

FTOS Command Line Reference Guide FTOS 8.4.1.5

Publication Date: August 2012



Notes, Cautions, and Warnings



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



CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



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

Information in this publication is subject to change without notice.

© 2011 Dell Force10. All rights reserved.

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

Trademarks used in this text: Dell™, the DELL logo, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core™ and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™, and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE™ is a trademark of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter®, and vSphere® are registered trademarks or trademarks of VMWare, Inc. in the United States or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

3	About this Guide	15
	Objectives	15
	Audience	15
	Conventions	15
	Information Symbols	16
	Related Documents	16
4	CLI Basics	17
	Accessing the Command Line	17
	Multiple Configuration Users	17
	Navigating the Command Line Interface	18
	Obtaining Help	19
	Using the Keyword No	21
	Filtering show Commands	21
	Displaying All Output	21
	Filtering Command Output Multiple Times	21
	Command Modes	22
	EXEC Mode	22
	EXEC Privilege Mode	22
	CONFIGURATION Mode	22
	INTERFACE Mode	22
	LINE Mode	23
	TRACE-LIST Mode	23
	MAC ACCESS LIST Mode	23
	IP ACCESS LIST Mode	24
	ROUTE-MAP Mode	24
	PREFIX-LIST Mode	24
	AS-PATH ACL Mode	24
	IP COMMUNITY LIST Mode	25
	REDIRECT-LIST Mode	25
	SPANNING TREE Mode	25
	Per-VLAN SPANNING TREE Plus Mode	25
	RAPID SPANNING TREE Mode	26
	MULTIPLE SPANNING TREE Mode	26
	PROTOCOL GVRP Mode	26
	ROUTER OSPF Mode	26
	ROUTER RIP Mode	26
	ROUTER ISIS Mode	27
	ROUTER BGP Mode	27
	Determining the Chassis Mode	27
5	File Management	29
	Overview	29
	Basic File Management Commands	29
	Upgrading the C-Series FPGA	59

6	BOOT_USER Mode	61
	Overview	61
	Commands	61
7	Control and Monitoring	75
	Overview	75
	Commands	75
8	802.1ah	161
	Overview	161
	Commands	161
9	802.1X	173
	Important Points to Remember	173
10	Access Control Lists (ACL)	187
	Overview	187
	Commands Common to all ACL Types	187
	Common IP ACL Commands	190
	Standard IP ACL Commands	193
	Extended IP ACL Commands	200
	Common MAC Access List Commands	230
	Standard MAC ACL Commands	233
	Extended MAC ACL Commands	237
	IP Prefix List Commands	242
	Route Map Commands	249
	AS-Path Commands	266
	IP Community List Commands	269
11	ACL VLAN Group	275
	Overview	275
	Commands	275
12	Bidirectional Forwarding Detection (BFD)	281
	Overview	281
	Commands	281
13	Border Gateway Protocol IPv4 (BGPv4)	293
	Overview	293
	BGPv4 Commands	293
	MBGP Commands	371

	BGP Extended Communities (RFC 4360)	399
14	Content Addressable Memory (CAM) for ExaScale	409
	Overview	409
	Commands	409
	Important Points to Remember	409
15	Content Addressable Memory (CAM)	415
	Overview	415
	CAM Profile Commands	415
	Important Points to Remember	415
	CAM IPv4flow Commands	426
	CAM Layer 2 ACL Commands	428
16	Configuration Rollback.	431
	Overview	431
	Commands	431
17	Dynamic Host Configuration Protocol (DHCP)	441
	Overview	441
	Commands to Configure the System to be a DHCP Server	441
	Commands to Configure Secure DHCP	448
18	Equal Cost Multi-Path	455
	Overview	455
	Commands	455
19	Far-End Failure Detection (FEFD).	461
	Overview	461
	Commands	461
20	Force10 Resilient Ring Protocol (FRRP).	467
	Overview	467
	Commands	467
	Important Points to Remember	467
21	Force10 Service Agent	475
	Overview	475
	Commands	475

22	GARP VLAN Registration (GVRP)	505
	Overview	505
	Commands	505
	Important Points to Remember	506
23	High Availability (HA)	515
	Overview	515
	Commands	515
24	Internet Group Management Protocol (IGMP)	525
	Overview	525
	IGMP Commands	525
	Important Points to Remember	525
	IGMP Snooping Commands	534
	Important Points to Remember for IGMP Snooping	535
	Important Points to Remember for IGMP Querier	535
25	Interfaces	541
	Overview	541
	Basic Interface Commands	541
	Port Channel Commands	593
	Time Domain Reflectometