPv4 VRRP operations.

**Syntax**

clear counters vrrp [vrid | vrf instance]

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrid</td>
<td>(OPTIONAL) Enter the number of the VRRP group ID. Range: 1 to 255</td>
</tr>
<tr>
<td>vrf instance</td>
<td>(OPTIONAL) E-Series only: Enter the name of a VRF instance (32 characters maximum) to clear the counters of all VRRP groups in the specified VRF.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Support was added for VRRP groups in non-default VRF instances.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version 6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

debug vrrp

Allows you to enable debugging of IPv4 and IPv6 VRRP.

**Syntax**

ddebug vrrp [ipv6] interface [vrid] {all | packets | state | timer}

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6</td>
<td>(OPTIONAL) Enter the keyword ipv6 to enable debugging of the IPv6 VRRP groups.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port 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>C-Series Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.</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 the VLAN ID. The VLAN ID range is from 1 to 4094.</td>
</tr>
<tr>
<td>vrid</td>
<td>(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.</td>
</tr>
<tr>
<td>all</td>
<td>Enter the keyword all to enable debugging of all VRRP groups.</td>
</tr>
<tr>
<td>bfd</td>
<td>Enter the keyword bfd to enable debugging of all VFP BFD interactions</td>
</tr>
<tr>
<td>packets</td>
<td>Enter the keyword packets to enable debugging of VRRP control packets.</td>
</tr>
<tr>
<td>state</td>
<td>Enter the keyword state to enable debugging of VRRP state changes.</td>
</tr>
<tr>
<td>timer</td>
<td>Enter the keyword timer to enable debugging of the VRRP timer.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege
Virtual Router Redundancy Protocol (VRRP)

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.6.0</td>
<td>Added support for the keyword fortyGigE.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

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

Parameters

text

Defaults

Not enabled.

Command Modes

VRRP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.2.0</td>
<td>Introduced for IPv6 on E-Series TeraScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

disable

Disable a VRRP group.

Syntax
disable

Defaults

C and S-Series default: VRRP is enabled.

E-Series default: VRRP is disabled.

Command Modes

VRRP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.2.0</td>
<td>Introduced for IPv6 on E-Series TeraScale</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

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 Specify 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

```plaintext
hold-time time
```

### Parameters

- **time**: Enter a number of seconds for IPv4 or centiseconds for IPv6.
  - Range: 0 to 65535, in multiples of 25 for IPv6
  - Default: 0

### Defaults

zero (0) seconds

### Command Modes

VRRP

### Command History

- **Version 8.3.2.0**: Introduced for IPv6 on E-Series TeraScale
- **Version 7.6.1.0**: Introduced on S-Series
- **Version 7.5.1.0**: Introduced on C-Series
- **pre-Version 6.2.1.1**: Introduced on E-Series

### Related Commands

- **disable**: Disable a VRRP group.

---

**preempt**

Permit a BACKUP router with a higher priority value to preempt or become the MASTER router.

### Syntax

```plaintext
preempt
```

### Defaults

Enabled (that is, a BACKUP router can preempt the MASTER router).

### Command Modes

VRRP

### Command History

- **Version 8.3.2.0**: Introduced for IPv6 on E-Series TeraScale
- **Version 7.6.1.0**: Introduced on S-Series
- **Version 7.5.1.0**: Introduced on C-Series
- **pre-Version 6.2.1.1**: Introduced on E-Series
priority

Specify a VRRP priority value for the VRRP group. This value is used by the VRRP protocol during the MASTER election process.

Syntax

```
priority priority
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>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.</td>
</tr>
</tbody>
</table>

Defaults

100

Command Modes

VRRP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced for IPv6 on E-Series TeraScale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Usage Information

To guarantee that a VRRP group becomes MASTER, configure the VRRP group’s virtual address with same IP address as the interface’s primary IP address and change the priority of the VRRP group to 255.

If you set the priority to 255 and the virtual-address is not equal to the interface’s primary IP address, an error message appears.

show config

View the non-default VRRP configuration.

Syntax

```
show config [verbose]
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>verbose</td>
<td>(OPTIONAL) Enter the keyword verbose to view all VRRP group configuration information, including defaults.</td>
</tr>
</tbody>
</table>

Command Modes

VRRP

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced for IPv6 on E-Series TeraScale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>pre-Version</td>
<td>Introduced on E-Series</td>
</tr>
</tbody>
</table>

Example

```
Figure 63-1. Command Example: show config

FTOS(conf-if-vrid-4)#show config
vrrp-group 4
  virtual-address 119.192.182.124
```
show vrrp

Display information on the IPv4 and IPv6 VRRP groups that are active. If no VRRP groups are active, the FTOS returns the message: No Active VRRP group.

Syntax

show vrrp [ipv6] [vrid] [vrf instance | interface] [brief]

Parameters

ipv6  (OPTIONAL) Enter the keyword ipv6 to display information on IPv6 VRRP groups.

vrid  (OPTIONAL) Enter a Virtual Router identifier to display information on only the specified VRRP group. Range: 1 to 255.

vrf instance  (OPTIONAL) Enter the keyword vrf and the name of a VRF instance to display information only on VRRP groups in the specified VRF. If no VRF instance is entered, information on VRRP groups in all VRFs is displayed.

interface  (OPTIONAL) Enter any of the following keywords and slot/port or number:
- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
- For a Port Channel interface, enter the keyword port-channel followed by a number:
  - C-Series and S-Series Range: 1-128
  - E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale and 1 to 512 for ExaScale.
- For SONET interfaces, enter the keyword sonet followed by the slot/port.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port.
- 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 the VLAN ID. The VLAN ID range is from 1 to 4094.

brief  (OPTIONAL) E-Series only: Enter the keyword brief to display summary information on VRRP groups.

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.4.6.0  Added support for the keyword fortyGigE.
Version 8.4.1.0  Support was added for displaying the VRRP groups in a non-default VRF instance.
Version 7.6.1.0  Introduced on S-Series
Version 7.5.1.0  Introduced on C-Series
pre-Version 6.2.1.1  Introduced on E-Series

Example

Figure 63-2.  Command Example: show vrrp brief

FTOS> show vrrp brief
Interface  Grp Pri Pre State  Master addr     Virtual addr(s)                     Description
---------------------------------------------------------------
Gi 10/37  1   100  Y   Master 200.200.200.200 200.200.200.201
Gi 10/37  3   100  Y   Master 200.200.200.200 200.200.200.201
### Table 63-1. Command Example Description: show vrrp brief

<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.</td>
</tr>
<tr>
<td></td>
<td>If the track command is configured to track that interface and the interface is disabled, the <strong>cost</strong> is subtracted from the priority value assigned to the interface.</td>
</tr>
<tr>
<td>Pre</td>
<td>States whether preempt is enabled on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Y = Preempt is enabled.</td>
</tr>
<tr>
<td></td>
<td>• N = Preempt is not enabled.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the operational state of the interface by using one of the following:</td>
</tr>
<tr>
<td></td>
<td>• NA/IF (the interface is not available).</td>
</tr>
<tr>
<td></td>
<td>• MASTER (the interface associated with the MASTER router).</td>
</tr>
<tr>
<td></td>
<td>• BACKUP (the interface associated with the BACKUP router).</td>
</tr>
<tr>
<td>Master addr</td>
<td>Displays the IP address of the MASTER router.</td>
</tr>
<tr>
<td>Virtual addr(s)</td>
<td>Displays the virtual IP addresses of the VRRP routers associated with the interface.</td>
</tr>
</tbody>
</table>
**Figure 63-3. Command Example: show vrrp**

```
FTOS>show vrrp
------------------
GigabitEthernet 12/3, VRID: 1, Net: 10.1.1.253
VRF: 0 default-vrf
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 GigabitEthernet 12/17 priority-cost 10
------------------
GigabitEthernet 12/4, VRID: 2, Net: 10.1.2.253
VRF: 0 default-vrf
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 GigabitEthernet 2/1 priority-cost 10
  Up GigabitEthernet 12/17 priority-cost 10
------------------
GigabitEthernet 7/30, IPv6 VRID: 3, Version: 3, Net: fe80::201:e8ff:fe01:95cc
VRF: 0 default-vrf
State: Master, Priority: 100, Master: fe80::201:e8ff:fe01:95cc (local)
Accept Mode: FALSE, Master AdvInt: 100 centisec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 310
Virtual MAC address: 00:00:5e:00:201:e8ff:fe01:95cc
Virtual IP address: 2007::1 fe80::1
Tracking states for 2 resource Ids:
  2 - Up IPv6 route, 2040::/64, priority-cost 20, 00:02:11
  3 - Up IPv6 route, 2050::/64, priority-cost 30, 00:02:11
```

**Table 63-2. Command Example Description: show vrrp**

<table>
<thead>
<tr>
<th>Line Beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet...</td>
<td>Displays the Interface, the VRRP group ID, and the network address. If the interface is no sending VRRP packets, 0.0.0.0 appears as the network address.</td>
</tr>
<tr>
<td>VRF</td>
<td>VRF instance to which the interface (on which the VRRP group is configured) belongs</td>
</tr>
</tbody>
</table>
| State: master...    | Displays the interface’s state:  
  • Na/If (not available),  
  • master (MASTER virtual router)  
  • backup (BACKUP virtual router)  
  the interface’s priority and the IP address of the MASTER. |
| Hold Down:...       | This line displays additional VRRP configuration information:  
  • Hold Down displays the hold down timer interval in seconds.  
  • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.  
  • AdvInt displays the Advertise Interval in seconds. |
Table 63-2. Command Example Description: show vrrp

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adv rcvd:</strong>...</td>
<td>This line displays counters for the following:</td>
</tr>
<tr>
<td></td>
<td>• <em>Adv rcvd</em> displays the number of VRRP advertisements received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• <em>Adv sent</em> displays the number of VRRP advertisements sent on the interface.</td>
</tr>
<tr>
<td></td>
<td>• <em>Gratuitous ARP</em> sent displays the number of gratuitous ARPs sent.</td>
</tr>
<tr>
<td><strong>Virtual MAC address</strong></td>
<td>Displays the virtual MAC address of the VRRP group.</td>
</tr>
<tr>
<td><strong>Virtual IP address</strong></td>
<td>Displays the virtual IP address of the VRRP router to which the interface is connected.</td>
</tr>
<tr>
<td><strong>Authentication:</strong>...</td>
<td>States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.</td>
</tr>
<tr>
<td><strong>Tracking states...</strong></td>
<td>Displays information on the tracked interfaces or objects configured for a VRRP group (track command), including:</td>
</tr>
<tr>
<td></td>
<td>• UP or DOWN state of the tracked interface or object (U or D)</td>
</tr>
<tr>
<td></td>
<td>• Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object</td>
</tr>
<tr>
<td></td>
<td>• Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.</td>
</tr>
</tbody>
</table>
Monitor an interface or a configured object and, optionally, reconfigure the cost value subtracted from the VRRP group priority if the tracked interface or object goes down. You can assign up to 12 tracked interfaces and up to 20 tracked objects per virtual group.

**Syntax**

```
track {interface | object-id} [priority-cost cost]
```

**Parameters**

- **interface**
  - Enter one of the following values:
    - For a 1-Gigabit Ethernet interface, enter `gigabitethernet slot-number/port-number`.
    - For a Loopback interface, enter `loopback number`, where valid loopback interface numbers are from 0 to 16383.
    - For a Port Channel interface, enter `port-channel number`, where valid port-channel numbers are:
      - **C-Series** and **S-Series**: 1 to 128
      - **E-Series**: 1 to 32 for EtherScale; 1 to 255 for TeraScale; 1 to 512 for ExaScale.
    - For SONET interfaces, enter `sonet slot-number/port-number`.
    - For a 10-Gigabit Ethernet interface, enter `tengigabitethernet slot-number/port-number`.
    - For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` followed by the slot/port information.
    - For a VLAN interface, enter `vlan id-number`, where valid VLAN IDs are from 1 to 4094.

- **object-id**
  - Enter the ID number of an object (for example, IPv4/IPv6 route or Layer 2/Layer 3 interface) configured with one of the `track object-id` commands.
  - Range: 1 to 65535.

- **cost**
  - (OPTIONAL) Enter a number as the cost amount to be subtracted from the VRRP priority value.

**Defaults**

```
cost = 10
```

**Command Modes**

VRRP

**Command History**

- **Version 8.4.6.0**  Added support for the keyword `fortyGigE`.
- **Version 8.4.1.0**  Support for the `object-id` variable was added.
- **Version 8.3.2.0**  Introduced for IPv6 on E-Series TeraScale
- **Version 7.6.1.0**  Introduced on S-Series
- **Version 7.5.1.0**  Introduced on C-Series
- **pre-Version 6.2.1.1**  Introduced on E-Series

**Usage Information**

The sum of the costs of all tracked interfaces and objects cannot equal or exceed the priority of the VRRP group.

If the VRRP group is configured as the Owner router (priority 255), tracking for the group is disabled, irrespective of the state of tracked interfaces and objects. The priority of the owner group always remains as 255 and does not change.
If the specified interface or object goes down or is disabled, the cost value is subtracted from the priority value. As a result, a new MASTER election may occur if the resulting priority value is lower than the priority value in the BACKUP virtual routers.
virtual-address

Configure up to 12 IP addresses of virtual routers in the VRRP group. You must set at least one virtual address for the VRRP group to start sending VRRP packets. For IPv4 addresses multiple addresses can be entered in the same command line. For IPv6 addresses, each address must be entered separately.

Syntax

```
virtual-address address1 [...address12]
```

Parameters

- `address1`: Enter an IPv4 address or IPv6 address for the virtual router.
  The IP address must be on the same subnet as the interface’s primary IP address.

- `... address12`: For IPv4 addresses only: Enter up 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space.
  The IP addresses must be on the same subnet as the interface’s primary IP address.

Defaults

Not configured.

Command Modes

VRRP

Command History

- **Version 8.3.2.0**: Introduced for IPv6 on E-Series TeraScale
- **Version 7.6.1.0**: Introduced on S-Series
- **Version 7.5.1.0**: Introduced on C-Series
- **Version 7.4.1.0**: Introduced support for telnetting to the VRRP group IP address assigned using this command
- **pre-Version 6.2.1.1**: Introduced on E-Series

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. The priority of the VRRP group is then automatically set to 255 and the interface becomes the MASTER/OWNER router of the VRRP group. You can also configure a priority for the group even if the group is owned. The configured priority is saved but only applied as the run-time priority when the last virtual address is removed from the group.

You can ping the virtual addresses configured in all VRRP groups.
vrrp-group

Assign an interface to a VRRP group.

Syntax

vrrp-group vrid

Parameters

vrid

Enter the virtual-router ID number of the VRRP group.

VRID range (C-Series and S-Series): 1-255.

VRID range (E-Series): 1-255 when VRF microcode is not loaded and 1-15 when VRF microcode is loaded.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.4.2.1 When VRF microcode is loaded in CAM, the range of valid VRID values on the E-Series changed to 1-15.

Version 8.4.1.0 Support was added for configuring a VRRP group on an interface in a non-default VRF instance.

Version 7.6.1.0 Introduced on S-Series

Version 7.5.1.0 Introduced on C-Series

pre-Version 6.2.1.1 Introduced on E-Series

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.

Starting in release 8.4.1.0, you can configure a VRRP group on an interface in a non-default VRF instance.

E-Series ExaScale only: You can configure up to 16 VRRP groups per VLAN and up to 511 groups on all VLANs.

E-Series ExaScale and TeraScale only: Starting in release 8.4.2.1, you can configure up to 255 VRRP groups per interface if VRF microcode is not loaded, and up to 15 groups if VRF microcode is loaded.

E-Series ExaScale and TeraScale only: Starting in release 8.4.2.1, the VRID used by the VRRP protocol changes according to whether VRF microcode is loaded or not:

- When VRF microcode is not loaded in CAM, the VRID for a VRRP group is the same as the VRID number configured with the vrrp-group or vrrp-ipv6-group command.
- When VRF microcode is loaded in CAM, the VRID for a VRRP group is equal to 16 times the vrrp-group or vrrp-ipv6-group vrid number plus the ip vrf vrf-id number.

For example, if VRF microcode is loaded and VRRP group 10 is configured in VRF 2, the VRID used for the VRRP group is (16 x 10) + 2, or 162. This VRID value is used in the lowest byte of the virtual MAC address of the VRRP group and is also used for VRF routing.
Figure 63-4 shows how the actual VRID used by a VRRP group is displayed:

- Below the command line - when VRF microcode is loaded and you enter the `vrrp-group` or `vrrp-ipv6-group` command in VRRP-group configuration mode.
- In `show vrrp` command output.

**Important**: You must configure the same VRID on neighboring routers (Dell Networking or non-Dell Networking) in the same VRRP group in order for all routers to interoperate.

**Figure 63-4. VRRP used when VRF microcode is loaded**

```
FTOS(conf)#ip vrf orange 2
FTOS(conf)#interface GigabitEthernet 3/0
FTOS(conf-if-gi-3/0)#ip vrf forwarding orange
FTOS(conf-if-gi-3/0)#ip address 1.1.1.1/24
FTOS(conf-if-gi-3/0)#vrrp-group 10
  % Info: The VRID used by the VRRP group 10 in VRF 2 is 162.
FTOS(conf-if-gi-3/0-vrid-162)#virtual-ip 1.1.1.10
FTOS(conf-if-gi-3/0-vrid-162)#exit
FTOS(conf-if-gi-3/0)#no shutdown

FTOS#show vrrp
------------------
GigabitEthernet 3/0, IPv4 Vrrp-group: 10, VRID: 162, Version: 2, Net: 1.1.1.1
VRF: 2 orange
State: Master, Priority: 120, Master: 1.1.1.1 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 76, Gratuitous ARP sent: 1
Virtual MAC address:
  00:00:5e:00:01:a2
Virtual IP address:
  1.1.1.10
Authentication: (none)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-address</td>
<td>Assign up to 12 virtual IP addresses per VRRP group.</td>
</tr>
</tbody>
</table>
IPv6 VRRP Commands

The IPv6 VRRP commands are:

- clear counters vrrp ipv6
- debug vrrp ipv6
- show vrrp ipv6
- vrrp-ipv6-group

The following commands apply to IPv4 and IPv6:

- advertise-interval
- description
- disable
- hold-time
- preempt
- priority
- show config
- track
- virtual-address

**clear counters vrrp ipv6**

Clear the counters recorded for IPv6 VRRP groups.

**Syntax**

```
clear counters vrrp ipv6 [vrid | vrf instance]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrid</td>
<td>(OPTIONAL) Enter the number of an IPv6 VRRP group. Range: 1 to 255</td>
</tr>
<tr>
<td>vrf instance</td>
<td>(OPTIONAL) E-Series only: Enter the name of a VRF instance (32 characters maximum) to clear the counters of all IPv6 VRRP groups in the specified VRF.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4.1.0</td>
<td>Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.</td>
</tr>
<tr>
<td>8.3.2.0</td>
<td>Introduced on E-Series TeraScale</td>
</tr>
</tbody>
</table>
**debug vrrp ipv6**

Allows you to enable debugging of VRRP.

**Syntax**

```
depbug vrrp ipv6 interface [vrid] [all | packets | state | timer]
```

**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 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.  
| • For a Port Channel interface, enter the keyword **port-channel** followed by a number:  
| E-Series Range: 1 to 255 for TeraScale  
| • 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.  
| vrid | (OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.  
| all | Enter the keyword **all** to enable debugging of all VRRP groups.  
| bfd | Enter the keyword **bfd** to enable debugging of all VRRP BFD interactions  
| database | Enter the keyword **database** to display changes related to group, prefix, and interface entries in the VRRP table.  
| packets | Enter the keyword **packets** to enable debugging of VRRP control packets.  
| state | Enter the keyword **state** to enable debugging of VRRP state changes.  
| timer | Enter the keyword **timer** to enable debugging of the VRRP timer.  

**Command Modes**

EXEC Privilege

**Command History**

- Version 8.4.1.0 Introduced on E-Series ExaScale, C-Series, and S-Series.
- Version 8.3.2.0 Introduced on E-Series TeraScale

**Usage Information**

If no options are specified, debug is active on all interfaces and all VRRP groups.
show vrrp ipv6

View the IPv6 VRRP groups that are active. If no VRRP groups are active, the FTOS returns “No Active VRRP group.”

Syntax

```
show vrrp ipv6 [vrid] [interface] [brief]
```

Parameters

- **vrid** (OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group.
  
  Range: 1 to 255.

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
  
  - For a Port Channel interface, enter the keyword `port-channel` followed by a number:
    - **E-Series** Range: 1 to 255 for TeraScale
  
  - For SONET interfaces, enter the keyword `sonet` followed by the 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.
  
  - 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 on the E-Series.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 8.3.2.0 Introduced

Figure 63-5. Command Example: show vrrp ipv6

```
FTOS#show vrrp ipv6
------------------
VRF: 0 default-vrf
State: Master, Priority: 101, Master: fe80::201:e8ff:fe7a:6bb9 (local)
Hold Down: 0 centisec, Preempt: TRUE, AdvInt: 100 centisec
Accept Mode: FALSE, Master AdvInt: 100 centisec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 64
Virtual MAC address: 00:00:5e:00:02:ff
Virtual IP address: 1::255 fe80::255
```

Table 63-3. Command Example Description: show vrrp ipv6

<table>
<thead>
<tr>
<th>Line Beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet...</td>
<td>Displays the Interface, the VRRP group ID, and the network address. If the interface is no sending VRRP packets, 0.0.0.0 appears as the network address.</td>
</tr>
<tr>
<td>VRF</td>
<td>VRF instance to which the interface (on which the VRRP group is configured) belongs</td>
</tr>
</tbody>
</table>
### Table 63-3. Command Example Description: show vrrp ipv6

<table>
<thead>
<tr>
<th>State: master...</th>
<th>Displays the interface’s state:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Na/If (not available),</td>
</tr>
<tr>
<td></td>
<td>• master (MASTER virtual router)</td>
</tr>
<tr>
<td></td>
<td>• backup (BACKUP virtual router)</td>
</tr>
<tr>
<td></td>
<td>the interface’s priority and the IP address of the MASTER.</td>
</tr>
<tr>
<td>Hold Down:....</td>
<td>This line displays additional VRRP configuration information:</td>
</tr>
<tr>
<td></td>
<td>• Hold Down displays the hold down timer interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>• Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.</td>
</tr>
<tr>
<td></td>
<td>• AdvInt displays the Advertise Interval in seconds.</td>
</tr>
<tr>
<td>Adv rcvd:....</td>
<td>This line displays counters for the following:</td>
</tr>
<tr>
<td></td>
<td>• Adv rcvd displays the number of VRRP advertisements received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Adv sent displays the number of VRRP advertisements sent on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Bad pkts rcvd displays the number of invalid packets received on the interface.</td>
</tr>
<tr>
<td>Virtual MAC address</td>
<td>Displays the virtual MAC address of the VRRP group.</td>
</tr>
<tr>
<td>Virtual IP address</td>
<td>Displays the virtual IP address of the VRRP router to which the interface is connected.</td>
</tr>
<tr>
<td>Tracking states...</td>
<td>Displays information on the tracked interfaces or objects configured for a VRRP group (track command), including:</td>
</tr>
<tr>
<td></td>
<td>• UP or DOWN state of the tracked interface or object (Up or Dn)</td>
</tr>
<tr>
<td></td>
<td>• Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object</td>
</tr>
<tr>
<td></td>
<td>• Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN</td>
</tr>
</tbody>
</table>
vrrp-ipv6-group

Assign an interface to a VRRP group.

Syntax

vrrp-ipv6-group vrid

Parameters

vrid

Enter the virtual-router ID number of the VRRP group.

VRID range (C-Series and S-Series): 1-255.
VRID range (E-Series): 1-255 when VRF microcode is not loaded and 1-15 when VRF microcode is loaded.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

Version 8.4.2.1 The range of valid VRID values on the E-Series when VRF microcode is loaded in CAM changed to 1-15.

Version 8.4.1.0 Introduced on E-Series ExaScale, C-Series, and S-Series.

Version 8.3.2.0 Introduced on E-Series TeraScale

Usage Information

The VRRP group only becomes active and sends VRRP packets when a link-local virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

E-Series ExaScale and TeraScale only: Starting in release 8.4.2.1, you can configure up to 255 VRRP groups per interface if VRF microcode is not loaded, and up to 15 groups if VRF microcode is loaded.

E-Series ExaScale and TeraScale only: Starting in release 8.4.2.1, the VRID used by the VRRP protocol changes according to whether VRF microcode is loaded or not:

- When VRF microcode is not loaded in CAM, the VRID for a VRRP group is the same as the VRID number configured with the vrrp-group or vrrp-ipv6-group command.
- When VRF microcode is loaded in CAM, the VRID for a VRRP group is equal to 16 times the vrrp-group or vrrp-ipv6-group vrid number plus the ip vrf vrf-id number.

For example, if VRF microcode is loaded and VRRP group 10 is configured in VRF 2, the VRID used for the VRRP group is (16 x 10) + 2, or 162. This VRID value is used in the lowest byte of the virtual MAC address of the VRRP group and is also used for VRF routing.

Important: You must configure the same VRID on neighboring routers (Dell Networking or non-Dell Networking) in the same VRRP group in order for all routers to interoperate.

Related Commands

virtual-address Assign up to 12 virtual IP addresses per VRRP group.
C-Series Diagnostics and Debugging

Overview

This chapter contains the following sections:

- Inter-process Communication Commands
- RPM Management Port Commands
- Data Path Debugging Commands
- Interface Troubleshooting Commands
- Advanced ASIC Debugging Commands
- ACL and System-Flow Debug Commands
- Interface Management Debug Commands
- Layer 2 Debug Command
- Trace Logging Commands
- Offline Diagnostic Commands
- PoE Hardware Status Commands
- Buffer Tuning Commands

Inter-process Communication Commands

The following are Inter-Process Communication (IPC) commands. IPC commands display receive and transmit frame counters for the party-bus switch and CPU interfaces. These interfaces are the interfaces over which Dell Networking OS task-to-task control messages are exchanged.

- clear hardware cpu party-bus
- clear hardware rpm mac counters
- hardware monitor linecard
- hardware monitor mac
- hardware watchdog
- show hardware cpu party-bus
- show hardware rpm mac

**clear hardware cpu party-bus**

Clear the receive, transmit, and error counters for the party-bus port on the CPU of the specified line card or RPM.

**Syntax**

```
clear hardware {linecard | rpm} number cpu party-bus statistics
```
### clear hardware rpm mac counters

Clear receive and transmit Ethernet statistics for all ports on the party-bus switch of the specified RPM.

**Syntax**

```
clear hardware rpm number mac counters
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter the RPM slot number. Range: 0-1</td>
</tr>
</tbody>
</table>

**Defaults**

None.

**Command Mode**

EXEC

EXEC Privilege

**Command History**

Version 7.5.10 Introduction

**Usage Information**

⚠️ **Warning:** Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.
**hardware monitor linecard**

Configure the system to take an action upon a line card hardware error.

**Syntax**

```plaintext
hardware monitor linecard asic \{btm \[action-on-error \{card-problem | card-reset | card-shutdown\}\] \| fpc \[action-on-error | parity-correction\]\}
```

**Parameters**

- **action-on-error** Enter the keyword `action-on-error` to further specify actions that should be taken in the event of a hardware error.
- **btm** Enter the keyword `btm` to configure the system to take an action upon a Buffer Traffic Manager hardware error.
- **fpc** Enter the keyword `fpc` to configure the system to take an action upon a Flexible Packet Classifier hardware error.
- **card-problem** Enter the keyword `card-problem` to place a line card in a card-problem state upon a hardware error.
- **card-reset** Enter the keyword `card-reset` to reset a line card upon a hardware error.
- **card-shutdown** Enter the keyword `card-shutdown` to shutdown a line card upon a hardware error.
- **parity-correction** Enter the keyword `parity-correction` to enable automatic parity corrections for SRAM. The line card must be reloaded before the feature becomes operational.

**Defaults**

None

**Command Mode**

CONFIGURATION

**Command History**

- Version 8.2.1.0 Introduced

---

**hardware monitor mac**

Configure the system to shut down all ports on a line card upon a MAC hardware error.

**Syntax**

```plaintext
hardware monitor mac action-on-error port-shutdown
```

**Defaults**

None

**Command Mode**

CONFIGURATION

**Command History**

- Version 8.2.1.0 Introduced

---

**hardware watchdog**

Set the watchdog timer to trigger a reboot and restart the system.

**Syntax**

```plaintext
hardware watchdog
```

**Defaults**

Enabled
This command enables a hardware watchdog mechanism that automatically reboots an Dell Networking OS switch/router with a single unresponsive RPM. This is a last resort mechanism intended to prevent a manual power cycle.

**show hardware cpu party-bus**

View advanced debugging counters for the party-bus port on the CPU of the specified line card or RPM.

**Syntax**

```plaintext
show hardware {linecard | rpm} number cpu party-bus statistics
```

**Parameters**

- **linecard**
  - Enter the keyword `linecard` to view debugging counters for a line card.

- **rpm**
  - Enter the keyword `rpm` to view cpu debugging counters for an RPM.

- **number**
  - Enter a number after the following keywords:
    - After the keyword `rpm`:
      - Range: 0-1
    - After the keyword `linecard`:
      - Range: 0-7 for the C300

**Defaults**

None.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

Version 7.7.1.0 Introduced

Version 7.5.1.0 Introduction
Example Figure 64-1. show hardware linecard Command Example

```
FTOS#show hardware linecard 1 cpu party-bus statistic
ACTIVE EMAC DEVICE:2 STATISTICS
  Num of Pkts. Tx Requested = 2788452, Number of Pkts Transmitted = 2788452
  Num of Pkts. Received  = 139662, Number of Pkts Given to MUX = 139662
  Transmit Errors due to no Data = 0
  Transmit Errors due to exceed num of Desc = 0
  Transmit Block Count (Stall Count) = 0
 Recv Pkts Dropped due to Bad Pkts Rx = 0
  Recv Pkts Dropped due to more than one Buf = 0
  Recv Pkts Dropped due to out of Mem = 0
  Recv Pkts Dropped due to out of CBlk = 0
  Recv Pkts Dropped due to out of MBlk = 0
ALTERNATIVE EMAC DEVICE:3 STATISTICS
  Num of Pkts. Tx Requested = 0, Number of Pkts Transmitted = 0
  Num of Pkts. Received  = 0, Number of Pkts Given to MUX = 0
  Transmit Errors due to no Data = 0
  Transmit Errors due to exceed num of Desc = 0
  Transmit Block Count (Stall Count) = 0
  Recv Pkts Dropped due to Bad Pkts Rx = 0
  Recv Pkts Dropped due to more than one Buf = 0
  Recv Pkts Dropped due to out of Mem = 0
  Recv Pkts Dropped due to out of CBlk = 0
  Recv Pkts Dropped due to out of MBlk = 0
```

Warning: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear hardware cpu party-bus</td>
<td>Clear the receive, transmit, and error counters and for the party-bus port on the CPU of the specified RPM.</td>
</tr>
</tbody>
</table>

show hardware rpm mac

View receive and transmit counters for the party-bus switch in the IPC subsystem.

Syntax

```
show hardware rpm number mac {counters | port-statistics {linecard number | rpm number}}
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>Enter the keyword counters to view high-level receive and transmit counters.</td>
</tr>
<tr>
<td>port-statistics</td>
<td>Enter the keyword port-statistics to view detailed Ethernet statistics for the specified port on the party-bus switch.</td>
</tr>
<tr>
<td>linecard</td>
<td>Enter the keyword linecard to view information about a particular line card.</td>
</tr>
<tr>
<td>rpm</td>
<td>Enter the keyword rpm to view information about a particular RPM.</td>
</tr>
<tr>
<td>number</td>
<td>Enter a number after the following keywords:</td>
</tr>
<tr>
<td></td>
<td>• After the keyword rpm:</td>
</tr>
<tr>
<td></td>
<td>Range: 0-1</td>
</tr>
<tr>
<td></td>
<td>• After the keyword linecard:</td>
</tr>
<tr>
<td></td>
<td>Range: 0-7 for the C300</td>
</tr>
</tbody>
</table>

Defaults

None

Command Mode

EXEC
EXEC Privilege
**Command History**

**Version 7.5.1.0**

**Introduction**

**Example**

**Figure 64-2. show hardware rpm mac counters Command Example**

```
FTOS#show hardware rpm 0 mac counters
Received and Transmitted Packets without Errors
SLOT ID#  Rx Counter  TxCounter
RSM SLOTS:
  0          1         17
  1          0         0
LCM SLOTS:
  0          0         0
  1          17        1
  2          0         0
  3          0         0
  4          0         0
  5          0         0
  6          0         0
```

**Table 64-1. show hardware rpm mac counters Output Description**

<table>
<thead>
<tr>
<th>Slot ID #</th>
<th>Port number on the party-bus control switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Frames</td>
<td>Number of packets received by the party-bus switch from the processor in the specified slot.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Verify the counters are incrementing.</td>
</tr>
<tr>
<td>TX Frames</td>
<td>Number of packets sent by the party-bus switch to the processor in the specified slot.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Verify the counters are incrementing.</td>
</tr>
</tbody>
</table>

**Figure 64-3. show hardware rpm mac port-statistics Command Example**

```
FTOS#show hardware rpm 0 mac port-statistics linecard 1
IPC Switch Port Number :7
snmpIfInOctets : 2471340
snmpIfInUcastPkts : 2410
snmpIfOutOctets : 16046
snmpIfOutUcastPkts : 99
snmpDot1dTpPortInFrames : 2410
snmpDot1dTpPortOutFrames : 99
snmpEtherStatsPkts128to255Octets : 491
snmpEtherStatsPkts512to1023Octets : 640
snmpEtherStatsPkts1024to1518Octets : 1378
snmpEtherStatsOctets : 2487386
snmpEtherStatsTxNoErrors : 99
snmpEtherStatsRXNoErrors : 2410
snmpIfHCInOctets : 2471340
snmpIfHCInUcastPkts : 2410
snmpIfHCOutOctets : 16046
snmpIfHCOutUcastPkts : 99
```

**Usage Information**

**Warning:** Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

**Related Commands**

- `clear hardware rpm mac counters` Clear the receive, transmit, and error counters and for the party-bus port on the CPU of the specified RPM.
RPM Management Port Commands

**show hardware rpm cpu management**

View standard Ethernet receive and transmit counters as well as auto-negotiation debugging information for the external management interface.

**Syntax**

```
show hardware rpm number cpu management statistics
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter the RPM slot number. Range: 0-1</td>
</tr>
</tbody>
</table>

**Defaults**

None.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- Version 7.5.1.0 Introduction
Example Figure 64-4. show hardware rpm Command Example

```
FTOS#show hardware rpm 0 cpu management statistics
Port #0 MIB Counters
GoodFramesReceived = 4214683
BadFramesReceived = 2
BroadcastFramesReceived = 275828
MulticastFramesReceived = 3787188
GoodOctetsReceived = 0x0000303000000000
GoodFramesSent = 9539
BroadcastFramesSent = 0
MulticastFramesSent = 0
GoodOctetsSent = 128

FC Control Counters
UnrecogMacControlReceived = 0
GoodFCFramesReceived = 0
BadFCFramesReceived = 0
FCFramesSent = 0

RX Errors
BadOctetsReceived = 260
UndersizeFramesReceived = 0
FramesReceived = 0
OversizeFramesReceived = 0
JabbersReceived = 0
MacReceiveErrors = 0
BadCrcReceived = 0
Rx Discarded packets counter = 0
Rx Overrun packets counter = 0

TX Errors
TxErrors = 0
TxEcessiveCollisions = 0
TXCollisions = 2
TXLateCollisions = 0

10 BASE-T half-duplex
Auto-negotiation is complete
```

The PHY Port power is normal
ethGiga #0 port Status: 0x2444 = 0x00000402

Link=UP, Speed=10, Duplex=HALF, RxFlowControl=DISABLE, padLen=136
RxCol = 0 usec, TXCol = 0 usec
MacAddr (0x3bc75e54) = 00:01:e8:2e:2f:20
RX Queue #0: base=0x42000000, free=1024
TX Queue #0: base=0x42008020, free=2048

```
MANAGEMENT PHY REGISTER VALUES
0x00: 0x1000 0x01: 0x796D 0x02: 0x0143 0x03: 0xBCB1
0x04: 0x0021 0x05: 0x41E1 0x06: 0x0065 0x07: 0x2001
0x08: 0x0000 0x09: 0x0000 0x0A: 0x0000 0x0B: 0x0000
0x0C: 0x0000 0x0D: 0x0000 0x0E: 0x0000 0x0F: 0x0000
0x10: 0x0000 0x11: 0x0000 0x12: 0x0000 0x13: 0x0000
0x14: 0x0000 0x15: 0x0000 0x16: 0x0000 0x17: 0x0000
0x18: 0x0400 0x19: 0x8114 0x1A: 0x0000 0x1B: 0x0FFF
0x1C: 0x38A3 0x1D: 0x0000 0x1E: 0x0000 0x1F: 0x0000

MII Control Register
SpeedSelection: 10Mbps
--More--
```

**Warning:** Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.
Data Path Debugging Commands

Data path refers to external data and control packets that are sent to an RPM or line card, or processed by FP and forwarded through the system.

- show hardware drops
- show hardware cpu data-plane

show hardware drops

View internal packet-drop counters on a line card or RPM.

**Syntax**

```
show hardware {linecard number | rpm number} drops [unit number] [port number]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linecard</td>
<td>Enter the keyword <strong>linecard</strong> to view information about a line card.</td>
</tr>
<tr>
<td>rpm</td>
<td>Enter the keyword <strong>rpm</strong> to view information about an RPM.</td>
</tr>
<tr>
<td>unit</td>
<td>(OPTIONAL) Enter the keyword <strong>unit</strong> to view information about a unit. Range: 0-3</td>
</tr>
<tr>
<td>port</td>
<td>(OPTIONAL) Enter the keyword <strong>port</strong> to view information about a port. Range: 1-8</td>
</tr>
</tbody>
</table>

**number**

Enter a number after the following keywords:

- After the keyword **linecard**: Range: 0-7 for the C300
- After the keyword **rpm**: Range: 0-1
- After the keyword **unit**, enter the number of CSF or FP ASIC.
- After the keyword **port**, enter the port number.

**Defaults**

None.

**Command Mode**

EXEC

EXEC Privilege

**Command History**

Version 7.5.1.0 Introduction
Example

**Figure 64-5. show hardware drops Command Example**

FTOS#show hardware rpm 0 drops

UNIT No: 0
Total Ingress Drops :0
Total IngMac Drops :0
Total Mmu Drops :0
Total EgMac Drops :0
Total Egress Drops :0

UNIT No: 1
Total Ingress Drops :0
Total IngMac Drops :0
Total Mmu Drops :0
Total EgMac Drops :0
Total Egress Drops :0

UNIT No: 2
Total Ingress Drops :0
Total IngMac Drops :0
Total Mmu Drops :0
Total EgMac Drops :0
Total Egress Drops :0

UNIT No: 3
Total Ingress Drops :0
Total IngMac Drops :0
Total Mmu Drops :0
Total EgMac Drops :0
Total Egress Drops :0

The figure below shows the command to display dropped packets per unit, in other words, dropped packets for a particular FP or CSF ASIC.

**Figure 64-6. show hardware drops unit Command Example**

FTOS#show hardware rpm 0 drops unit 0

<table>
<thead>
<tr>
<th>Port#</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>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The figure below shows the command to display dropped packets for a particular port on a unit.
Figure 64-7.  show hardware drops unit port Command Example

```
FTOS#show hardware rpm 0 drops unit 0 port 1
--- Ingress Drops ---
Unknown HiGig HDR :0
Unknown HiGig OPCODE :0
Unknown HiGig HDR Format :0
RX EgressBlockMask :0
Rx LinkBlockCnt :0
Rx SrcModBlockCnt :0
IBP CBP FullDrops :0
Rx AgedCnt :0
--- Ingress MAC Drops ---
IngressMacDrops :0
--- MMU Drops ---
HOL DROPS on COS0 :0
HOL DROPS on COS1 :0
HOL DROPS on COS2 :0
HOL DROPS on COS3 :0
HOL DROPS on COS4 :0
HOL DROPS on COS5 :0
HOL DROPS on COS6 :0
HOL DROPS on COS7 :0
--- Egress MAC counters ---
egressMACDrops :0
--- Egress Drops ---
Tx AgedCounter :0
Tx ErrCounter :0
Tx MacUnderFlow :0
```

Usage

```
Warning: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.
```

show hardware cpu data-plane

View the driver statistics on the CPU of the specified line card or RPM.

Syntax

```
show hardware {linecard | rpm} number cpu data-plane statistics
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linecard</td>
<td>Enter the keyword linecard to view cpu data plane statistics for a line card.</td>
</tr>
<tr>
<td>rpm</td>
<td>Enter the keyword rpm to view cpu data plane statistics for an RPM.</td>
</tr>
</tbody>
</table>
| number    | Enter a number after the following keywords:  
|           | • After the keyword rpm:  
|           |   Range: 0-1  
|           | • After the keyword linecard:  
|           |   Range: 0-7 for the C300 |

Defaults

None

Command Mode

EXEC

EXEC Privilege

Command History

Version 7.5.1.0  Introduction
Example 1  
**Figure 64-8. show hardware linecard Command Example**

FTOS#show hardware linecard 1 cpu data-plane statistics

-----SOCEND driver statistics for device 4-----
rxHandle :0
noBuff :0
noMblk :0
noClblk :0
recvd :0
dropped :0
recvToMux :0
txInt :0
transmitted :0
txRequested :0
noTxDesc :0
txError :0
txWrongIntf :0
txNotInit :0
txReqTooLarge :0
txInternalError :0
rxError :0
Socend Driver Pool Statistics for device 4
-----------------------------------------
poolMBlkGetCnt = 0
poolMC1GetCnt = 0
poolCBlkGetCnt = 0
poolClusterGetCnt = 0
poolMBlkFreeCnt = 0
poolMBlkClFreeCnt = 0
poolCBlkFreeCnt = 0
poolCLFreeCnt = 0
poolC1PoolIdGetCnt = 1
-----------------------------------------

Example 2  
**Figure 64-9. show hardware rpm Command Example**

FTOS#show hardware rpm 0 cpu data-plane statistics

-----SOCEND driver statistics for device 2-----
rxHandle :0
noBuff :0
noMblk :0
noClblk :0
recvd :0
dropped :0
recvToMux :0
txInt :0
transmitted :0
txRequested :0
noTxDesc :0

**Warning:** Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

### Interface Troubleshooting Commands

This command provides additional information related to standard `show interface` commands.

See also in Chapter 23, Interfaces*:

- `show interfaces phy`
- `show interfaces transceiver`
show hardware interface phy

View MAC- and PHY-related registers and link status information, including the transmitted and received auto-negotiation control words.

Syntax

```
show hardware interface interface phy [registers]
```

Parameters

- **phy**
  - Enter the keyword `phy` to display sent and received auto-negotiation and Layer 1 link status information.
- **registers**
  - (OPTIONAL) Use the `registers` keyword to display a dump of the PHY registers in hexadecimal.
- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the 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.

Defaults

None.

Command Mode

- EXEC
- EXEC Privilege

Command History

- **Version 8.4.6.0** Added support for the keyword `fortyGigE`.
- **Version 7.5.1.0** Introduction
FTOS#show hardware interface gig 1/0 phy
MII Control Register
  SpeedSelection: 1000Mbps
  AutoNeg: ON
  Loopback: False
  PowerDown: False
  Isolate: False
  DuplexMode: Full
  MII Status Register:
  AutoNegComplete: False
  RemoteFault: False
  LinkStatus: False
  JabberDetect: False
  PHY Identifier Register:
  PHY Identifier Register:
  Auto-Negotiation Advertisement Register
  100MegFullDplx: True
  100MegHalfDplx: True
  10MegFullDplx: True
  10MegHalfDplx: True
  Asym Pause: False
  Sym Pause: True
  Auto-Negotiation Link Partner Register:
  100MegFullDplx: False
  100MegHalfDplx: False
  10MegFullDplx: False
  10MegHalfDplx: False
  Asym Pause: False
  Sym Pause: False
  1000Base-T Control Register:
  Master/Slave Mode: Auto
  1000MegFullDplx: True
  1000MegHalfDplx: True
  1000Base-T Status Register
  Master/Slave Fault: No
  Master/Slave: Slave
  Local RX OK: False
  Remote RX OK: False
  Link Partner 1000MegFullDplx: False
  Link Partner 1000MegHalfDplx: False
  Idle Error Count: 0
  1000Base-T/100Base-TX/10Base-T IEEE Extnd Status Register
  1000Base-T/100Base-TX/10Base-T PHY Extnd Control Register
  Automatic MDI Crossover Mode: Enable
  1000Base-T/100Base-TX/10Base-T PHY Extnd Status Register
  Automatic MDI Crossover State: Crossover

<table>
<thead>
<tr>
<th>Mode Control</th>
<th>Indicates whether auto-negotiation is enabled and the selected speed and duplex.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode Status</td>
<td>Displays auto-negotiation fault information. The AutoNegComplete shows True and the LinkStatus field says OK when the interface completes auto-negotiation successfully.</td>
</tr>
<tr>
<td>AutoNegotiation Advertise</td>
<td>Displays the control words advertised by the local interface during negotiation. The duplex can be full-duplex or half-duplex. The &quot;AsymPause&quot; and &quot;SymPause&quot; describes the types of flow control supported by the local interface.</td>
</tr>
<tr>
<td>AutoNegotiation Remote Partner's Ability</td>
<td>Displays the control words advertised by the remote interface during negotiation. The duplex can be full-duplex or half-duplex. The &quot;AsymPause&quot; and &quot;SymPause&quot; fields describe the types of flow control supported by the remote interface.</td>
</tr>
<tr>
<td>AutoNegotiation Expansion</td>
<td>Parallel detection refers to a handshaking scheme in which the link partners continuously transmit an &quot;idle&quot; data packet using the Fast Ethernet MLT-3 waveform. Equipment that does not support auto-negotiation must be configured to exactly match the mode of operation as the link partner, or else no link can be established.</td>
</tr>
</tbody>
</table>
Use the `show hardware interface interface phy` command when you are troubleshooting a link issue, such as when the `show interfaces interface` command is reporting an auto-negotiation mismatch (there is an “Auto-neg Error” string in the output, as shown below.

**Figure 64-11. Auto-negotiation Mismatch Example**

```
FTOS#show interfaces gigabit 0/3
GigabitEthernet 0/3 is up, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:07:16:b3
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto, Mode full duplex, Auto-neg Error
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 04:39:17
[output omitted]
```

The `no auto-negotiation` command disables auto-negotiation on an interface. Dell Networking recommends keeping auto-negotiation enabled.

If the remote interface is not configured for auto-negotiation, the Dell Networking interface can detect the speed at which the remote device is operating by the type of electrical signal that is arriving.

If the local and remote interfaces are configured differently for auto-negotiation—for example, one side is configured for auto-negotiation and the other side is configured for a particular speed—the link does not come up. Both sides of the link must be configured for auto-negotiation (recommended) or else the same speed.

1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting the speed manually to 1000 Mbps.
Advanced ASIC Debugging Commands

- clear hardware unit
- show cpu-interface-stats
- show hardware unit
- show revision

**clear hardware unit**

Clear debugging information on the internal Gigabit Ethernet interfaces on the CSF and FP ASICs.

**Syntax**
```
clear hardware {linecard number | rpm number} unit number counters
```

**Parameters**
- **linecard**
  - Enter the keyword `linecard` to clear information about a line card.
- **rpm**
  - Enter the keyword `rpm` to clear information about an RPM.
- **number**
  - Enter a number:
    - After the keyword `linecard`:
      - Range: 0-7 for the C3000
    - After the keyword `rpm`:
      - Range: 0-1
    - After the `unit` keyword:
      - For a line card: Range: 0 - 3
      - For an RPM: Range 0 - 4

**Defaults**
None.

**Command Mode**
- EXEC
- EXEC Privilege

**Command History**
Version 7.5.1.0 Introduction

**Usage Information**

⚠️ **Warning:** Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

**show cpu-interface-stats**

The command provides an immediate snapshot of the health of the internal RPM and line card CPU. Generally this command is used in concert with Dell Networking Technical Support engineers.

**Syntax**
```
show cpu-interface-stats {cp | lp | rp1 | rp2}
```

**Parameters**
- **cp**
  - Enter the keyword `cp` to display the CP's interface statistics.
- **lp**
  - Enter the keyword `lp` to display the LP’s interface statistics
Defaults
No default behavior or values

Command Modes
EXEC
EXEC Privilege

Command History
Version 7.6.1.0 Introduced on C-Series

Example
Figure 64-12. show cpu-interface-stats lp Command Example (Partial)

FTOS#show cpu-interface-stats lp 1
-- Dataplane PP1 interface statistics --
 Link state : Up
 Recv Interrupts/Polls: 0
 Recv Packets : 9807  Transmit Packets : 9808
...  
-- Dataplane PP0 interface statistics --
 Link state : Up
 Recv Interrupts/Polls: 0
 Recv Packets : 9807  Transmit Packets : 9807
 Recv Desc Error : 0  Transmit Desc Error : 0
...  
-- Partybus RPM0 interface statistics --
 Link state : Up
 Recv Interrupts/Polls: 0
 Recv Packets : 171611  Transmit Packets : 329859
...  
-- Partybus RPM1 interface statistics --
 Link state : Up
 Recv Interrupts/Polls: 0
 Recv Packets : 0  Transmit Packets : 0
 Recv Desc Error : 0  Transmit Desc Error : 0
 Recv Out of Mem : 0  Transmit Out of Mem : 0
 Recv Upper Layer Full: 0  Transmit Pause Pkts : 0
 Recv Other Error : 0  Transmit Other Error : 0
 Recv Restarts : 0
 Recv Restarts Fatal : 0
FTOS#
Example

Figure 64-13.  show cpu-interface-stats cp Command Example (Partial)

FTOS#show cpu-interface-stats cp
  -- Partybus ethernet statistics --
  Link state       : Down
  Recv Interrupts/Polls:  438532
  Recv Packets :   440125  Transmit Packets :   290784 ...
  -- Dataplane ethernet statistics --
  Link state       : Down
  Recv Interrupts/Polls:    9875
  Recv Packets :    9875   Transmit Packets :    9841 ...
  -- OOB ethernet statistics --
  Link state       : Up
  Recv Interrupts/Polls:   15439
  Recv Packets :   19298   Transmit Packets :       11 ...
  -- Partybus switch statistics --
  Dropped cells  : 0
  Dropped packets: 0
  LC0 :  Ingress:         0        Egress:      1780
  LC1 :  Ingress:   331581        Egress:     176297
  CP :  Ingress:    292114        Egress:    440141
  RP1 :  Ingress:   61250        Egress:    66663
  RP2 :  Ingress:   54346        Egress:    59750
  IRC :  Ingress:         0        Egress:      1780
  -- Partybus ethernet rate statistics --
  - 0: Peak rate at Thu Dec 6 18:20:32 2007 -
  Total rate (bps) :   1634400
  Total Size (bytes):      4086
  Total Arp (bytes):   0
  From 127.10.10.23:0  2128 bytes
  From 127.10.10.23:9093    1500 bytes
  From 127.10.10.12:4233    368 bytes
  - 1: Peak rate at Thu Dec 6 18:16:40 2007 -
  Total rate (bps) :   1634400
  Total Size (bytes):      4086
  Total Arp (bytes):   0
  From 127.10.10.23:0  2128 bytes
  From 127.10.10.23:9093    1500 bytes
  From 127.10.10.12:4233    368 bytes
  - 2: Peak rate at Thu Dec 6 18:20:43 2007 -
  Total rate (bps) :   1634400
  Total Size (bytes):      4086
  Total Arp (bytes):   0
  From 127.10.10.23:0  2128 bytes
  From 127.10.10.23:9093    1500 bytes
  From 127.10.10.11:4229    368 bytes
  -- IRC Statistics --
  irc phy: DOWN
  -- Helios Statistics --
  ACL Fpga Cp  dataplane packets:9875 denied:0 dropped:0
  ACL Fpga Rp1 dataplane packets:39125 denied:0 dropped:0
  ACL Fpga Rp2 dataplane packets:274 denied:0 dropped:0
  ACL Fpga Mgmt packets:19441 denied:0 dropped:0
FTOS#
show hardware unit

View advanced debugging information on the internal Gigabit Ethernet interfaces on the CSF and FP ASICS.

Syntax

```
show hardware {linecard number | rpm number} unit number {counters | details | port-stats | register}
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linecard</td>
<td>Enter the keyword <code>linecard</code> to view information about a line card.</td>
</tr>
<tr>
<td>rpm</td>
<td>Enter the keyword <code>rpm</code> to view information about an RPM.</td>
</tr>
<tr>
<td>number</td>
<td>Enter a number after the following keywords: • After the keyword <code>linecard</code>: Range: 0-7 for the C300 • After the keyword <code>rpm</code>: Range: 0-1 • After the keyword <code>unit</code>, enter the number of CSF or FP ASIC.</td>
</tr>
</tbody>
</table>

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

Version 7.5.1.0 Introduction

Usage Information

⚠️ **Warning**: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show revision

Displays the currently loaded FPGA images.

Syntax

```
show revision
```

Defaults

No default behavior or value

Command Modes

- EXEC Privilege

Command History

Version 7.5.1.0 Introduced
Example Figure 64-14. show revision Command Example

FTOS#show revision

-- RPM 0 --
C300 RPM FPGA : 3.8
Required FPGA version : 3.8

-- Secondary RPM --
C300 RPM FPGA : 3.8
Required FPGA version : 3.8

-- Line card 3 --
48 Port 1G LCM FPGA : 2.6
Required FPGA version : 2.6

-- Line card 7 --
48 Port 1G LCM FPGA : 2.6
Required FPGA version : 2.6
FTOS#

ACL and System-Flow Debug Commands

- clear hardware system-flow
- show hardware acl
- show hardware layer3 qos linecard port-set
- show hardware system-flow layer2 linecard port-set

clear hardware system-flow

Clear system-flow entry counters.

Syntax

clear hardware system-flow layer2 linecard number port-set number counters

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter a number after the following keywords:</td>
</tr>
<tr>
<td></td>
<td>• After the keyword <strong>linecard</strong>:</td>
</tr>
<tr>
<td></td>
<td>Range: 0-7 for the C300</td>
</tr>
<tr>
<td></td>
<td>• After the keyword <strong>port-set</strong>, enter the Port-Pipe/FB ID.</td>
</tr>
</tbody>
</table>

Defaults

None.

Command Mode

EXEC

EXEC Privilege

Command History

Version 4.2.1.0 Introduction

Usage Information

**Warning:** Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.
show hardware acl

View Layer 2 or Layer 3 access control list entries.

Syntax

```
show hardware {layer2 | layer 3} acl linecard number port-set number
```

Parameters

- **layer2**
  - Enter the keyword `layer2` to view Layer 2 access control list entries for the specified line card.
- **layer3**
  - Enter the keyword `layer3` to view Layer 3 access control list entries for the Forwarding Processor of the specified line card.
- **number**
  - Enter a number after the following keywords:
    - After the keyword `linecard`:
      - Range: 0-7 for the C300; 0–3 for the C7004/C150
    - After the keyword `port-set`, enter the Port-Pipe/FB ID.

Defaults

None

Command Mode

- EXEC
- EXEC Privilege

Command History

Version 4.2.1.0 Introduction

Warning: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show hardware layer3 qos linecard port-set

View Layer 3 QoS messages.

Syntax

```
show hardware layer3 qos linecard port-set
```

Parameters

- **number**
  - Enter a number after the following keywords:
    - After the keyword `linecard`:
      - Range: 0-7 for the C300
    - After the keyword `port-set`, enter the Port-Pipe/FB ID.

Defaults

None

Command Mode

- EXEC
- EXEC Privilege

Command History

Version 7.5.1.0 Introduction
show hardware system-flow layer2 linecard port-set

View system-flow entries.

**Syntax**

```
show hardware system-flow layer2 linecard number port-set number [counters]
```

**Parameters**

- `number` Enter a number after the following keywords:
  - After the keyword `linecard`:
    - Range: 0-7 for the C300
  - After the keyword `port-set`, enter the Port-Pipe/FB ID.
- `counters` Enter the keyword `counters` to view counters of system-flow entries.

**Defaults**

None.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

Version 4.2.1.0 Introduction

**Usage Information**

⚠️ **Warning**: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

---

**Related Commands**

- `clear hardware system-flow` Clear system-flow entry counters.

---

**Interface Management Debug Commands**

These commands display advanced debugging information related to the Interface Manager (IFM) process.

- `debug ifm trace-flags`
- `show software ifm`
debug ifm trace-flags

Turn on IFM internal trace-flags.

Syntax

depend ifm trace-flags trace-flag

Disable this command using the no debug ifm trace-flags command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trace-flag</td>
<td>Enter a hexadecimal number representing the trace-flag.</td>
</tr>
</tbody>
</table>

Defaults

None.

Command Mode

EXEC
EXEC Privilege

Command History

Version 4.2.1.0 Introduction

Usage Information

Turning on a trace flag does not result in an output to the console/terminal. It prints trace information to the trace buffer, which is viewed using the show trace history command.

⚠️ Warning: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show software ifm

View interface management information.

Syntax

show software ifm {clients [summary] | ifagt number | ifcb interface | linecard number | trace-flags}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clients</td>
<td>(OPTIONAL) Enter the keyword clients to view information on IFM clients.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword summary to view show brief information of IFM clients.</td>
</tr>
<tr>
<td>ifagt</td>
<td>Enter the keyword ifagt to view software pipe and IPC statistics for IFAGT.</td>
</tr>
<tr>
<td>ifcb</td>
<td>Enter the keyword ifcb to view information about the Interface Control Block.</td>
</tr>
<tr>
<td>linecard</td>
<td>Enter the keyword linecard view interface management information for line cards.</td>
</tr>
<tr>
<td>trace-flags</td>
<td>Enter the keyword trace-flags to view interface management information for internal trace flags.</td>
</tr>
</tbody>
</table>
**Layer 2 Debug Command**

**show software macagent**

This command displays tables and advanced debugging information related to the MAC Agent process.

**Syntax**

```
show software macagent {configs | mac-addr-table {dump | count} | port interface interface | port-channel number | stg number | vlan number} line-card number
```

**Parameters**

- `configs`: The keyword `configs` shows the initial configurations of the MAC Agent.
- `mac-addr-table`: The keyword `mac-addr-table` shows the number of MAC addresses in the MAC Agent software.
- `dump`: The keyword `dump` shows the MAC addresses present in the software.

---

**Defaults**

None.

**Command Mode**

EXEC

EXEC Privilege

**Command History**

Version 4.2.1.0 Introduction

**Usage Information**

**Warning**: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.
### Trace Logging Commands

Trace logging is a critical debugging tool most often used by the Dell Networking Technical Assistance Center (TAC) to isolate and resolve both software and hardware issues.

- `debug cpu-traffic-stats`
- `show command-history`
- `show console lp`
- `show cpu-traffic-stats`
- `show hardware linecard fpga`
- `show hardware rpm fpga`

---

<table>
<thead>
<tr>
<th>count</th>
<th>The keyword <strong>count</strong> shows the number of MAC addresses present in the software.</th>
</tr>
</thead>
<tbody>
<tr>
<td>port interface</td>
<td>The keywords <strong>port interface</strong> show Layer 2 information for a port on a particular line card.</td>
</tr>
<tr>
<td>stg</td>
<td>The keyword <strong>stg</strong> shows the state of each port in a particular Spanning Tree Group on a line card.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword <strong>vlan</strong> shows Layer 2 information in the MAC Agent for a VLAN on a particular line card.</td>
</tr>
<tr>
<td>interface</td>
<td>Enter one of the following keywords and slot/port or number information:</td>
</tr>
<tr>
<td></td>
<td>• For a 1-Gigabit Ethernet interface, enter the keyword <strong>GigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 10-Gigabit Ethernet interface, enter the keyword <strong>TenGigabitEthernet</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td></td>
<td>• For a 40-Gigabit Ethernet interface, enter the keyword <strong>fortyGigE</strong> followed by the slot/port information.</td>
</tr>
<tr>
<td>number</td>
<td>Enter a number after the following keywords:</td>
</tr>
<tr>
<td></td>
<td>• After the keyword <strong>linecard</strong>:</td>
</tr>
<tr>
<td></td>
<td>Range: 0-7 for the C300; 0-3 for the C7004/C150</td>
</tr>
<tr>
<td></td>
<td>• After the <strong>port-channel</strong> keyword, enter the port-channel number.</td>
</tr>
<tr>
<td></td>
<td>Range: 1-128</td>
</tr>
<tr>
<td></td>
<td>• After the keyword <strong>stg</strong>, enter the Spanning Tree Group number.</td>
</tr>
<tr>
<td></td>
<td>• After the keyword <strong>vlan</strong>:</td>
</tr>
<tr>
<td></td>
<td>Range: 1 - 4095 for the C300</td>
</tr>
</tbody>
</table>

**Defaults** None.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- **Version 8.4.6.0**: Added support for the keyword **fortyGigE**.
- **Version 4.2.1.0**: Introduction

**Usage Information**

⚠️ **Warning**: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.
**debug cpu-traffic-stats**

Enable the collection of CPU traffic statistics.

**Syntax**

```
debug cpu-traffic-stats [linecard [all | number]]
```

To disable debugging, execute the `no debug cpu-traffic-stats` command.

**Parameters**

- `linecard` (OPTIONAL) Enter the keyword `linecard` to view CPU traffic statistics for a particular line card.
- `all` Enter the keyword `all` to specify all line cards.
- `number` Enter a line card number
  
  Range: 0-7 for the C300

**Defaults**

Disabled

**Command Modes**

EXEC Privilege

**Command History**

- **Version 4.2.1.0** Introduced

**Usage Information**

This command can be used to turn on CPU traffic statistics collection either on a specific linecard or on all linecards. The statistics currently collected are:

- Numbers of packets trapped due to Egress MTU violation
- Numbers of packets trapped due to TTL 1 or IP Options
- Numbers of packets trapped due to TTL 0

**Note:** Use `show cpu-traffic-stats` to view traffic statistics.

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 will automatically turn on the collection of CPU traffic statistics. The message is an indication that collection of CPU traffic is automatically turned on:

```
Excessive traffic is received by CPU and traffic will be rate controlled.
```

**Note:** This command must be enabled before the `show cpu-traffic-stats` command will display traffic statistics. Dell Networking recommends that you disable debugging (`no debug cpu-traffic-stats`) once troubleshooting is complete.

**Related Commands**

- `show cpu-traffic-stats` Display CPU traffic statistics.

---

**show command-history**

View a buffered time-stamped log of all commands entered by all users.

**Syntax**

```
show command-history
```

**Parameters**

None

**Defaults**

None
show console lp
View the buffered console log for a line card.

Syntax
```
show console lp number
```

Parameters
- `lp` Enter the keyword `lp` to view buffered console messages for a line card processor.
- `number` Enter a line card number.
  Range: 0-7 for the C300; 0-3 for the C7004/C150

Defaults
None

Command Mode
- EXEC
- EXEC Privilege

Usage Information
This log displays initialization messages while the line card is going through the steps to reach check-in status.

show cpu-traffic-stats
View traffic statistics for a line card CPU.

Syntax
```
show cpu-traffic-stats [linecard {all | number}]
```

Parameters
- `linecard` (OPTIONAL) Enter the keyword `linecard` to view CPU traffic statistics for a particular line card.
- `all` Enter the keyword `all` to specify all line cards.
- `number` Enter a line card number
  Range: 0-7 for the C300; 0-3 for the C7004/C150

Defaults
None

Command Mode
- EXEC
- EXEC Privilege
show hardware linecard fpga

Display internal information about the line card FPGA.

Syntax

show hardware linecard slot fpga {errorlog | registers | stats}

Parameters

- **slot**
  - Enter the line card slot number.
  - Range: 0 to 7
- **errorlog**
  - (OPTIONAL) Enter the keyword errorlog to dump the FPGA Error Log.
- **registers**
  - (OPTIONAL) Enter the keyword registers to dump the FPGA Registers.
- **stats**
  - (OPTIONAL) Enter the keyword stats to dump the FPGA Interrupt Statistics.

Defaults

No default behavior or values

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 7.5.1.0 Introduced

Usage Information

- **Warning**: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show hardware rpm fpga

Display internal RPM FPGA information.

Syntax

show hardware rpm slot fpga {errorlog | linecard {slot registers} | registers | stats | standby-rpm registers}
Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>rpm slot</strong></td>
<td>Enter the keyword <strong>rpm</strong> followed by the RPM slot number. Range: 0 or 1</td>
</tr>
<tr>
<td><strong>errorlog</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>errorlog</strong> to dump the FPGA Error Log.</td>
</tr>
<tr>
<td><strong>linecard slot registers</strong></td>
<td>Enter the keyword <strong>linecard</strong> followed by the line card slot number and the keyword <strong>registers</strong> to dump the line card’s FPGA registers. Range: 0-7 for the C300; 0-3 for the C7004/C150</td>
</tr>
<tr>
<td><strong>registers</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>registers</strong> to dump the FPGA registers.</td>
</tr>
<tr>
<td><strong>stats</strong></td>
<td>(OPTIONAL) Enter the keyword <strong>stats</strong> to dump the FPGA Interrupt Statistics.</td>
</tr>
<tr>
<td><strong>standby-rpm register</strong></td>
<td>(OPTIONAL) Enter the keywords <strong>standby-rpm register</strong> to display the stand-by RPMs registers.</td>
</tr>
</tbody>
</table>

Defaults
No default behavior or values

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Added support for Stand-by RPM Registers</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

⚠️ **Warning:** Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Example

**Figure 64-16. show hardware rpm fpga registers (C-Series Command Example)**

```
FTOS>show hardware rpm 0 fpga registers
***************************************************
Local Memory Dump
0x0000: 00010401 5a5a1234 01200b11 00000111 00000011 0000001f 000003ff 00000000
0x0020: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0040: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0060: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0080: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x00a0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x00c0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x00e0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0100: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0120: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0140: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0160: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0180: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x01a0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x01c0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x01e0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0200: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0220: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0240: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0260: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
FTOS>
```
Example Figure 64-17. show hardware rpm fpga stats (C-Series Command Example)

orcel0#show hardware rpm 1 fpga stats

DUMPING FPGA INTERRUPT STATISTICS

FAN Interrupts received - 0
PSU Interrupts received - 0
Card Presence Interrupts received - 0
I2C[0] Interrupts received - 0
I2C[0] Interrupts handled - 0
I2C[1] Interrupts received - 337
I2C[1] Interrupts handled - 337
I2C[2] Interrupts received - 0
I2C[2] Interrupts handled - 0
I2C[3] Interrupts received - 1209
...
I2C[7] Interrupts handled - 0
HDLC[0] Interrupts received - 0
HDLC[0] Interrupts handled - 0
HDLC[1] Interrupts received - 0
HDLC[1] Interrupts handled - 0
HDLC[2] Interrupts received - 0
HDLC[2] Interrupts handled - 0
...
HDLC[6] Interrupts handled - 0
SPI Interrupts received - 0
SMI Write Interrupts received - 0
LM 80 Interrupts received - 0
LCLK Interrupts received - 0
Mastership change Interrupts received - 1
Over temperature Interrupts received - 0
Low temperature Interrupts received - 0
XFP[0] Interrupts received - 0
XFP[1] Interrupts received - 0
XFP[2] Interrupts received - 0
XFP[3] Interrupts received - 0
XFP[4] Interrupts received - 0
XFP[5] Interrupts received - 0
XFP[6] Interrupts received - 0
XFP[7] Interrupts received - 0
POE[0] Interrupts received - 0
POE[1] Interrupts received - 0
POE[2] Interrupts received - 0
POE[3] Interrupts received - 0
PCI Reset Interrupts received - 0
Spurious interrupts received - 0
FTOS>
Offline Diagnostic Commands

The commands in this section are:

• diag linecard
• offline
• online
• show diag

The offline diagnostics test suite is useful for isolating faults and debugging hardware. The tests results are written to a file in flash memory and can be displayed on screen. Detailed statistics for all tests are collected. These statistics include:

• last execution time
• first and last test pass time
• first and last test failure time
• total run count
• total failure count
• consecutive failure count
• error code

### diag linecard

Run offline diagnostics on a line card.

**Syntax**

```plaintext
diag linecard number {alllevels | level0 | level1 | level2}
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alllevels</td>
<td>Enter the keyword <strong>alllevels</strong> to run the complete diagnostics test suite.</td>
</tr>
<tr>
<td>level0</td>
<td>Enter the keyword <strong>level0</strong> to check the device inventory and verify the existence of the devices (e.g., device ID test).</td>
</tr>
<tr>
<td>level1</td>
<td>Enter the keyword <strong>level1</strong> to verify that the devices are accessible via the designated paths (e.g., line integrity tests) and test the internal parts (e.g., registers) of the devices.</td>
</tr>
<tr>
<td>level2</td>
<td>Enter the keyword <strong>level2</strong> to perform on-board loopback tests on various data paths (e.g., data Port-Pipe and Ethernet).</td>
</tr>
<tr>
<td>number</td>
<td>Enter a number: Range: 0-7 for the C300; 0-3 for the C7004/C150</td>
</tr>
</tbody>
</table>

**Defaults**

None.

**Command Mode**

EXEC

EXEC Privilege

**Command History**

- **Version 7.5.1.0**  Introduction

**Usage Information**

⚠️ **Warning:** Do not use this command when a line card is in a booting state.
**offline**

Place a line card or SFM in an offline state.

**Syntax**

```
offline {linecard number | sfm standby}
```

**Parameters**

- **linecard**
  - Enter the keyword `linecard` to place the linecard in an offline state.

- **sfm standby**
  - Enter the keywords `sfm standby` to place the RPM in an offline state.

- **number**
  - After the keyword `linecard`:
    - Range: 0-7 for the C300

**Defaults**

None.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- **Version 7.5.1.0**
  - Introduction

**Usage Information**

- **Warning:** Do not use this command when a line card is in a booting state.

---

**online**

Place a linecard or RPM in an online state.

**Syntax**

```
online {linecard number | sfm standby}
```

**Parameters**

- **linecard**
  - Enter the keyword `linecard` to place the linecard in an online state.

- **sfm standby**
  - Enter the keywords `sfm standby` to place the RPM in an online state.

- **number**
  - After the keyword `linecard`:
    - Range: 0-7 for the C300; 0-3 for the C7004/C150

**Defaults**

None.

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- **Version 7.5.1.0**
  - Introduction

**Usage Information**

- **Warning:** Do not use this command when a line card is in a booting state.
show diag

View diagnostics information.

Syntax

```
show diag {information | linecard number | summary | detail}
```

Parameters

- **information**
  - Enter the keyword `information` to view diagnostics processes by line card.
- **linecard**
  - Enter the keyword `linecard` for diagnostics information for a particular line card.
- **number**
  - Enter a line card number.
  - Range: 0-7 for the C300
- **summary**
  - Enter the keyword `summary` for brief diagnostics information.
- **detail**
  - Enter the keyword `detail` for detailed diagnostics information.

Defaults

None.

Command Mode

- EXEC
- EXEC Privilege

Command History

- Version 7.5.1.0 Introduced
- Version 7.7.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series

Usage Information

⚠️ **Warning:** Do not use this command when a line card is in a booting state.

PoE Hardware Status Commands

Inspect C-Series line card internal commands with regard to Power over Ethernet (PoE).

show hardware linecard poe-status

Display the status of the four C-Series PoE controllers and the entire registers associated with each controller.

Syntax

```
show hardware linecard number poe-status
```

Parameters

- **linecard number**
  - Enter the keyword `linecard` followed by the line card slot number.

Defaults

No default behavior or values

Command Modes

- EXEC

Command History

- Version 7.7.1.0 Introduced on S-Series
- Version 7.5.1.0 Introduced on C-Series
Example Figure 64-18. show hardware linecard (C-Series Command Example)

```text
FTOS#show hardware linecard 7 poe-status
HW Status for POE Controller 0
The HW Status is
----------------
The Internal address is - 0x0000
The I2C address is - w005c
Is Master - Yes
The I2C Mode is - I2C
The mode is configured properly
The address is configured properly
The Controller and I2C is configured properly
FTOS#
```

Usage Information If the command is executed on a non-POE line card, the following error message is generated:

```text
FTOS#sh hardware linecard 6 poe-status
% Error: POE is not supported for this card.
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show power supply</td>
<td>Display the power supply status.</td>
</tr>
</tbody>
</table>

Buffer Tuning Commands

The buffer tuning commands are:

- `buffer (Buffer Profile)`
- `buffer (Configuration)`
- `buffer-profile (Configuration)`
- `buffer-profile (Interface)`
- `show buffer-profile`
- `show buffer-profile interface`

⚠️ Warning: Altering the buffer allocations is a sensitive operation. Do not use any buffer tuning commands without first contacting the Dell Networking Technical Assistance Center.

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 | packet-pointers] queue0 number queue1 number queue2 number queue3 number
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dedicated</code></td>
<td>Enter this keyword to configure the amount of dedicated buffer space per queue.</td>
</tr>
<tr>
<td><code>dynamic</code></td>
<td>Enter this keyword to configure the amount of dynamic buffer space per Field Processor.</td>
</tr>
<tr>
<td><code>packet-pointers</code></td>
<td>Enter this keyword to configure the number of packet pointers per queue.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced on</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7.1.0</td>
<td>S-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>C-Series</td>
</tr>
</tbody>
</table>

Related Commands

Buffer-profile (Configuration) Create 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.

Syntax
buffer [csf | fp-uplink] linecard slot port-set port-pipe buffer-policy buffer-profile

Parameters

- csf
  Enter this keyword to apply a buffer profile to all Switch Fabric processors in a port-pipe.

- fp-uplink
  Enter this keyword to apply a buffer profile to all Field Processors in a port-pipe.
buffer-profile (Configuration)  Create a buffer profile that can be applied to an interface.

### Syntax

```
buffer-profile { { fp | csf } profile-name | global { 1Q | 4Q } }
```

### Parameters

- **fp**
  - Enter this keyword to create a buffer profile for the Field Processor.

- **csf**
  - Enter this keyword to create a buffer profile for the Switch Fabric Processor.

- **profile-name**
  - Create a name for the buffer profile.

- **global**
  - Apply one of two pre-defined buffer profiles to all of the port-pipes in the system.

- **1Q**
  - Enter this keyword to choose a pre-defined buffer profile for single queue (i.e non-QoS) applications.

- **4Q**
  - Enter this keyword to choose a pre-defined buffer profile for four queue (i.e QoS) applications.

### Defaults

```
global 4Q
```

### Command Mode

CONFIGURATION

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.8.1.0</td>
<td>Added <em>global</em> keyword.</td>
</tr>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>
When you remove a buffer-profile using the command `no buffer-profile [fp | csf]` 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] linecard port-set buffer-policy` from CONFIGURATION mode and `no buffer-policy` from INTERFACE mode.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>buffer</code> (Buffer Profile)</td>
<td>Allocate an amount of dedicated buffer space, dynamic buffer space, or packet pointers to queues 0 to 3.</td>
</tr>
<tr>
<td><code>reload</code></td>
<td>Reboot the system.</td>
</tr>
</tbody>
</table>

### Usage Information

The `buffer-profile global` command fails if you have already applied a custom buffer-profile on an interface. Similarly, when `buffer-profile global` is configured, you cannot apply buffer-profile on any interface.

If the default buffer-profile (4Q) is active, Dell Networking OS displays an error message instructing you to remove the default configuration using the command `no buffer-profile global`. You must reload the system for the global buffer-profile to take effect.

**Note:** When you removed a buffer-profile using the command `no buffer-profile [fp | csf]` 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 output using the command `no buffer [fp | csf] linecard port-set buffer-policy` from CONFIGURATION mode.

### buffer-profile (Interface)

**Apply a buffer profile to an interface.**

**Syntax**

`buffer-profile profile-name`

**Parameters**

- `profile-name` Enter the name of the buffer profile you want to apply to the interface.

**Defaults**

None

**Command Mode**

INTERFACE

**Command History**

- Version 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series

**Usage Information**

When you move to a different chassis a line card that has a buffer profile applied at interface level on the fp-uplink, the line card retains the buffer profile. To return the line card to the default buffer profile, remove the current profile using the command `no buffer-profile fp-uplink linecard` from INTERFACE mode, and then reload the chassis.

**Related Commands**

- `buffer-profile (Configuration)` Create a buffer profile that can be applied to an interface.
show buffer-profile

Display the buffer profile that is applied to an interface.

Syntax

```
show buffer-profile {detail | summary} {csf | fp-uplink}
```

Parameters

- **detail**: Display the buffer allocations of the applied buffer profiles.
- **summary**: Display the buffer-profiles that are applied to line card port-pipes in the system.
- **csf**: Display the Switch Fabric Processor buffer profiles that you have applied to line card port-pipes in the system.
- **fp-uplink**: Display the Field Processor buffer profiles that you have applied to line card port-pipes in the system.

Defaults
None

Command Mode

`INTERFACE`

Command History

- **Version 7.7.1.0**: Introduced on S-Series
- **Version 7.6.1.0**: Introduced on C-Series

Example

```
Figure 64-19. show buffer-profile Command Example

FTOS#show buffer-profile summary fp-uplink
Linecard Port-set Buffer-profile
0 0 test1
4 0 test2
FTOS#
```

Related Commands

- `buffer-profile (Configuration)` Create a buffer profile that can be applied to an interface.

show buffer-profile interface

Display the buffer profile that is applied to an interface.

Syntax

```
show buffer-profile {detail | summary} interface interface slot/port
```

Parameters

- **detail**: Display the buffer allocations of a buffer profile.
- **summary**: Display the Field Processors and Switch Fabric Processors that are applied to line card port-pipes in the system.
- **interface**: Enter the keyword `interface` followed by the interface type, `gigabitethernet` or `tengigabitethernet` or `fortyGigE`.
- **slot/port**: Enter the slot and port number of the interface.

Defaults
None

Command Mode

`INTERFACE`
Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Added support for the keyword fortyGigE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 7.7.1.0</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>Version 7.6.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

Example

**Figure 64-20. show buffer-profile interface Command Example**

```
FTOS#show buffer-profile detail csf linecard 4 port-set 0
Linecard 4 Port-set 0
Buffer-profile test
  Queue#  Dedicated Buffer (Bytes)  Buffer Packets
  0       36960                    718
  1       18560                    358
  2       18560                    358
  3       18560                    358
  4       9600                     64
  5       9600                     64
  6       9600                     64
  7       9600                     63
FTOS#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buffer-profile (Configuration)</td>
<td>Create a buffer profile that can be applied to an interface.</td>
</tr>
</tbody>
</table>
E-Series Debugging and Diagnostics

Overview

Dell Networking OS supports an extensive suite of protocol-specific debug commands for packet- and event-level debugging. These commands are described throughout this document. In addition, Dell Networking OS supports commands for diagnosing suspected hardware issues.

This chapter contains the following sections:

- Diagnostics and Monitoring Commands
- Offline Diagnostic Commands
- Hardware Commands

Diagnostics and Monitoring Commands

The diagnostics and monitoring commands are:

- dataplane-diag disable loopback
- dataplane-diag disable sfm-bringdown
- dataplane-diag disable sfm-walk
- dataplane-diag disable dfo-reporting
- diag linecard
- diag sfm
- ip control-plane egress-filter-traffic
- ipv6 control-plane egress-filter-traffic
- logging coredump kernel disable
- logging coredump kernel server
- logging coredump linecard
- power-off/on sfm
- reset linecard
- reset sfm
- show command-history
- show console
- show diag sfm
- show processes ipc
- show processes ipc
- show processes ipc flow-control
- show revision
In addition to these debug commands, Dell Networking OS supports diagnostics, monitoring, and fault isolation commands to assist in gathering information.

**Important Points to Remember**

- Unless otherwise noted, these commands are available on TeraScale systems only.
- The trace-log file captures failure information on most failure events.
- The RPM-SFM runtime loopback test failure initiates an SFM walk. The system automatically places each SFM (in sequential order) in an offline state, runs the loopback test, and then places the SFM back in an active state. This continues until the system determines a working SFM combination. If no working combination is found, the system restores to the pre-walking SFM state.
- If the line card runtime loopback test fails, the system does not launch an SFM walk.

>Note: SFM walking assumes a chassis with the maximum number of SFMs in an active state.

**dataplane-diag disable loopback**

Disable the runtime loopback test on the primary RPM and line cards.

**Syntax**

`dataplane-diag disable loopback`

To re-enable, use the `no dataplane-diag disable loopback` command.

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

Version 6.5.4.0 Introduced

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diag sfm</code></td>
<td>Display the loopback test results</td>
</tr>
<tr>
<td><code>dataplane-diag disable sfm-bringdown</code></td>
<td>Disable the automatic SFM bringdown</td>
</tr>
<tr>
<td><code>dataplane-diag disable sfm-walk</code></td>
<td>Disable the automatic SFM walk</td>
</tr>
</tbody>
</table>
The runtime dataplane loopback test, by default, runs in the background. Every 10 seconds, the primary RPM and each line card sends packets through the SFMs and back again (loopback) to monitor the overall health status of the dataplane at a system level. This command disables that automatic runtime loopback test. Execute the `show diag sfm` command to view the diagnostics results (see Figure 65-1).

Note: Only the Primary RPM can perform runtime dataplane loopback test.

```
Figure 65-1. show diag sfm Command Example

FTOS#show diag sfm
Switch Fabric Module Loopback Test: enabled
SFM Walk-Through in Loopback Test: enabled
SFM Bring-Down in Loopback Test: enabled
Switch Fabric Module Loopback State: on

-- Route Processor Modules --
Slot Test Status Last Result Time Stamp
-----------------------------------------------
0 off none
1 on pass Feb 16 2007 15:50:26

-- Line cards --
Slot Test Status Last Result Time Stamp
-----------------------------------------------
0 off none
1 off none
2 on pass Feb 16 2007 15:50:26
3 off none
4 on pass Feb 16 2007 15:50:26
5 off none
6 off none
FTOS#
```

dataplane-diag disable sfm-bringdown

Disable the automatic bring down of the single faulty SFM identified by the SFM walk during the RPM-SFM runtime loopback test.

**Syntax**

`dataplane-diag disable sfm-bringdown`

To re-enable the automatic SFM bring down, use the `no dataplane-diag disable sfm-bringdown` command.

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.4.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Information**

If a full set of SFMs are online during the runtime loopback test and a failure occurs, an automatic SFM walk is launched in an attempt to determine if the failure is due to a single faulty SFM. If confirmed, the single faulty SFM is identified and disabled by default. This command disables the automatic bring down of that suspect SFM.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dataplane-diag disable loopback</code></td>
<td>Disable the runtime dataplane loopback test</td>
</tr>
</tbody>
</table>
**dataplane-diag disable sfm-walk**

Disable the automatic SFM walk that is launched after an RPM-SFM runtime loopback test failure.

**Syntax**

dataplane-diag disable sfm-walk

To re-enable the automatic SFM walk, use the `no dataplane-diag disable sfm-walk` command.

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

| Version 6.5.4.0 | Introduced |

**Usage Information**

If a full set of SFMs are online during the runtime loopback test and a failure occurs, an automatic SFM walk is launched in an attempt to determine if the failure is due to a faulty SFM. This command disables the automatic SFM walk.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dataplane-diag disable loopback</td>
<td>Disable the runtime dataplane loopback test</td>
</tr>
<tr>
<td>dataplane-diag disable sfm-bringdown</td>
<td>Disable the automatic SFM bringdown.</td>
</tr>
<tr>
<td>show diag sfm</td>
<td>Display the loopback test results</td>
</tr>
</tbody>
</table>

**dataplane-diag disable dfo-reporting**

Disable the per-channel DFO (deskew FIFO overflow) reporting via event logging.

**Syntax**

dataplane-diag disable dfo-reporting

To re-enable, use the `no dataplane-diag disable dfo-reporting` command.

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

| Version 6.5.4.0 | Introduced |

**Usage Information**

The per-channel DFO error reporting via event logging is enabled by default on TeraScale chassis. The error reporting issues a warning when a temporary dataplane glitch occurs or when a persistent malfunction is detected.

When a DFO error is detected, no automatic action is initiated by the system. The message issued is similar to:

%RPM1-P:CP %CHMGR-2-SFM_PCDFO: PCDFO error detected for SFM4

This command disables the per-channel DFO reporting.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diag sfm</td>
<td>Initiate a manual dataplane loopback test.</td>
</tr>
<tr>
<td>show diag sfm</td>
<td>Display the loopback test results</td>
</tr>
</tbody>
</table>

Note: This command is not supported on the E600i chassis.

diag linecard

Run a diagnosis on a linecard.

Syntax

diag linecard [slot] [alllevels | level0 | level1 | level2 | terminate]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>Enter the slot number of the card you with to diagnose.</td>
</tr>
<tr>
<td>alllevels</td>
<td>level0</td>
</tr>
<tr>
<td>terminate</td>
<td>Enter the keyword terminate to stop the test</td>
</tr>
</tbody>
</table>

Defaults

Level 0-2

Command Modes

EXEC Privilege

Command History

Version 6.5.4.0 Introduced

Related Commands

reset linecard Reset the line card and bring it back online.

diag sfm

Execute a manual dataplane loopback test.

Syntax

diag sfm [all-loopback | rpm-loopback]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-loopback</td>
<td>(OPTIONAL) Enter the keyword all-loopback to execute a dataplane loopback test from the RPMs and all line cards.</td>
</tr>
<tr>
<td>rpm-loopback</td>
<td>(OPTIONAL) Enter the keyword rpm-loopback to execute a dataplane loopback test on the RPMs only.</td>
</tr>
</tbody>
</table>

Defaults

No default behavior or value

Command Modes

EXEC Privilege

Command History

Version 6.5.4.0 Introduced

Usage Information

If the RPM-SFM or line card-SFM loopback test detects an SFM failure, an attempt is made to isolate a single faulty SFM by automatically walking the SFMs. For this failure case, error messages similar to the runtime loopback test error are generated.
If the test passes when the switch fabric is down and there are at least \((\text{max}-1)\) SFMs in the chassis, then the system will bring the switch fabric back up automatically. Like the runtime loopback test, the manual loopback test failure will not bring the switch fabric down.

**Note:** Line card-SFM loopback test failure, during the manual test, will trigger an SFM walk.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset sfm</td>
<td>Reset the SFM and bring it back online.</td>
</tr>
</tbody>
</table>

### ip control-plane egress-filter-traffic

Apply Layer 3 egress ACLs to the CPU generated traffic.

**Syntax**

```
ip control-plane egress-filter-traffic
```

To disable, use the `no ip control-plane egress-filter-traffic` command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series only</td>
</tr>
</tbody>
</table>

**Usage Information**

CPU ACLs are useful for troubleshooting packet flow that has bypassed the hardware-based distributed forwarding path and is traveling directly to the RPM CPU. This command is useful in debugging the CPU originated control traffic. You can use the egress ACL with count option to verify if the control traffic sent by the CPU made it to the line card egress or not.

Using permit rules with the count option, you can track, on a per-flow basis, whether CPU-generated packets were transmitted successfully. In addition, you can block certain CPU-generated and soft-forwarded traffic.

This feature also allows you to configure an extended ACL that matches ICMP packets using the count option, apply the ACL to an egress physical interface, and then ping through that interface to the remote device.

**Note:** Only Layer 3 traffic goes through the ACL—i.e. BPDUs will not be captured.

### ipv6 control-plane egress-filter-traffic

Apply Layer 3 egress ACLs to the CPU generated traffic.

**Syntax**

```
ipv6 control-plane egress-filter-traffic
```

To disable, use the `no ipv6 control-plane egress-filter-traffic` command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION
CPU ACLs are useful for troubleshooting packet flow that has bypassed the hardware-based distributed forwarding path and is traveling directly to the RPM CPU. This command is useful in debugging the CPU originated control traffic. You can use the egress ACL with count option to verify if the control traffic sent by the CPU made it to the line card egress or not.

Using permit rules with the count option, you can track, on a per-flow basis, whether CPU-generated packets were transmitted successfully. In addition, you can block certain CPU-generated and soft-forwarded traffic.

This feature also allows you to configure an extended ACL that matches ICMP packets using the count option, apply the ACL to an egress physical interface, and then ping through that interface to the remote device.

Note: Only Layer 3 traffic goes through the ACL—i.e. BPDUs will not be captured.

logging coredump kernel disable

Disables kernel core-dump logging to the CORE_DUMP_DIR on the flash.

Syntax

[no] logging coredump kernel disable

To re-enable kernel core-dump logging (return to the default), use the no logging coredump kernel disable command.

Defaults

Enabled (core-dump logging is enabled)

Command Modes

CONFIGURATION

Usage

By default, the kernel core-dump is enable and stored in the flash directory:

- Storage Directory Name: flash:CORE_DUMP_DIR
  - Kernel core-dump naming convention is: f10rpProcessorID.kcore.gz
    For example: F10rp1.kcore.gz
  - Application core-dump naming convention is:
    rpProcessorID_ApplicationName_timestamp.core.gz
    For example: rp1_ospf_060307172608.core.gz
- Multiple core-dumps
  - Application core-dumps are timestamp embedded and are not overwritten by default. Manually delete the older core-dumps to allow more space on the flash.
  - Kernel core-dumps are overwritten whenever there is a new core-dump.
Should a crash occur, the large crash kernel file may take more than ten minutes to upload and may require more space on the flash than is available. The HA module is aware of a core-dump in process and will wait until the upload is complete before rebooting the RPM.

**Note:** Application core-dumps are also automatically uploaded to flash. If there is not enough available space for the kernel core-dump on the flash, the kernel upload will terminate.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>logging coredump linecard</code></td>
<td>Enable core-dump logging on line cards</td>
</tr>
<tr>
<td><code>logging coredump kernel server</code></td>
<td>Save core-dump logging files to an alternate server</td>
</tr>
</tbody>
</table>

### logging coredump kernel server

**Description:** Designate the logging core-dump files to be saved to a remote server rather than flash.

**Syntax:**

```plaintext
logging coredump kernel server
```

**To save the logging core-dump files to flash (the default), use the**

```plaintext
no logging coredump kernel server
```

**Defaults:** Saved on flash

**Command Modes:** CONFIGURATION

**Command History:**

- **Version 6.5.4.0** Introduced

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>logging coredump linecard</code></td>
<td>Enable core-dump logging on line cards</td>
</tr>
<tr>
<td><code>logging coredump kernel disable</code></td>
<td>Disable kernel core-dump logging</td>
</tr>
</tbody>
</table>

### logging coredump linecard

**Description:** Enable line card core-dump logging on a specific line card or on all line cards.

**Syntax:**

```plaintext
logging coredump linecard {slot_number [port-shutdown | no-port-shutdown] | all}
```

**To disable line card core-dump logging, use the**

```plaintext
no logging coredump linecard [slot_number | all]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linecard slot number</td>
<td>Enter the keyword <code>linecard</code> followed by the slot number to enable core-dump logging line card details. Range: 0 to 13 on the E1200; 0 on 6 for E600/E600i, and 0 to 5 on the E300.</td>
</tr>
<tr>
<td>port-shutdown</td>
<td>Enter the keyword <code>port-shutdown</code> to configure the system to shutdown the physical interfaces during a software exception and the subsequent core dump.</td>
</tr>
<tr>
<td>no-port-shutdown</td>
<td>Enter the keyword <code>no-port-shutdown</code> to configure the system so that the physical interfaces remain up during a software exception and the subsequent core dump. This is an “undo” feature for the <code>port-shutdown</code> option.</td>
</tr>
<tr>
<td>linecard all</td>
<td>Enter the keyword <code>linecard all</code> to enable core-dump logging details on all line cards.</td>
</tr>
</tbody>
</table>
Defaults
Disabled (core-dump logging is off)

Command Modes
CONFIGURATION

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced the port-shutdown and no-port-shutdown variables</td>
</tr>
<tr>
<td>6.5.4.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information
The line card core-dump is stored on flash in a directory:

- Storage Directory Name: \texttt{flash:CORE\_DUMP\_DIR}
- Line Card core-dump naming convention is: \texttt{f10lpSlot\_Number.core.gz}

For example: \texttt{f10lp6.core.gz}

- Multiple core-dumps
  - If multiple line cards crash, the core-dump files will upload simultaneously. However, a second core-dump from the same line card slot will overwrite the first core-dump.
  - During a line card core-dump, the line card interface remains up while the core-dump is being written to the directory. Use the \texttt{port-shutdown} option to shutdown the physical interfaces during the core dump, allowing for a failover to a backup system.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging coredump kernel server</td>
<td>Save core-dump logging files to an alternate server.</td>
</tr>
<tr>
<td>logging coredump kernel disable</td>
<td>Disable kernel core-dump logging.</td>
</tr>
</tbody>
</table>

**power on/off linecard**

Power on or off a specified line card.

Syntax

```
power-{off | on} linecard slot-number
```

Parameters

- \texttt{power-off} Enter the keyword \texttt{power-off} to power off the SFM.
- \texttt{power-on} Enter the keyword \texttt{power-on} to power on the SFM
- \texttt{sfm slot-number} Enter the keyword \texttt{linecard} followed by the slot number of the SFM to power on/off.
  
  Range: 0 to 6

Defaults
No default values or behavior

Command Modes
EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.4.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show linecard</td>
<td>Display the current line card status.</td>
</tr>
</tbody>
</table>
### power-off/on sfm

**Purpose:**
Power on or off a specified SFM.

**Syntax:**
```
power-\{off | on\} sfm slot-number
```

**Parameters**

- **power-off**
  - Enter the keyword `power-off` to power off the SFM.

- **power-on**
  - Enter the keyword `power-on` to power on the SFM

- **sfm slot-number**
  - Enter the keyword `sfm` followed by the slot number of the SFM to power on/off.
  
  *Range: 0 to 7*

**Defaults**
No default values or behavior

**Command Modes**
EXEC

**Command History**

- Version 6.5.4.0 Introduced

**Usage Information**
This command is used for diagnostic purposes to isolate and identify a failed SFM when troubleshooting issues related to the chassis dataplane.

**Note:** Execute this command only during an offline diagnostics; this command may bring down the switch fabric.

When there are a full set of SFMs online, powering down one SFM will reduce the total bandwidth supported by the chassis, and may affect data flow. A warning message is issued at the command line that requires user confirmation to proceed with the command (Figure 65-2).

**Example**

**Figure 65-2. power-off sfm Command Example with Data Traffic Warning Message**

```
FTOS#power-off sfm 0
SFM0 is active. Powering it off it might impact the data traffic.
Proceed with power-off [confirm yes/no]:yes
Feb 15 23:52:53: %RPM1-P:CP %CHMGR-2-MINOR_SFM: Minor alarm: only eight working SFM
FTOS#
```

Since this command is for diagnostic purposes, you can power off more than one SFM causing a switch fabric module to go down. A warning message is issued at the command line and requires user confirmation to proceed with the command (Figure 65-3).

**Example**

**Figure 65-3. power-off sfm Command Example with Switch Fabric Down Warning Message**

```
FTOS#power-off sfm 1
WARNING!! SFM1 is active. Powering it off it will cause Switch Fabric to go down!!
Proceed with power-off [confirm yes/no]:yes
Feb 16 00:03:19: %RPM1-P:CP %CHMGR-2-MINOR_SFM: Minor alarm: only eight working SFM
FTOS#
```

**Example**

Once the SFM is powered off, the SFM status indicates that the SFM has been powered off by the user. Use the `show sfm all` command to display the status (Figure 65-4).
Example

Figure 65-4. show sfm all Command Example

```
FTOS#show sfm all
Switch Fabric State: down (Not enough working SFMs)
Switch Mode: SFM
-- Switch Fabric Modules --
Slot Status
--------------------------------------------------------------------------------
 0   power off            (SFM powered off by user)
 1   power off            (SFM powered off by user)
 2   power off            (SFM powered off by user)
 3   active
 4   active
 5   active

FTOS#
```

Related Commands

show sfm  Display the current SFM status.

show command-history

Display the trace command history log.

Syntax

```
show command-history line number
```

Parameters

```
line number  (OPTIONAL) Enter the number of the most recent command history lines (commands).
For example, if you want to view the most recent ten command, enter the number 10.
```

Defaults

No default behaviors or values

Command Modes

EXEC

Command History

Version 7.4.1.0  Introduced

Example

Figure 65-5. show command-history Command Example

```
exce10#show command-history 15
[1/15 14:59:27]: CMD-(CLI):[enable]by default from console
[1/15 15:9:15]: CMD-(CLI):[show linecard all]by default from console
[1/15 15:9:28]: CMD-(CLI):[interface gigabitethernet 12/0]by default from console
[1/15 15:11:51]: CMD-(CLI):[show startup-config]by default from console
[1/15 15:24:24]: CMD-(TEL46):[enable]by admin from vty0 (peer RPM)
[1/15 15:24:39]: CMD-(TEL46):[show version]by admin from vty0 (peer RPM)
[1/15 15:25:23]: CMD-(TEL46):[show interfaces managementethernet 1]by admin from vty0 (peer RPM)
[1/15 15:25:45]: CMD-(CLI):[configure]by default from console
- Repeated 1 time.
[1/15 15:25:56]: CMD-(CLI):[username mari password ********]by default from console
[1/15 15:26:33]: CMD-(CLI):[configure]by default from console
- Repeated 1 time.
[1/15 15:26:47]: CMD-(CLI):[ip ssh server enable]by default from console
[1/15 15:26:59]: CMD-(SSH47):[enable]by mari from vty0 (10.11.9.207)
[1/15 15:27:8]: CMD-(SSH47):[show command-history 15]by mari from vty0 (10.11.9.207)
FTOS#
```

Usage Information

The command history output includes:

- [username name password ********] — when the command is executed via telnet
- [by default from console] — when the command is executed via console
• **[by admin from vty0 (peer RPM)]** — with brackets, when the command is executed to primary rpm via standby rpm using telnet-peer-rpm command.

Each command contains up to 50 characters in the display output. Dell Networking OS compares the first 50 characters of each command and if the characters are the same (i.e. the same command was issued), then the display output indicates the duplicate entry with “Repeated X times” (see Figure 65-5).

All commands executed by all users, except password related commands, are captured in the trace command history log. Each command has a date and time stamp (see Figure 65-5). The trace-log file has a separate 3000 line buffer to hold command history on a FIFO basis. When the buffer is full, the contents wraps (i.e. the first line is automatically deleted to make room for the last command line). This file can be analyzed by the Dell Networking Technical Assistance Center (TAC) to assist in troubleshooting.

Note: No password information is saved to the trace command history log.

### show console

Display, onto the console, background resets, calls, initialization etc. of the designated line card.

**Syntax**

```
show console lp slot-number
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lp slot-number</td>
<td>(OPTIONAL) Enter the keyword lp and the slot number to view information on the line-card processor in that slot. Range: 0 to 13 on an E1200, 0 to 6 on an E600/E600i, and 0 to 5 on an E300.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Modes**

EXEC Privilege

**Command History**

Version 7.5.1.0 Introduced

**Example**

```
FTOS#show console lp 0
MINI FIFO CONTRL = 0x0a
MINI FIFO RPM POINTER = 0x000
MINI FIFO CPU POINTER = 0xb0b
Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 69
frrpaProcessIfmNotif(): Default case. type = 69
frrpaProcessIfmNotif(): Default case. type = 70
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 11
frrpaProcessIfmNotif(): Default case. type = 11
FTOS#
```
**reset linecard**

Reset a specific line card module (power-off and then power-on).

**Syntax**

```
reset linecard slot-number
```

**Parameters**

- `slot-number` Enter the slot number of the SFM to reset. Range: 0 to 6

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

Version 6.5.4.0 Introduced

**Related Commands**

- `power on/off linecard` Power on/off a line card

---

**reset sfm**

Reset a specific SFM module (power-off and then power-on).

**Syntax**

```
reset sfm slot-number
```

**Parameters**

- `slot-number` Enter the slot number of the SFM to reset. Range: 0 to 7

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

Version 6.5.4.0 Introduced

**Usage Information**

When an error is detected on an SFM module, this command is a manual recovery mechanism. Since this command can be used with live traffic running, the switch fabric will not go down if the switch fabric is in an UP state. When there is a full set of SFMs online in the chassis, resetting one SFM will reduce the total bandwidth supported by the chassis and may affect data flow. A warning message is issued at the command line and requires user confirmation to proceed (Figure 65-7).

**Example**

```
FTOS#reset sfm 0
SFM0 is active. Resetting it might temporarily impact data traffic. Proceed with reset [confirm yes/no]:yes
Feb 16 00:39:30: %RPM1-P:CP %TSM-5-SFM_DISCOVERY: Found SFM 0
FTOS#
```

This command does not permit resetting any SFM when the system has (max-1) SFM and switch fabric is up (Figure 65-8).
Example

**Figure 65-8. reset sfm error message**

FTOS#reset sfm 1
% Error: SFM1 is active. Resetting it will impact data traffic.
FTOS#

**Note:** Resetting an SFM in a power-off state is not permitted. Use the command `power-on sfm` to bring the SFM back to a power-on state.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>power-off/on sfm</code></td>
<td>Power on/off an SFM</td>
</tr>
</tbody>
</table>

**show diag sfm**

Display the results and status of the last chassis runtime/onetime loopback test.

**Syntax**

```
show diag sfm
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC

**Command History**

Version 6.5.4.0 Introduced

**Example**

**Figure 65-9. show diag sfm command Example**

FTOS#show diag sfm

Switch Fabric Module Loopback Test: enabled
SFM Walk-Through in Loopback Test: enabled
SFM Bring-Down in Loopback Test: enabled
Switch Fabric Module Loopback State: on

-- Route Processor Modules --

<table>
<thead>
<tr>
<th>Slot</th>
<th>Test Status</th>
<th>Last Result</th>
<th>Time Stamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>on</td>
<td>pass</td>
<td>Mar 26 2007 12:41:56</td>
</tr>
<tr>
<td>1</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

-- Line cards --

<table>
<thead>
<tr>
<th>Slot</th>
<th>Test Status</th>
<th>Last Result</th>
<th>Time Stamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>on</td>
<td>pass</td>
<td>Mar 26 2007 12:41:56</td>
</tr>
<tr>
<td>3</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>on</td>
<td>pass</td>
<td>Mar 26 2007 12:41:56</td>
</tr>
<tr>
<td>12</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>off</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

FTOS#
show processes ipc

Display IPC messaging used internally between Dell Networking OS processes.

Syntax

```
show processes ipc [recv-stats | send-stats] [cp | rp1 | rp2 | lp linecard-number]
```

Parameters

- **recv-stats**: (OPTIONAL) Enter the keyword `recv-stats` to display the receiver-side details of the IPC messages.
- **send-stats**: (OPTIONAL) Enter the keyword `send-stats` to display the sender-side details of the IPC messages.
- **cp**: (OPTIONAL) Enter the keyword `cp` to view the Control Processor’s swpq statistics.
- **rp1**: (OPTIONAL) Enter the keyword `rp1` to view the Control Processor’s swpq statistics on Route Processor 1.
- **rp2**: (OPTIONAL) Enter the keyword `rp2` to view the Control Processor’s swpq statistics on Route Processor 2.
- **lp linecard-number**: (OPTIONAL) Enter the keyword `lp` followed by the line card number to view the Control Processor’s swpq statistics on the specified line card.

Defaults

No default values or behavior

Command Modes

EXEC
EXEC Privilege

Command History

Version 7.5.1.0 Introduced

Example

```
Figure 65-10. show processes ipc recv-stats Command Example

FTOS#show processes ipc recv-stats lp 0
IPC Receive Statistics on LP 0
Memory Used by Recv DB on this processor: 6825992 bytes
SeqNo - Last successfull Guaranteed IPC Pkt Seq No delivered from source to destination
HiWtmk - Highest socket watermark reached for destination
M-SkSize - Max socket size of destination
NonG-Rcvd - No of non-guaranteed IPC pkts received
Pri-Dr - Priority drops done for non-guaranteed pkts due to socket almost-full condition
SkFull-Dr - Any IPC packet dropped because of socket full condition

Source-> Destination SeqNo HiWtmk(%) M-SkSize NonG-Rcvd Pri-Dr SkFull-Dr
TME: 0 -> TME: 3 0 0 41600 1 0 0
TME: 3 -> LCMGR: 0 0 0 41600 1 0 0
IPC: 0 -> IPC: 3 37557 0 41600 0 0 0
IPC: 3 -> TME: 3 16215 0 41600 0 0 0
CLI: 0 -> SYSADMTSK: 3 11483 0 41600 0 0 0
FTOS#
```
Example Figure 65-11.  show processes ipc send-stats Command Example

FTOS#show processes ipc send-stats
IPC Send Statistics on CP
Memory Used by Send DB on this processor: 2303000 bytes
Success - No of successful guaranteed IPC packets sent from source to destination
1st-R - No of first retry attempts
2nd-R - No of second retry attempts
Fails - No of guaranteed IPC pkts that could not be transmitted
RTT(ms) - Avg. Round Trip time for guaranteed IPC packets in milliseconds
NonG-S - No of non-guaranteed IPC pkts sucessfully sent. This does not include those sent by SWP
NonG-F - No of non-guaranteed IPC pkt transmission failures
SWP-S - No of non-guaranteed SWP IPC pkts sucessfully sent
SWP-F - No of non-guaranteed SWP IPC pkt transmission failures

<table>
<thead>
<tr>
<th>Source-&gt;</th>
<th>Destination</th>
<th>SeqNo</th>
<th>Success</th>
<th>1st-R</th>
<th>2nd-R</th>
<th>Fails</th>
<th>RTT(ms)</th>
<th>NonG-S</th>
<th>NonG-F</th>
<th>SWP-S</th>
<th>SWP-F</th>
</tr>
</thead>
<tbody>
<tr>
<td>TME: 0 -&gt; TME: 1</td>
<td>15868</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Usage Information
These commands should be used only when you are working directly with Dell Networking TAC (Technical Assistance Center) while troubleshooting a problem.

show processes ipc flow-control
Display the Single Window Protocol Queue (swpq) statistics.

Syntax
show processes ipc flow-control [cp | rp1 | rp2 | lp linecard-number]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp</td>
<td>(OPTIONAL) Enter the keyword cp to view the Control Processor’s swpq statistics.</td>
</tr>
<tr>
<td>rp1</td>
<td>(OPTIONAL) Enter the keyword rp1 to view the Control Processor’s swpq statistics on Route Processor 1.</td>
</tr>
<tr>
<td>rp2</td>
<td>(OPTIONAL) Enter the keyword rp2 to view the Control Processor’s swpq statistics on Route Processor 2.</td>
</tr>
<tr>
<td>lp linecard-number</td>
<td>(OPTIONAL) Enter the keyword lp followed by the line card number to view the Control Processor’s swpq statistics on the specified line card.</td>
</tr>
</tbody>
</table>

Defaults
No default values or behavior

Command Modes
EXEC
EXEC Privilege

Command History
Version 7.5.1.0 Introduced
Example Figure 65-12. show processes ipc flow-control rp Command Example

FTOS# show processes ipc flow-control rp2

<table>
<thead>
<tr>
<th>[qid]</th>
<th>Source-&gt;Dest</th>
<th>Cur Len</th>
<th>High Mark</th>
<th>Time Out</th>
<th>Retries</th>
<th>Msg Sent</th>
<th>Ack Rcvd</th>
<th>Aval Retrans</th>
<th>Max Retrans</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>unknown2-&gt;unknown2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>[2]</td>
<td>12pm0-&gt;spanMgr0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2298</td>
<td>2298</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>[3]</td>
<td>fvrp0-&gt;macMgr0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1905</td>
<td>1905</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>[4]</td>
<td>12pm0-&gt;fvrp0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>[5]</td>
<td>fvrp0-&gt;l2pm0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>[6]</td>
<td>stp0-&gt;l2pm0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>[7]</td>
<td>spanMgr0-&gt;macMgr0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>[8]</td>
<td>spanMgr0-&gt;ipMgr0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>

FTOS#

Example Figure 65-13. show processes ipc flow-control lp Command Example

FTOS# show processes ipc flow-control lp 10

<table>
<thead>
<tr>
<th>TxProcess</th>
<th>RxProcess</th>
<th>Cur Len</th>
<th>High Mark</th>
<th>Time Out</th>
<th>Retries</th>
<th>Msg Sent</th>
<th>Ack Rcvd</th>
<th>Aval Retrans</th>
<th>Max Retrans</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL_AGENT10</td>
<td>PIM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>ACL_AGENT10</td>
<td>PIM0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>FRRPAGENT10</td>
<td>PFRP0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>IFAGENT10</td>
<td>IFMGR0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>LPMACAGENT10</td>
<td>MACMGR0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>

FTOS#

Table 65-1 defines the fields displayed in Figure 65-13.

Table 65-1. show processes ipc flow-control Display Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxProcess</td>
<td>Sender Process</td>
</tr>
<tr>
<td>RxProcess</td>
<td>Receiver Process</td>
</tr>
<tr>
<td>Cur Len</td>
<td>The number of messages, in the sender process, waiting to be sent to the receiver process</td>
</tr>
<tr>
<td>High Mark</td>
<td>The maximum number of accumulated messages (over the life of the queue), in the sender process, waiting to be sent out to the receiver process</td>
</tr>
<tr>
<td>Time Out</td>
<td>The time period the sender process waits for acknowledgement from the receiver process before attempting to resend the queued messages</td>
</tr>
<tr>
<td>Retries</td>
<td>The number of successive attempts (retries) the sender process will make to send the messages to the receiver process</td>
</tr>
<tr>
<td>Msg Sent</td>
<td>The accumulated number of messages sent between the sender and receiver processes from the time the queue was created.</td>
</tr>
<tr>
<td>Ack Rcvd</td>
<td>The number of acknowledgements received from the receiver process</td>
</tr>
<tr>
<td>Aval Retrans</td>
<td>The current number of attempts, for retransmission, available in the event an acknowledgement is not received. This value decrements on every retry and may fall below the initial value, of “Max Retrans” to zero, in case the receiver is not responding. This count is reset dynamically to Max Retrans value in case the queue starts to function after experiencing some acknowledgement loss</td>
</tr>
<tr>
<td>Max Retrans</td>
<td>The max number of retransmission attempts configured for a sender - receiver pair</td>
</tr>
</tbody>
</table>

Usage Information

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 period of time, the SWP time-out mechanism re-submits the message at the head of the FIFO queue.
- After retrying several times, the following time-out message is generated:

  SWP-2-NOMORETIMEOUT

- In the display output in Figure 65-13, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

show revision

Display revision numbers of all line card, RPM, and SFM components.

Syntax

show revision

Defaults

No default behavior or value

Command Modes

EXEC Privilege

Command History

Version 7.5.1.0 Introduced
Example  

Figure 65-14. show revision Command Example (Partial)

FTOS#show revision

-- RPM 0 --
panda : ASIC - 0x72632000
bedrock : 0x34
helio : 0x13
tabby : 0x7
willow : 0x13

-- Line card 0 --
lc pic 0 : 1.0
lc pic 1 : 1.0
marvel serdes : 0x0
aquarius : 0x15
galle : 0x11
lynx : 0x7
mini : 0x22
pandora : 0xd

-- Line card 1 --
lc pic 0 : 1.1
lc pic 1 : 1.1
marvel serdes : 0xcd4
aquarius : 0x15
galle : 0x11
lynx : 0x7
mini : 0x25
pandora : 0x9

-- SFM 0 --
simba : 0x1
faith : 0xc

-- SFM 1 --
simba : 0x1
faith : 0xc

-- SFM 2 --
simba : 0x1
faith : 0xc

-- SFM 3 --
simba : 0x1
faith : 0xc

-- SFM 4 --
simba : 0x1
faith : 0xc

show tech-support

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

Syntax  

show tech-support [linecard | page] {display | except | find | grep | no-more | save}

Parameters

<table>
<thead>
<tr>
<th>(linecard &lt;0-6&gt;)</th>
<th>(OPTIONAL) Enter the keyword linecard followed by the linecard number to view information relating to a specific linecard.</th>
</tr>
</thead>
<tbody>
<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>
**Command Modes**

**EXEC Privilege**

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Added save option</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
<tr>
<td>6.5.4.0</td>
<td>Show clock included in display</td>
</tr>
</tbody>
</table>

**Usage Information**

The display output is an accumulation of the same information that is displayed when you execute one of the following show commands:

- `show cam-profile`
- `show cam-ipv4flow`
- `show chassis`
- `show clock`
- `show environment`
- `show file-system`
- `show interface`
- `show inventory`
- `show ip management-route`
- `show ip protocols`
- `show ip route summary`
- `show processes cpu`
- `show processes memory`
- `show redundancy`
- `show rpm`
- `show running-conf`
- `show sfm`
- `show version`

Without the `page` option, the command output is continuous, use CNTL-z to interrupt the command output.

**display, except, find, grep, no-more**

When using the pipe command ( | ), enter one of these keywords to filter command output. Refer to CLI Basics in the Dell Networking OS Command Reference Guide for details on filtering commands.

**save:**

Enter the save keyword (following the pipe) to save the command output.

- `flash`: Save to local flash drive (flash://filename (max 20 chars))
- `slot0`: Save to local file system (slot0://filename (max 20 chars))
Example Figure 65-15. show tech-support (E-Series Command Example) Partial Output

FTOS#show tech-support
----------------------------------- show version -------------------------------
Force10 Networks Real Time Operating System Software
System image file is "flash://FTOS-EF-6.5.4.1.bin"

Chassis Type: E600
Control Processor: IBM PowerPC 750FX (Rev D2.2) with 536870912 bytes of memory.
Route Processor 1: IBM PowerPC 750FX (Rev D2.2) with 1073741824 bytes of memory.
Route Processor 2: IBM PowerPC 750FX (Rev D2.2) with 1073741824 bytes of memory.

128K bytes of non-volatile configuration memory.
1 Route Processor Module
9 Switch Fabric Module
1 48-port GE line card with SFP optics (EF)
1 4-port 10GE LAN/WAN PHY line card with XFP optics (EF)
1 48-port 10/100/1000Base-T line card with RJ-45 interfaces (EF)
1 FastEthernet/IEEE 802.3 interface(s)
96 GigabitEthernet/IEEE 802.3 interface(s)
4 Ten GigabitEthernet/IEEE 802.3 interface(s)
------------------------------------ show clock -------------------------------
 coax clock information

--  RPM Status --
----------------------------------- show HA information ----------------------
-- RPM Redundancy Configuration --
----------------------------------- show running-config ------------------------
Current Configuration ...
! Version 6.5.4.1
! boot system rpm0 primary flash://FTOS-EF-6.5.4.1.bin
boot system rpm0 secondary flash://FTOS-EF-6.5.4.1.bin
boot system rpm0 default flash://FTOS-EF-6.5.4.1.bin
! redundancy auto-failover-limit count 3 period 60
redundancy auto-synchronize full
redundancy disable-auto-reboot rpm
redundancy primary rpm0
! hostname E600-TAC-3
! cam-ipv4flow multicast-fib 9 pbr 1 qos 8 system-flow 5 trace-list 1
! ...

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>Display the Dell Networking OS version.</td>
</tr>
<tr>
<td>show linecard</td>
<td>Display the line card(s) status.</td>
</tr>
</tbody>
</table>
Offline Diagnostic Commands

The offline diagnostics test suite is useful for isolating faults and debugging hardware. The tests results are written to a file in flash memory and can be displayed on screen. Detailed statistics for all tests are collected.

These statistics include:
- last execution time
- first test pass time and last test pass time
- first test failure time and last test failure time
- total run count
- total failure count
- consecutive failure count
- error code

The offline diagnostics commands are:
- diag linecard
- offline
- online
- show diag

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show environment (C-Series and E-Series)</td>
<td>Display system component status.</td>
</tr>
<tr>
<td>show processes memory (C-Series and E-Series)</td>
<td>Display memory usage based on running processes.</td>
</tr>
</tbody>
</table>

**diag linecard**

Run offline diagnostics on a line card(s).

**Syntax**

```
diag linecard number {alllevels | level0 | level1 | level2} | {terminate}
```

To terminate the offline diagnostics, use the `diag linecard number terminate` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.</td>
</tr>
<tr>
<td>alllevels</td>
<td>Enter the keyword <code>alllevels</code> to run the complete offline diagnostic test.</td>
</tr>
<tr>
<td>level0</td>
<td>Enter the keyword <code>level0</code> to check the device inventory and verify the existence of the devices.</td>
</tr>
<tr>
<td>level1</td>
<td>Enter the keyword <code>level1</code> to verify that the devices are accessible via the designated paths (line integrity tests) and test the internal registers of the devices.</td>
</tr>
<tr>
<td>level2</td>
<td>Enter the keyword <code>level2</code> to perform on-board loopback tests on various data paths (data Port-Pipe and Ethernet).</td>
</tr>
<tr>
<td>terminate</td>
<td>Enter the keyword <code>terminate</code> to stop the offline diagnostics tests.</td>
</tr>
</tbody>
</table>
## offline

Place a line card in an offline state.

### Syntax

```
offline {linecard number}
```

### Parameters

- `linecard number`: Enter the keyword `linecard` followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

### Defaults

No default behavior or values

### Command Mode

- EXEC
- EXEC Privilege

### Command History

- Version 6.5.4.0: Introduced

## online

Place a line card in an online state.

### Syntax

```
online {linecard number | rpm number}
```

### Parameters

- `linecard number`: Enter the keyword `linecard` followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

### Defaults

No default behavior or values

### Command Mode

- EXEC
- EXEC Privilege

### Command History

- Version 6.5.4.0: Introduced
show diag

Display current diagnostics information.

**Syntax**

```
show diag {information} [linecard number [detail | periodic | summary]]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>information</td>
<td>Enter the keyword <strong>information</strong> to view current diagnostics information in the system.</td>
</tr>
<tr>
<td>linecard number</td>
<td>(OPTIONAL) Enter the keyword <strong>linecard</strong> followed by the line card slot number. Range: 0 to 13 on an E1200, 0 to 6 on an E600, and 0 to 5 on an E300.</td>
</tr>
<tr>
<td>detail</td>
<td>(OPTIONAL) Enter the keyword <strong>detail</strong> to view detailed diagnostics information.</td>
</tr>
<tr>
<td>periodic</td>
<td>(OPTIONAL) Enter the keyword <strong>periodic</strong> to display diagnostics results periodically.</td>
</tr>
<tr>
<td>summary</td>
<td>(OPTIONAL) Enter the keyword <strong>summary</strong> to view a summary of the diagnostics information.</td>
</tr>
</tbody>
</table>

**Defaults**

summary

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.4.0</td>
<td></td>
</tr>
</tbody>
</table>

**Hardware Commands**

These commands display information from a hardware sub-component or ASIC.

**Warning:** These commands should be used only when you are working directly with Dell Networking TAC (Technical Assistance Center) while troubleshooting a problem. Do not use these command without the assistance of a Dell Networking TAC representative. To contact Dell Networking TAC for assistance:

- E-mail Direct Support: Dell-Force10_Technical_Support@Dell.com
- Web: support.dell.com
- Telephone support:
  - US and Canada customers: 866-965-5800
  - International customers: 408-965-5800

The commands in this section are:

- clear hardware btm
- clear hardware rpm mac counters
- hardware monitor linecard
- hardware monitor mac
- hardware watchdog
- show cpu-interface-stats
- show hardware btm
clear hardware btm

Clear the Buffer Traffic Manager (BTM) error counters and status registers.

**Syntax**

clear hardware \{rpm | linecard\} number port-set pipe-number btm \{egress | ingress | all\} \{errors | status\}

**Parameters**

- **rpm**
  Enter the keyword `rpm` to clear BTM error counters or status registers on the RPM.

- **linecard number**
  Enter the keyword `linecard` followed by the line card slot number to clear BTM error counters or status registers on the specified line card.
  Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300

- **port-set pipe-number**
  Enter the keyword `port-set` followed by the number of the line card or RPM’s Port-Pipe.
  Range: 0 to 1

- **egress errors | status**
  (OPTIONAL) Enter the keywords `egress errors` or `egress status` to clear egress BTM error counters or ingress BTM status registers.

- **ingress errors | status**
  (OPTIONAL) Enter the keywords `ingress errors` or `ingress status` to clear ingress BTM error counters or ingress BTM status registers.

- **all errors | status**
  (OPTIONAL) Enter the keywords `all errors` or `all status` to clear both egress and ingress BTM error counters and status registers.

**Defaults**

No default behavior or values

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 6.5.4.0 Introduced
clear hardware rpm mac counters

Clear the MAC counters for the party-bus control switch on the IPC subsystem of the RPM.

**Syntax**

```
clear hardware rpm slot-number mac counters
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot-number</td>
<td>Enter the RPM slot number.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 -1</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values

**Command Mode**

- EXEC
- EXEC Privilege

**Command History**

- Introduced in Version 6.5.4.0

hardware monitor linecard

Configure the system to take an action upon a line card hardware error.

**Syntax**

```
hardware monitor linecard asic [btm | fpc] [action-on-error {card-problem | card-reset | card-shutdown}] | parity-correction
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action-on-error</td>
<td>Enter the keyword action-on-error to further specify actions that should be</td>
</tr>
<tr>
<td></td>
<td>taken in the event of a hardware error.</td>
</tr>
<tr>
<td>btm</td>
<td>Enter the keyword btm to configure the system to take an action upon a Buffer</td>
</tr>
<tr>
<td></td>
<td>Traffic Manager hardware error.</td>
</tr>
<tr>
<td>fpc</td>
<td>Enter the keyword fpc to configure the system to take an action upon a Flexible</td>
</tr>
<tr>
<td></td>
<td>Packet Classifier hardware error.</td>
</tr>
<tr>
<td>card-problem</td>
<td>Enter the keyword card-problem to place a line card in a card-problem state</td>
</tr>
<tr>
<td></td>
<td>upon a hardware error.</td>
</tr>
<tr>
<td>card-reset</td>
<td>Enter the keyword card-reset to reset a line card upon a hardware error.</td>
</tr>
<tr>
<td>card-shutdown</td>
<td>Enter the keyword card-shutdown to shutdown a line card upon a hardware error.</td>
</tr>
<tr>
<td>parity-correction</td>
<td>Enter the keyword parity-correction to enable automatic parity corrections for</td>
</tr>
<tr>
<td></td>
<td>SRAM. The line card must be reloaded before the feature becomes operational.</td>
</tr>
</tbody>
</table>
hardware monitor mac

Configure the system to shut down all ports on a line card upon a MAC hardware error.

**Syntax**

```plaintext
hardware monitor mac action-on-error port-shutdown
```

**Defaults**
None

**Command Mode**
CONFIGURATION

**Command History**
Version 7.7.1.0 Introduced

**Usage Information**
This command enables a hardware monitor mechanism that automatically shuts down all ports on a line card upon a MAC hardware error. This is a last resort mechanism intended to prevent a manual power cycle.

hardware watchdog

Set the watchdog timer to trigger a reboot and restart the system.

**Syntax**

```plaintext
hardware watchdog
```

**Defaults**
Enabled

**Command Mode**
CONFIGURATION

**Command History**
Version 7.7.1.0 Introduced

**Usage Information**
This command enables a hardware watchdog mechanism that automatically reboots an Dell Networking OS switch/router with a single unresponsive RPM. This is a last resort mechanism intended to prevent a manual power cycle.

show cpu-interface-stats

The command provides an immediate snapshot of the health of the internal RPM and line card CPU. Generally this command is used in concert with Dell Networking Technical Support engineers.

**Syntax**

```plaintext
show cpu-interface-stats {cp | lp | rp1 | rp2}
```

**Parameters**

- `cp` Enter the keyword `cp` to display the CP's interface statistics.
- `lp` Enter the keyword `lp` to display the LP's interface statistics
- `rp1` Enter the keyword `rp1` to display the RP1's interface statistics
- `rp2` Enter the keyword `rp2` to display the RP2's interface statistics.
Defaults
No default behavior or values

Command Modes
EXEC
EXEC Privilege

Command History
Version 7.6.1.0 Introduced on E-Series

Example

Figure 65-17. show cpu-interface-stats Ip Command Example

FTOS#show cpu-interface-stats lp 1
--- Dataplane PP1 interface statistics ---
Link state : Up
Recv Interrupts/Polls: 0
Recv Packets : 9807 Transmit Packets : 9808
Recv Desc Error : 0 Transmit Desc Error : 0
Recv Out of Mem : 0 Transmit Out of Mem : 0
Recv Upper Layer Full: 0 Transmit Pause Pkts : 0
Recv Other Error : 0 Transmit Other Error: 0
Recv Restarts : 0
Recv Restarts Fatal : 0
--- Dataplane PP0 interface statistics ---
Link state : Up
Recv Interrupts/Polls: 0
Recv Packets : 9807 Transmit Packets : 9807
Recv Desc Error : 0 Transmit Desc Error : 0
Recv Out of Mem : 0 Transmit Out of Mem : 0
Recv Upper Layer Full: 0 Transmit Pause Pkts : 0
Recv Other Error : 0 Transmit Other Error: 0
Recv Restarts : 0
Recv Restarts Fatal : 0
--- Partybus RPM0 interface statistics ---
Link state : Up
Recv Interrupts/Polls: 0
Recv Packets : 171611 Transmit Packets : 329859
Recv Desc Error : 0 Transmit Desc Error : 0
Recv Out of Mem : 0 Transmit Out of Mem : 0
Recv Upper Layer Full: 0 Transmit Pause Pkts : 0
Recv Other Error : 0 Transmit Other Error: 0
Recv Restarts : 0
Recv Restarts Fatal : 0
--- Partybus RPM1 interface statistics ---
Link state : Up
Recv Interrupts/Polls: 0
Recv Packets : 0 Transmit Packets : 0
Recv Desc Error : 0 Transmit Desc Error : 0
Recv Out of Mem : 0 Transmit Out of Mem : 0
Recv Upper Layer Full: 0 Transmit Pause Pkts : 0
Recv Other Error : 0 Transmit Other Error: 0
Recv Restarts : 0
Recv Restarts Fatal : 0
FTOS#
**Example Figure 65-18. show cpu-interface-stats cp command Example (Partial)**

```
FTOS#show cpu-interface-stats cp
-- Partybus ethernet statistics --
  Link state : Down
  Recv Interrupts/Polls: 438532
  Recv Packets : 440125  Transmit Packets : 290784
  ...
-- Dataplane ethernet statistics --
  Link state : Down
  Recv Interrupts/Polls: 9875
  Recv Packets : 9785  Transmit Packets : 9841
  ...
-- OOB ethernet statistics --
  Link state : Up
  Recv Interrupts/Polls: 15439
  Recv Packets : 19298  Transmit Packets : 11
  ...
-- Partybus switch statistics --
  Dropped cells : 0
  Dropped packets: 0
  LC0 :  Ingress: 0  Egress: 1780
  LC1 :  Ingress: 331581  Egress: 176297
  ...
  CP :  Ingress: 292114  Egress: 440141
  RP1 :  Ingress: 61250  Egress: 66663
  RP2 :  Ingress: 54346  Egress: 59750
  IRC :  Ingress: 0  Egress: 1780
-- Partybus ethernet rate statistics --
  0: Peak rate at Thu Dec 6 18:20:32 2007 -
  Total rate (bps) : 1634400
  Total Size (bytes): 4086
  Total Arp (bytes): 0
  From 127.10.10.23:0 2128 bytes
  From 127.10.10.23:9093 1500 bytes
  From 127.10.10.12:4233 368 bytes
  1: Peak rate at Thu Dec 6 18:16:40 2007 -
  Total rate (bps) : 1634400
  Total Size (bytes): 4086
  Total Arp (bytes): 0
  From 127.10.10.23:0 2128 bytes
  From 127.10.10.23:9093 1500 bytes
  From 127.10.10.12:4233 368 bytes
  2: Peak rate at Thu Dec 6 18:20:43 2007 -
  Total rate (bps) : 1634400
  Total Size (bytes): 4086
  Total Arp (bytes): 0
  From 127.10.10.23:0 2128 bytes
  From 127.10.10.23:9093 1500 bytes
  From 127.10.10.11:4229 368 bytes
-- IRC Statistics --
  irc phy: DOWN
-- Helios Statistics --
  ACL Fpga Cq  dataplane packets:9875 denied:0 dropped:0
  ACL Fpga Rpl  dataplane packets:39125 denied:0 dropped:0
  ACL Fpga Rp2  dataplane packets:274 denied:0 dropped:0
  ACL Fpga Mgmt  packets:19441 denied:0 dropped:0
FTOS#
```

**show hardware btm**

Display the Buffer Traffic Manager (BTM) error counters, status registers, or packet queue.

**Syntax**

```
show hardware {rpm | linecard} number port-set pipe-number btm {egress | ingress | all} [errors | status | queues] {register starting-value [number_of_registers]}
```
show hardware linecard (E-Series) Command Example

FTOS#show hardware linecard 1 port-set 2 btm all errors
Output for portpipe 0 Ingress
PC_SPI4_BADPORT_CNTR [0x000230] = 16777216
PC_SPI4_EOP_ABORT_CNTR [0x000234] = 33554432
PC_SPI4_MISS_SOP_CNTR [0x0238] = 50331648
Output for portpipe 0 Egress
PC_BAD_CRC_ERR_CNTR [0x000250] = 150994944
FTOS#
show hardware fpc forward

Display receive and transmit counters, error counters and status registers for the forwarding functional area of the FPC (flexible packet classification engine).

Syntax

```
show hardware linecard number port-set pipe-number fpc forward {counters | drops | spi {err-counters | spichannel# counters} | status}
```

Parameters

- **linecard number**: Enter the keyword `linecard` followed by the line card slot number. Range: 0 to 13 on E1200, 0 to 6 on E600/E600i, and 0 to 5 on E300
- **port-set pipe-number**: Enter the keyword `port-set` followed by the number of the line card’s Port-Pipe. Range: 0 to 1
- **counters**: (OPTIONAL) Enter the keyword `counters` to display the FPC receive and transmit packet, byte counters, and error counters.
- **drops**: (OPTIONAL) Enter the keyword `drops` to display FPC drop-related error counters.
- **spi err-counters**: (OPTIONAL) Enter the keywords `spi err-counters` to display the FPC System Packet Interface (SPI) receive and transmit packet, byte counters, error counters, and key status registers on the ingress and egress paths.
- **spi spichannel# counters**: (OPTIONAL) Enter the keywords `spi spichannel# counters` to display the FPC System Packet Interface level 4 (SPI4) counters.
- **status**: (OPTIONAL) Enter the keywords `status` to display FPC status registers.

Defaults

No default values or behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 6.5.4.0 Introduced

Example

```
Figure 65-20. show hardware fpc forward drops Command Example

FTOS#show hardware linecard 4 port-set 0 fpc forward drops
SPI 0
  ICMP Drops : 0x0
  ACL Drops  : 0x0
  IBC_DROP   : 0
  EBC_DROP   : 0
  IFA_DROP_CNT : 0
  EFA_DROP_CNT : 0
  CMB_Lg_DROP : 0
  CMB_SF_DROP : 0
  CMB_Ipm_DROP : 0
  CMB_Opm_DROP : 0
  SPI 1
  ICMP Drops : 0x0
  ACL Drops  : 0x0
  IBC_DROP   : 0
  EBC_DROP   : 0
  IFA_DROP_CNT : 0
  EFA_DROP_CNT : 0
  CMB_Lg_DROP : 0
  CMB_SF_DROP : 0
  CMB_Ipm_DROP : 0
  CMB_Opm_DROP : 0
FTOS#
```
Example

Figure 65-21. `show hardware fpc forward counters` Command Example

```
FTOS#show hardware linecard 4 port-set 0 fpc forward counters
Portpipe 0
Ingress Counters
SPI 0
SPI4_ABORT: 0
MAC_2_T2_DIP2: 0
MAC_2_T2_DIP4: 0
SPI4_LOSS_CNT: 0
MAC_2_T2_RX_PKT_COUNTER_CRC: 0
MAC_2_T2_RX_PKT_COUNTER_LO: 0
MAC_2_T2_RX_PKT_COUNTER_HI: 0
IBC_DROP: 0
IFA_TX_PKT_LO: 0
IFA_TX_PKT_HI: 0
Egress Counters
SPI 0
SPI4_ABORT: 0
C2_TO_T2_DIP2: 0
C2_TO_T2_DIP4: 0
SPI4_LOSS_CNT1: 0
C2_TO_T2_RX_PKT_COUNTER_CRC: 0
C2_TO_T2_RX_PKT_COUNTER_LO: 0
C2_TO_T2_RX_PKT_COUNTER_HI: 0
EBC_DROP: 0
EFA_TX_PKT_LO: 0
EFA_TX_PKT_HI: 0
EGRESS_DROP_COUNT: 0

Portpipe 0
Ingress Counters
SPI 1
SPI4_ABORT: 0
MAC_2_T2_DIP2: 0
MAC_2_T2_DIP4: 0
SPI4_LOSS_CNT: 0
MAC_2_T2_RX_PKT_COUNTER_CRC: 0
MAC_2_T2_RX_PKT_COUNTER_LO: 0
MAC_2_T2_RX_PKT_COUNTER_HI: 0
IBC_DROP: 0
IFA_TX_PKT_LO: 0
IFA_TX_PKT_HI: 0
Egress Counters
SPI 1
SPI4_ABORT: 0
C2_TO_T2_DIP2: 0
C2_TO_T2_DIP4: 0
SPI4_LOSS_CNT1: 0
C2_TO_T2_RX_PKT_COUNTER_CRC: 0
C2_TO_T2_RX_PKT_COUNTER_LO: 0
C2_TO_T2_RX_PKT_COUNTER_HI: 0
EBC_DROP: 0
EFA_TX_PKT_LO: 0
EFA_TX_PKT_HI: 0
EGRESS_DROP_COUNT: 0

FTOS#

```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show hardware fpc lookup detail</code></td>
<td>Display fpc lookup information.</td>
</tr>
</tbody>
</table>
show hardware fpc lookup detail

Display diagnostic and debug information related to the lookup functional area of the Flexible Packet Classification (FPC).

**Syntax**

```
show hardware linecard number port-set pipe-number fpc lookup detail
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>linecard number</code></td>
<td>Enter the keyword <code>linecard</code> followed by the line card slot number.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300</td>
</tr>
<tr>
<td><code>port-set pipe-number</code></td>
<td>Enter the keyword <code>port-set</code> followed by the number of the line card’s</td>
</tr>
<tr>
<td></td>
<td>Port-Pipe.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 to 1</td>
</tr>
</tbody>
</table>

**Defaults**

No default values or behavior

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

- Version 6.5.4.0   Introduced
Example

Figure 65-22. show hardware linecard Command Example

FTOS#show hardware linecard 0 port-set 0 fpc lookup detailed
Summary of Error Registers
--------- -- ------
0 Counters Enabled :
Cyclone 1.5 ChassisMap : 0x00000000
Cyclone 1.5 MixedMode : 0x00000000
T2L party Status : No Errors
partyType ErrorCount
--------- -------
Summary of Last 16 CamSearches
---------------------------------------------
I CamKey P T R PE N
n  a a P o g W
d  r b I r r r
e  i l D t e I
x  t e I s n
y  T d s d
y  e

21554 50697065.5f302045.72726f72.2026204d.61736b20 0x52656769
0x73746572 0x2044756d 1879719229 1027423549 1027423549
Summary of Last 16 CamHits
----------------------------------------
I Hit0/ Hit1/ S R PE N
n Index0 Index1 r P o g W
d  c i r r r
e  H D t e I
x  C I s n
o  d s d
d  e
x  e
0 0/0x00000 0/0x00000 0x00 0x00 00 0
1 0/0x00000 0/0x00000 0x00 0x00 00 0
2 0/0x00000 0/0x00000 0x00 0x00 00 0
3 0/0x00000 0/0x00000 0x00 0x00 00 0
4 0/0x00000 0/0x00000 0x00 0x00 00 0
5 0/0x00000 0/0x00000 0x00 0x00 00 0
6 0/0x00000 0/0x00000 0x00 0x00 00 0
7 0/0x00000 0/0x00000 0x00 0x00 00 0
8 0/0x00000 0/0x00000 0x00 0x00 00 0
9 0/0x00000 0/0x00000 0x00 0x00 00 0
10 0/0x00000 0/0x00000 0x00 0x00 00 0
11 0/0x00000 0/0x00000 0x00 0x00 00 0
12 0/0x00000 0/0x00000 0x00 0x00 00 0
13 0/0x00000 0/0x00000 0x00 0x00 00 0
FTOS#

show hardware fpc forward Display information related to FPC forward.

show hardware rpm cp
Display advanced debugging information for the RPM processors.

Syntax

show hardware rpm slot-number {data-plane | management-port} | party-bus} {counters | statistics}

Parameters

- **slot-number** Enter the RPM slot number 0 or 1.
- **data-plane** (OPTIONAL) Enter the keywords data-plane to display information about the dataplane interface on the control processor of the specified RPM.
management-port  (OPTIONAL) Enter the keywords management-port to display information about the management-port interface of the control processor on the specified RPM.

party-bus  (OPTIONAL) Enter the keywords party-bus to display control processor information on the party-bus of the specified RPM.

counters  (OPTIONAL) Enter the keyword counters to display the standard Ethernet counters.

statistics  (OPTIONAL) Enter the keyword statistics to display driver-related counters

<table>
<thead>
<tr>
<th>Defaults</th>
<th>No default values or behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
<tr>
<td></td>
<td>EXEC Privilege</td>
</tr>
<tr>
<td>Command History</td>
<td>Version 6.5.4.0 Introduced</td>
</tr>
</tbody>
</table>

**Figure 65-23. show hardware rpm Command Examples**

```
FTOS#show hardware rpm 0 cp data-plane counters
Input statistics
  31262 Bytes, 319 Frames,
  31262 Total Bytes, 319 Total Frames,
  0 Broadcasts, 0 Multicasts,
  0 CRC, 0 Oversize,
  0 Fragments, 0 Jabber,
  0 64-byte Frames, 638 127-byte Frames,
  0 255-byte Frames, 0 511-byte Frames,
  0 1023-byte Frames, 0 Max Frames,
  0 Error, 0 Dropped,
  0 Undersized

Output statistics
  31262 Bytes, 319 Frames, 357822480 Total Bytes,
  0 Collisions, 0 Late collisions,
  0 Broadcasts, 0 Multicasts

FTOS#show hardware rpm 0 cp data-plane statistics
Input statistics
  540 Interrupts, 0 Ticks,
  0 DMA Errors, 0 Stopped,
  0 Cleanup, 0 Throttle Drops,
  0 Status Error, 0 Too Large,
  0 Buff Err0, 320 Receive Interrupts,
  320 Readied for Protocols, 0 Jumbo,
  0 Jumbo Error, 0 Ignored,
  0 Jumbo Missing first, 0 Jumbo Dup First,
  0 Jumbo Mget Failed,
  0 Jumbo ClGet Failed, 0 No Mem,
  0 Overflow fix count,
  0 Mget Failed, 0 ClGet Failed

Output statistics
  0 Pause, 0 Watchdog,
  0 Late Collision, 0 Underrun,
  0 Retransmit Limit, 0 Out Frames,
  0 No Mem, 0 Phy Syncs

FTOS#
```
show hardware rpm mac counters

Display receive- and transmit-counters for the party-bus control switch on the IPC subsystem of the RPM.

Syntax

show hardware rpm slot-number mac counters [port port-number]

Parameters

- **slot-number**: Enter the RPM slot number 0 or 1.
- **port port-number**: (OPTIONAL) Enter the keyword **port** followed by the port number of the parity-bus control switch. Range: 0 to 24

Defaults

No default values or behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- Version 6.5.4.0 Introduced

Example

**Figure 65-24. show hardware rpm mac counters Command Example**

```
FTOS#show hardware rpm 0 mac counters
PORT#    RX Frames  TX Frames
--------------------------------------
 0 [LC0 ]     0          5
 1 [LC1 ] 25171       2119
 2 [LC2 ]  13967       2108
 3 [LC3 ]  13964       2108
 4 [LC4 ]     0          5
 5 [LC5 ] 25134       2108
 6 [LC6 ]     0          5
 7 [LC7 ]     0          5
 8 [LC8 ]     0          5
 9 [LC9 ]     0          5
10 [LC10 ]     0          5
11 [LC11 ]     0          5
12 [LC12 ]     0          5
13 [LC13 ]     0          5
20 [LOC-CP ] 23232     101339
21 [LOC-RP1]  5248       1097
22 [LOC-RP2]  5250       1104
23 [UNUSED ]     0          0
24 [REM-RPM] 12617      12630
FTOS#
```

Table 65-2 defines the fields displayed in **Figure 65-24**.

**Table 65-2. show hardware rpm mac counters Command Example Information**

<table>
<thead>
<tr>
<th>Slot ID #</th>
<th>Port number on the party-bus control switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Frames</td>
<td>Number of packets received by the party-bus switch from the processor in the specified slot.</td>
</tr>
<tr>
<td>TX Frames</td>
<td>Number of packets sent by the party-bus switch to the processor in the specified slot.</td>
</tr>
</tbody>
</table>
### show hardware rpm rp1/rp2
Display advanced debugging information for the RPM processors.

**Syntax**
```
show hardware rpm slot-number {rp1 | rp2} {data-plane | party-bus} {counters | statistics}
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>slot-number</code></td>
<td>Enter the RPM slot number 0 or 1.</td>
</tr>
<tr>
<td><code>rp1</code></td>
<td><code>rp2</code></td>
</tr>
<tr>
<td><code>data-plane</code></td>
<td>(OPTIONAL) Enter the keywords <code>data-plane</code> to display control processor information on the dataplane of the specified RPM.</td>
</tr>
<tr>
<td><code>party-bus</code></td>
<td>(OPTIONAL) Enter the keywords <code>party-bus</code> to display control processor information on the party-bus of the specified RPM.</td>
</tr>
<tr>
<td><code>counters</code></td>
<td>(OPTIONAL) Enter the keyword <code>counters</code> to display the standard Ethernet counters.</td>
</tr>
<tr>
<td><code>statistics</code></td>
<td>(OPTIONAL) Enter the keyword <code>statistics</code> to display driver-related counters.</td>
</tr>
</tbody>
</table>

**Defaults**
No default values or behavior

**Command Modes**
EXEC
EXEC Privilege

**Usage Information**
If the “dropped cell” field is non-zero, look for a pattern such as burstiness when the counters increment. It is normal to see a small number of continuous cell drops. Burstiness may indicate congestion on the internal switch at a particular point in time.

**Command History**
Version 6.5.4.0 Introduced

### show interfaces link-status
Displays 10-Gigabit Ethernet link fault signaling and port status information.

**Syntax**
```
show interfaces tenGigabitEthernet slot/port link-status
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tenGigabitEthernet</code></td>
<td>Enter the keyword <code>tenGigabitEthernet</code> followed by the slot/port information.</td>
</tr>
</tbody>
</table>

**Command Modes**
EXEC
EXEC Privilege

**Command History**
Version 6.5.4.0 Introduced
Example

Figure 65-25. show interfaces tengigabitethernet Command Example

```
FTOS#show interfaces tengigabitethernet 4/0 link-status
Port Status
  Loss of Signal: FALSE (XFP has power)
  RX Signal Lock Error: TRUE (Lock detected)
  PCS Link State: Down
  Link Faults
    Remote: None (No Fault)
    Local: Fault (Fault present)
    Idle Error: False (Not received)
    Illegal Symbol: False (Not received)
    Error Symbol: False (Not received)
FTOS#
```

Table 65-3 defines the information displayed in Figure 65-25.

Table 65-3. Lines in show interfaces tengigabitethernet Command Example

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Signal</td>
<td>Indicates if the interface has detected the required number of digital bit transitions (from 1 to 0 and 0 to 1) on the incoming signal. A 10 GE link must detect a certain number of such transitions for proper synchronization.</td>
</tr>
<tr>
<td>Rx Signal Lock Error</td>
<td>Indicates a loss of timing condition. The receive clock must be recovered from the incoming data stream to allow the receiving physical layer to synchronize with the incoming electrical pulses.</td>
</tr>
<tr>
<td>PCS Link State</td>
<td>Display the state of the PCS (Physical Coding sub-layer). The state is either up or down.</td>
</tr>
<tr>
<td>Link Fault Remote.</td>
<td>Indicates if the remote device has detected a fault, is inhibiting transmission of frames, and may be continuously transmitting idle messages.</td>
</tr>
<tr>
<td>Link Fault Local.</td>
<td>Indicates if a local fault is detected that may inhibit transmission of frames, and may be continuously transmitting remote fault signals.</td>
</tr>
<tr>
<td>Link Fault Idle Error</td>
<td>Indicates the detections of a non-idle symbol during an idle period.</td>
</tr>
<tr>
<td>Link Fault Illegal Symbol</td>
<td>Indicates the detections of an illegal symbol, other than an error symbol, while receiving data frames.</td>
</tr>
<tr>
<td>Link Fault Error Symbol</td>
<td>Indicates the detections of an error symbol while receiving data frames.</td>
</tr>
</tbody>
</table>

show logging driverlog

Display the driver log for the RPM CP processor or for the line card CPU in the specified slot.

Syntax

```
show logging driverlog [linecard number]
```

Parameters

<table>
<thead>
<tr>
<th>linecard number</th>
<th>(OPTIONAL) Enter the keyword linecard followed by the line card slot number to display the driver log for the specified line card.</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300</td>
</tr>
</tbody>
</table>

Defaults

No default values or behavior

Command Modes

<table>
<thead>
<tr>
<th>EXEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC Privilege</td>
</tr>
</tbody>
</table>
This command displays internal software driver information which may be useful during troubleshooting line card initialization errors, such as downed Port-Pipe.

**show running-config hardware-monitor**

Display the hardware-monitor action-on-error settings.

**Syntax**

```plaintext
show running-config hardware-monitor
```

**Defaults**

No default values or behavior

**Command Modes**

EXEC Privilege

**Command History**

Introduced in Version 6.5.4.0

Introduced in Version 7.8.1.0

**Example**

```plaintext
FTOS#show running-config hardware-monitor
!
hardware monitor mac action-on-error port-shutdown
hardware monitor linecard asic BTM action-on-error card-reset
hardware monitor linecard asic FPC action-on-error card-problem

FTOS#
```
S-Series 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, Dell Networking OS results are saved as a text file (TestReport-SU-X.txt) in the flash directory. This 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 console. In other words, you cannot run diagnostics on a unit to which you are connected via a stacking link.
- Diagnostic results are printed to the screen. Dell Networking OS does not write them to memory.
- 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 testname
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Enter the stack-unit number. Range: 0 to 7</td>
</tr>
<tr>
<td>alllevels</td>
<td>Enter the keyword <code>alllevels</code> to run the complete set of offline diagnostic tests.</td>
</tr>
<tr>
<td>level0</td>
<td>Enter the keyword <code>level0</code> to run Level 0 diagnostics. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.</td>
</tr>
</tbody>
</table>
### offline stack-unit

Place a stack unit in the offline state.

**Syntax**

```
offline stack-unit number
```

**Parameters**

- `number`: Enter the stack unit number.
  - Range: 0 to 7

**Defaults**

None

**Command Mode**

EXEC Privilege

**Command History**

- **Version 8.3.1.0**: Introduced the verbose option.
- **Version 7.7.1.0**: Introduced on S-Series

**Related Commands**

- `show environment (S-Series)`: View S-Series system component status (for example, temperature, voltage).

**Usage Information**

You cannot enter this command on a Master or Standby unit.

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 7

Defaults

None

Command Mode

EXEC Privilege

Command History

Version 7.7.1.0 Introduced on S-Series

Related Commands

```
show environment (S-Series) View S-Series system component status (for example, temperature, voltage).
```

Buffer Tuning Commands

The buffer tuning commands are:

- `buffer (Buffer Profile)`
- `buffer (Configuration)`
- `buffer-profile (Configuration)`
- `buffer-profile (Interface)`
- `show buffer-profile`
- `show buffer-profile interface`

⚠️ **Warning:** Altering the buffer allocations is a sensitive operation. Do not use any buffer tuning commands without first contacting the Dell Networking Technical Assistance Center.

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

dynamic

packets-pointers
```

Enter this keyword to configure the amount of dedicated buffer space per queue.

Enter this keyword to configure the amount of dynamic buffer space per Field Processor.

Enter this keyword to configure the number of packet pointers per queue.
buffer-profile (Configuration)

Apply a buffer profile to all Field or Switch Fabric processors in a port-pipe.

```plaintext
buffer [csf | fp-uplink] linecard slot port-set port-pipe buffer-policy buffer-profile
```

**Parameters**

- `csf`
  - Enter this keyword to apply a buffer profile to all Switch Fabric processors in a port-pipe.

- `fp-uplink`
  - Enter this keyword to apply a buffer profile to all Field Processors in a port-pipe.
buffer-profile (Configuration)

Create a buffer profile that can be applied to an interface.

Syntax

```
buffer-profile { {fp | csf} profile-name | global {1Q|4Q} }
```

Parameters

- **fp**: Enter this keyword to create a buffer profile for the Field Processor.
- **csf**: Enter this keyword to create a buffer profile for the Switch Fabric Processor.
- **profile-name**: Create a name for the buffer profile.
- **global**: Apply one of two pre-defined buffer profiles to all of the port-pipes in the system.
- **1Q**: Enter this keyword to choose a pre-defined buffer profile for single queue (i.e non-QoS) applications.
- **4Q**: Enter this keyword to choose a pre-defined buffer profile for four queue (i.e QoS) applications.

Defaults

```
global 4Q
```

Command Mode

```
CONFIGURATION
```
The `buffer-profile global` command fails if you have already applied a custom buffer-profile on an interface. Similarly, when `buffer-profile global` is configured, you cannot apply buffer-profile on any interface.

If the default buffer-profile (4Q) is active, Dell Networking OS displays an error message instructing you to remove the default configuration using the command `no buffer-profile global`.

You must reload the system for the global buffer-profile to take effect.

### buffer-profile (Interface)

**Syntax**

```
buffer-profile profile-name
```

**Parameters**

- `profile-name` Enter the name of the buffer profile you want to apply to the interface.

**Defaults**

None

**Command Mode**

`INTERFACE`

**Command History**

- Version 7.8.1.0 Added `global` keyword.
- Version 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series

**Related Commands**

- `buffer-profile (Configuration)` Create a buffer profile that can be applied to an interface.

### show buffer-profile

**Syntax**

```
show buffer-profile {detail | summary} {csf | fp-uplink}
```

**Parameters**

- `detail` Display the buffer allocations of the applied buffer profiles.
- `summary` Display the buffer-profiles that are applied to line card port-pipes in the system.
- `csf` Display the Switch Fabric Processor buffer profiles that you have applied to line card port-pipes in the system.
- `fp-uplink` Display the Field Processor buffer profiles that you have applied to line card port-pipes in the system.
show buffer-profile interface

Display the buffer profile that is applied to an interface.

Syntax

```
show buffer-profile {detail | summary} interface interface slot/port
```

Parameters

- **detail**
  - Display the buffer allocations of a buffer profile.
- **summary**
  - Display the Field Processors and Switch Fabric Processors that are applied to line card port-pipes in the system.
- **interface interface**
  - Enter the keyword interface followed by any one of the following interface type: `gigabitethernet`, `tengigabitethernet`, or `fortyGigE`.
- **slot/port**
  - Enter the slot and port number of the interface.

Defaults

None

Command Mode

INTERFACE

Command History

- Version 7.7.1.0 Introduced on S-Series
- Version 7.6.1.0 Introduced on C-Series
Figure 66-2. 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</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) Create a buffer profile that can be applied to an interface.

Hardware Commands

These commands display information from a hardware sub-component or ASIC.

The commands are:

- clear hardware system-flow
- clear hardware system-flow
- hardware watchdog
- 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 0–7 {counters | unit 0–1 counters | cpu data-plane statistics | cpu party-bus statistics | stack-port 0–52}
```

**Parameters**

- **stack-unit 0–7** Enter the keyword `stack-unit` followed by 0 to 7 to select a particular stack member and then enter one of the following command options to clear a specific collection of data.

- **counters** Enter the keyword `counters` to clear the counters on the selected stack member.

- **unit 0–1 counters** Enter the keyword `unit` along with a port-pipe number, from 0 to 1, followed by the keyword `counters` to clear the counters on the selected port-pipe.

**Note:** S25 models (S25N, S25P, S25V, etc.) have only port-pipe 0.
**clear hardware system-flow**

Clear system-flow statistics from selected hardware components.

**Syntax**
clear hardware system-flow layer2 stack-unit 0-7 port-set 0-1 counters

**Parameters**
- **stack-unit 0-7** Enter the keyword **stack-unit** followed by 0 to 7 to select a particular stack member and then enter one of the following command options to clear a specific collection of data.
- **port-set 0-1 counters** Enter the keyword **port-set** along with a port-pipe number, from 0 to 1, followed by the keyword **counters** to clear the system-flow counters on the selected port-pipe.

**Defaults**
No default behavior or values

**Command Modes**
EXEC Privilege

**Command History**
Version 7.8.1.0 Introduced on S-Series

**Related Commands**
show hardware stack-unit Display the data plane or management plane input and output statistics of the designated component of the designated stack member.

---

**hardware watchdog**

Set the watchdog timer to trigger a reboot and restart the system.
**Syntax**

`hardware watchdog`

**Defaults**

`Enabled`

**Command Mode**

`CONFIGURATION`

**Command History**

| Version 7.8.1.0 | Introduced |

**Usage Information**

This command enables a hardware watchdog mechanism that automatically reboots an Dell Networking OS switch/router with a single unresponsive unit. This is a last resort mechanism intended to prevent a manual power cycle.

### 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 0-7 port-set 0-1`

**Parameters**

- `stack-unit 0-7` Enter the keyword `stack-unit` followed by 0 to 7 to select a stack ID.
- `port-set 0-1` Enter the keyword `port-set` with a port-pipe number — 0 or 1. The S25 models of the S-Series have only port-pipe 0.

**Defaults**

No default behavior

**Command Modes**

EXEC Privilege

**Command History**

| Version 7.8.1.0 | Introduced on S-Series |

### 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 0-7 port-set 0-1`

**Parameters**

- `acl | qos` Enter either the keyword `acl` or the keyword `qos` to select between ACL or QoS data.
- `stack-unit 0-7` Enter the keyword `stack-unit` followed by a numeral from 0 to 7 to select a stack ID.
- `port-set 0-1` Enter the keyword `port-set` with a port-pipe number — 0 or 1. The S25 models of the S-Series have only port-pipe 0.

**Defaults**

No default behavior

**Command Modes**

EXEC Privilege

**Command History**

| Version 7.8.1.0 | Introduced on S-Series |
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

```plaintext
show hardware stack-unit 0-7 {cpu data-plane statistics [stack-port 0-52] | cpu party-bus statistics | drops [unit 0-1 [port 0-27]] | stack-port 0-52 | unit 0-1 {counters | details | port-stats [detail] | register}}
```

Parameters

- **stack-unit 0-7 {command-option}**: Enter the keyword `stack-unit` followed by 0 to 7 to select a particular stack member and then enter one of the following command options to display a collection of data based on the option entered.

- **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 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.

- **drops [unit 0-1 [port 0-27]]**: Enter the `drops` keyword to display internal drops on the selected stack member. Optionally, use the `unit` keyword with 0 or 1 to select port-pipe 0 or 1, and then use `port 0-27` to select a port on that port-pipe.

- **stack-port 0-52**: 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 0-1 {counters | details | port-stats [detail] | register}**: Enter the `unit` keyword followed by 0 or 1 for port-pipe 0 or 1, 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

No default behavior

Command Modes

- EXEC
- EXEC Privilege

Command History

- **Version 7.8.1.0**: Modified: `stack-port` keyword range expanded from 49-52 to 0-52; output modified for the `cpu data-plane statistics` option; the following options were added: `drops [unit 0-1 [port 0-27]] ; unit 0-1 {counters | details | port-stats [detail] | register}

- **Version 7.7.1.0**: Introduced on S-Series
Example 1
Figure 66-3. show hardware stack-unit cpu data-plane statistics Command Example

FTOS#show hardware stack-unit 0 cpu data-plane statistics stack-port 49
Input Statistics:
  1856 packets, 338262 bytes
  141 64-byte pkts, 1248 over 64-byte pkts, 11 over 127-byte pkts
  222 over 255-byte pkts, 236 over 511-byte pkts, 0 over 1023-byte pkts
  919 Multicasts, 430 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  325 packets, 27629 bytes, 0 underruns
  9 64-byte pkts, 310 over 64-byte pkts, 1 over 127-byte pkts
  1 over 255-byte pkts, 2 over 511-byte pkts, 2 over 1023-byte pkts
  0 Multicasts, 3 Broadcasts, 322 Unicasts
  0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
  Input 0.00 Mbits/sec
  Output 0.00 Mbits/sec
FTOS#

Example 2
Figure 66-4. 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 3
Figure 66-5. show hardware stack-unit drops Command Example

FTOS#show hardware stack-unit 0 drops unit 1 port 27
--- Ingress Drops      ---
  Ingress Drops                 : 0
  IBP CBF 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 FCS Drops             : 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 4**  
**Figure 66-6. show hardware stack-unit port-stats Command Example**

```plaintext
FTOS#show hardware stack-unit 0 unit 0 port-stats

<table>
<thead>
<tr>
<th>port</th>
<th>link</th>
<th>speed/</th>
<th>link</th>
<th>auto</th>
<th>STP</th>
<th>pause</th>
<th>discrd</th>
<th>lrn</th>
<th>inter</th>
<th>max</th>
<th>loop</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge0</td>
<td>down</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Block</td>
<td>Untag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge1</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Block</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge2</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Block</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge3</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Block</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge4</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge5</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge6</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge7</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge8</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge9</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge10</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge11</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge12</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge13</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge14</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge15</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge16</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge17</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge18</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge19</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge20</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge21</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge22</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge23</td>
<td>!ena</td>
<td>-</td>
<td>SW</td>
<td>Yes</td>
<td>Forward</td>
<td>Tag</td>
<td>FA</td>
<td>SGMI</td>
<td>1554</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hg0</td>
<td>up</td>
<td>12G FD</td>
<td>SW</td>
<td>No</td>
<td>Forward</td>
<td>None</td>
<td>F</td>
<td>XGMI</td>
<td>16360</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hg1</td>
<td>up</td>
<td>12G FD</td>
<td>SW</td>
<td>No</td>
<td>Forward</td>
<td>None</td>
<td>F</td>
<td>XGMI</td>
<td>16360</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hg2</td>
<td>down</td>
<td>10G FD</td>
<td>SW</td>
<td>No</td>
<td>Forward</td>
<td>None</td>
<td>F</td>
<td>XGMI</td>
<td>16360</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hg3</td>
<td>down</td>
<td>10G FD</td>
<td>SW</td>
<td>No</td>
<td>Forward</td>
<td>None</td>
<td>F</td>
<td>XGMI</td>
<td>16360</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FTOS# 0
```
Example 5  

**Figure 66-7. show hardware stack-unit unit 1 register Command Example**

FTOS#show hardware stack-unit 0 unit 1 register
0x0068003c AGINGCTRMEMDEBUG.mmu0 = 0x00000000
0x0068003d AGINGEXPMEMDEBUG.mmu0 = 0x00000000
0x00680017 ASFCONFIG.mmu0 = 0x00000000
0x0060004c ASFPORTSPEED.ge0 = 0x00000000
0x0060104c ASFPORTSPEED.ge1 = 0x00000000
0x0060204c ASFPORTSPEED.ge2 = 0x00000000
0x0060304c ASFPORTSPEED.ge3 = 0x00000000
0x0060404c ASFPORTSPEED.ge4 = 0x00000000
0x0060504c ASFPORTSPEED.ge5 = 0x00000000
0x0060604c ASFPORTSPEED.ge6 = 0x00000000
0x0060704c ASFPORTSPEED.ge7 = 0x00000000
0x0060804c ASFPORTSPEED.ge8 = 0x00000000
0x0060904c ASFPORTSPEED.ge9 = 0x00000000
0x0060a04c ASFPORTSPEED.ge10 = 0x00000000
0x0060b04c ASFPORTSPEED.ge11 = 0x00000000
0x0060c04c ASFPORTSPEED.ge12 = 0x00000000
0x0060d04c ASFPORTSPEED.ge13 = 0x00000000
0x0060e04c ASFPORTSPEED.ge14 = 0x00000000
0x0060f04c ASFPORTSPEED.ge15 = 0x00000000
0x0061004c ASFPORTSPEED.ge16 = 0x00000000
0x0061104c ASFPORTSPEED.ge17 = 0x00000000
0x0061204c ASFPORTSPEED.ge18 = 0x00000000
0x0061304c ASFPORTSPEED.ge19 = 0x00000000
0x0061404c ASFPORTSPEED.ge20 = 0x00000000
0x0061504c ASFPORTSPEED.ge21 = 0x00000000
0x0061604c ASFPORTSPEED.ge22 = 0x00000000
0x0061704c ASFPORTSPEED.ge23 = 0x00000000
0x0061804c ASFPORTSPEED.hg0 = 0x00000000
0x0061904c ASFPORTSPEED.hg1 = 0x00000000
0x0061a04c ASFPORTSPEED.hg2 = 0x00000000
0x0061b04c ASFPORTSPEED.hg3 = 0x00000000
0x0061c04c ASFPORTSPEED.cpu0 = 0x00000000
0x00780000 AUX_ARB_CONTROL.ipipe0 = 0x0000001c
0x0e700102 BCAST_BLOCK_MASK.ge0 = 0x00000000
0x0e701102 BCAST_BLOCK_MASK.ge1 = 0x00000000
0x0e702102 BCAST_BLOCK_MASK.ge2 = 0x00000000
0x0e703102 BCAST_BLOCK_MASK.ge3 = 0x00000000
0x0e704102 BCAST_BLOCK_MASK.ge4 = 0x00000000
0x0e705102 BCAST_BLOCK_MASK.ge5 = 0x00000000
0x0e706102 BCAST_BLOCK_MASK.ge6 = 0x00000000
0x0e707102 BCAST_BLOCK_MASK.ge7 = 0x00000000
0x0e708102 BCAST_BLOCK_MASK.ge8 = 0x00000000
0x0e709102 BCAST_BLOCK_MASK.ge9 = 0x00000000
0x0e70a102 BCAST_BLOCK_MASK.ge10 = 0x00000000
0x0e70b102 BCAST_BLOCK_MASK.ge11 = 0x00000000
0x0e70c102 BCAST_BLOCK_MASK.ge12 = 0x00000000
0x0e70d102 BCAST_BLOCK_MASK.ge13 = 0x00000000
0x0e70e102 BCAST_BLOCK_MASK.ge14 = 0x00000000
0x0e70f102 BCAST_BLOCK_MASK.ge15 = 0x00000000
0x0e710102 BCAST_BLOCK_MASK.ge16 = 0x00000000
0x0e711102 BCAST_BLOCK_MASK.ge17 = 0x00000000
0x0e712102 BCAST_BLOCK_MASK.ge18 = 0x00000000
0x0e713102 BCAST_BLOCK_MASK.ge19 = 0x00000000
0x0e714102 BCAST_BLOCK_MASK.ge20 = 0x00000000
0x0e715102 BCAST_BLOCK_MASK.ge21 = 0x00000000
0x0e716102 BCAST_BLOCK_MASK.ge22 = 0x00000000
0x0e717102 BCAST_BLOCK_MASK.ge23 = 0x00000000
0x0e718102 BCAST_BLOCK_MASK.hg0 = 0x00000000
0x0e719102 BCAST_BLOCK_MASK.hg1 = 0x00000000
0x0e71a102 BCAST_BLOCK_MASK.hg2 = 0x00000000
0x0e71b102 BCAST_BLOCK_MASK.hg3 = 0x00000000
0x0b700001 BCAST_STORM_CONTROL.ge0 = 0x00000000
0x0b701001 BCAST_STORM_CONTROL.ge1 = 0x00000000
0x0b702001 BCAST_STORM_CONTROL.ge2 = 0x00000000
0x0b703001 BCAST_STORM_CONTROL.ge3 = 0x00000000
0x0b704001 BCAST_STORM_CONTROL.ge4 = 0x00000000
0x0b705001 BCAST_STORM_CONTROL.ge5 = 0x00000000
0x0b706001 BCAST_STORM_CONTROL.ge6 = 0x00000000
0x0b707001 BCAST_STORM_CONTROL.ge7 = 0x00000000
0x0b708001 BCAST_STORM_CONTROL.ge8 = 0x00000000
0x0b709001 BCAST_STORM_CONTROL.ge9 = 0x00000000
0x0b70a001 BCAST_STORM_CONTROL.ge10 = 0x00000000
!------------------ output truncated ------------------!
Example 4  Figure 66-8.  show hardware stack-unit unit 1 details Command Example

FTOS# show hardware stack-unit 0 unit 1 details
****************************************************
The total no of FP & CSF Devices in the Card is 2
The total no of FP Devices in the Card is 2
The number of ports in device 0 is - 24
The number of Hg ports in devices 0 is - 4
The CPU Port of the device is 28
The number of ports in device 1 is - 24
The number of Hg ports in devices 1 is - 4
The CPU Port of the device is 28
The starting unit no the SWF in the device is 0
****************************************************
The Current Link Status Is
Front End Link Status 0x000000000000400000000000
Front End Port Present Status 0x000000000000000000000000
Back Plane Link Status 0x00000000
****************************************************
Link Status of all the ports in the Device - 1
The linkStatus of Front End Port 0 is FALSE
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 FALSE
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 TRUE
The linkStatus of Hg Port 24 is TRUE
The linkStatus of Hg Port 25 is TRUE
The linkStatus of Hg Port 26 is FALSE
The linkStatus of Hg Port 27 is FALSE
!------------------ output truncated -----------------!

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear hardware system-flow</td>
<td>Clear statistics from selected hardware components.</td>
</tr>
<tr>
<td>show interfaces stack-unit</td>
<td>Display statistics from all interfaces on a specific S-Series stack member.</td>
</tr>
<tr>
<td>show processes cpu (S-Series)</td>
<td>Display CPU usage information based on processes running in an S-Series.</td>
</tr>
<tr>
<td>show system stack-ports</td>
<td>Display information about the stacking ports on all switches in the S-Series stack.</td>
</tr>
<tr>
<td>show system (S-Series)</td>
<td>Display the current status of all stack members or a specific member.</td>
</tr>
</tbody>
</table>
show hardware system-flow

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax

```
show hardware system-flow layer2 stack-unit 0-7 port-set 0-1 [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 0-7**  
  Enter the keyword `stack-unit` followed by 0 to 7 to select a stack member ID.

- **port-set 0-1 [counters]**  
  Enter the keyword `port-set` with a port-pipe number — 0 or 1. The S25 models of the S-Series have only port-pipe 0. (OPTIONAL) Enter the keyword `counters` to display hit counters for the selected ACL or QoS option.

Defaults

No default behavior

Command Modes

EXEC Privilege

Command History

Version 7.8.1.0 Introduced on S-Series

Example 1

```
Figure 66-9.  show hardware system-flow layer2 counters Command Example

FTOS#show hardware system-flow layer2 stack-unit 0 port-set 0 counters
---------------------------------------------------------------------------
EntryId          Description                     #HITS
---------------------------------------------------------------------------
  2048            STP BPDU Redirects              0
  2047            LLDP BPDU Redirects             0
  2045            LACP traffic Redirects          0
  2044            GVRP traffic Redirects          0
  2043            ARP Reply Redirects             0
  2042            802.1x frames Redirects          0
  2041            VRRP frames Redirects            0
  2040            GRAT ARP                        0
  2039            DROP Cases                      0
  2038            OSPF1 STUB                      0
  2037            OSPF2 STUB                      0
  2036            VRRP STUB                       0
  2035            L2_DST_HIT+BC MAC+VLAN 4095      0
  2034            L2_DST_HIT+BC MAC               0
  2033            Catch all                       0
  384             OSPF[224.0.0.5] Packets          0
  383             OSPF[224.0.0.6] Packets          0
  382             VRRP Packets                   0
  380             BCast L2_DST_HIT on VLAN 4095    0
  379             BCast L2 DST_HIT Packets         0
  4               Unknown L2MC Packets             0
  3               L2DLF Packets                   0
  2               L2UCAST Packets                 0
  1               L2BCAST Packets                 0
  25
FTOS#
```
FTOS#show hardware system-flow layer2 stack-unit 0 port-set 0

Example 2 Figure 66-10. 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,
KEY=0x00000000 00000000 00000000 0180c200 00800000 00000000 00000000
, FPF4=0x00
0x00
action={act=Drop, 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,
KEY=0x00000000 00000000 00000000 0180c200 00e00000 00000000 00000000
, FPF4=0x00
0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
action={act=CopyToCpu, param0=7(0x07), 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,
KEY=0x00000000 00000000 00000000 0180c200 00200000 00000000 00000000
, FPF4=0x00
0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
action={act=CopyToCpu, param0=7(0x07), 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,
KEY=0x00000000 00000000 00000000 00000000 00000000 00008060 00016000
, FPF4=0x00
0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
action={act=CopyToCpu, param0=7(0x07), 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,
KEY=0x00000000 00000000 00000000 00000000 0008060 00016000
, FPF4=0x00
0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
action={act=CopyToCpu, param0=6(0x06), param1=0(0x00)},
action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
!--------- output truncated -----------------!
ICMP Message Types

This chapter lists and describes the possible ICMP Message Type 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 A-1. ICMP Messages and their definitions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
<th>Query</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td></td>
<td></td>
<td>Timeout (no reply)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>!</td>
<td>0</td>
<td>3</td>
<td>echo reply</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>U</td>
<td>3</td>
<td></td>
<td>destination unreachable:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td>network unreachable</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
<td>host unreachable</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>protocol unreachable</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
<td>port unreachable</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
<td>fragmentation needed but don’t fragment bit set</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td></td>
<td>source route failed</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td></td>
<td>destination network unknown</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td></td>
<td>destination host unknown</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td></td>
<td>source host isolated (obsolete)</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td></td>
<td>destination network administratively prohibited</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td></td>
<td>destination host administratively prohibited</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td></td>
<td>network unreachable for TOS</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td></td>
<td>host unreachable for TOS</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td></td>
<td>communication administratively prohibited by filtering</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td></td>
<td>host precedence violation</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>15</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></td>
<td>5</td>
<td></td>
<td>redirect</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td>redirect for network</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
<td>redirect for host</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>redirect for type-of-service and network</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
<td>redirect for type-of-service and host</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>0</td>
<td>echo request</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>0</td>
<td>router advertisement</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>0</td>
<td>router solicitation</td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>
Table A-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>&amp;</td>
<td>11</td>
<td>0</td>
<td>time exceeded:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>time-to-live equals 0 during transit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>time-to-live equals 0 during reassembly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>1</td>
<td>parameter problem:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>required option missing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>13</td>
<td>timestamp request</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>14</td>
<td>timestamp reply</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>0</td>
<td>information request (obsolete)</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>0</td>
<td>information reply (obsolete)</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>0</td>
<td>address mask request</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>0</td>
<td>address mask reply</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>
SNMP Traps

This chapter lists the traps sent by Dell Networking OS. Each trap is listed by the fields Message ID, Trap Type, and Trap Option, and the next is the message(s) associated with the trap.

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Trap Type</th>
<th>Trap Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLD_START</td>
<td>SNMP</td>
<td>COLDSTART</td>
</tr>
<tr>
<td>%SNMP-5-SNMP_COLD_START: 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></td>
<td></td>
<td></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: 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></td>
<td></td>
<td></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>%RPM0-P-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>%RPM0-P-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_RISHING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%RPM0-P-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>%RPM0-P-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>
<tr>
<td>RESV</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CHM_CARD_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-1-CARD_SHUTDOWN: %sLine card %d down - %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-CARD_DOWN: %sLine card %d down - %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_CARD_UP</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-LINECARDUP: %sLine card %d is up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_CARD_MISMATCH</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-3-CARD_MISMATCH: Mismatch: line card %d is type %s - type %s required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_CARD_PROBLEM</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_ALARM_CUTOFF</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_SFM_UP</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_SFM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_RPM_UP</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%RAM-6-RPM_STATE: RPM1 is in Active State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RAM-6-RPM_STATE: RPM0 is in Standby State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_RPM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-2-RPM_DOWN: RPM 0 down - hard reset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-RPM_DOWN: RPM 0 down - card removed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_RPM_PRIMARY</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%RAM-5-COLD_FAIlOVER: RPM Failover Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RAM-5-HOT_FAIlOVER: RPM Failover Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RAM-5-FAST_FAIlOVER: RPM Failover Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_SFM_ADD</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%TSM-5-SFM_DISCOVERY: Found SFM 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_SFM_REMOVE</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%TSM-5-SFM_REMOVE: Removed SFM 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_SFM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_SFM_DOWN_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-MAJOR_SFM_CLR: Major alarm cleared: Switch fabric up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_SFM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-2-MINOR_SFM: Minor alarm: No working standby SFM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_SFM_DOWN_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-MINOR_SFM_CLR: Minor alarm cleared: Working standby SFM present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_PWRSRC_DOWN</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>CHM_PWRSRC_CLR</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-5-PEM_OK: Major alarm cleared: power entry module %s is good</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_ALARM_PS</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-0-MAJOR_PS: Major alarm: insufficient power %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_ALARM_PS_CLR</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-5-MAJOR_PS_CLR: major alarm cleared: sufficient power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALARM_PS</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-1-MINOR_PS: Minor alarm: power supply non-redundant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALARM_PS_CLR</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-5-MINOR_PS_CLR: Minor alarm cleared: power supply redundant</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>%CHMGR-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 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>CHM_FANTRAY_BAD</td>
<td>ENVMON</td>
<td>FAN</td>
</tr>
<tr>
<td>For E1200: %CHMGR-2-FAN_TRAY_BAD: Major alarm: fan tray %d is missing or down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For E600 and E300: %CHMGR-2-FANTRAYBAD: Major alarm: fan tray is missing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-FANSBAD: Major alarm: most or all fans in fan tray are down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_FANTRAY_BAD_CLR</td>
<td>ENVMON</td>
<td>FAN</td>
</tr>
<tr>
<td>For the E1200: %CHMGR-5-FAN_TRAY_OK: Major alarm cleared: fan tray %d present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For the E600 and E300: %CHMGR-5-FANTRAYOK: Major alarm cleared: fan tray present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_FANBAD</td>
<td>ENVMON</td>
<td>FAN</td>
</tr>
<tr>
<td>For the E1200: %CHMGR-2-FAN_BAD: Minor alarm: some fans in fan tray %d are down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For the E600 and E300: %CHMGR-2-1FANBAD: Minor alarm: fan in fan tray is down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_FANBAD_CLR</td>
<td>ENVMON</td>
<td>FAN</td>
</tr>
<tr>
<td>For E1200: %CHMGR-2-FAN_OK: Minor alarm cleared: all fans in fan tray %d are good</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For E600 and E300: %CHMGR-5-FANOK: Minor alarm cleared: all fans in fan tray are good</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>
</tbody>
</table>

Table B-1. SNMP Traps and Error Messages (continued)
### Table B-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>%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MEM_THRESHOLD_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_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_BADAUTH</td>
<td>PROTO</td>
<td>NONE</td>
</tr>
<tr>
<td>%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication type mismatch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 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>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>
</tbody>
</table>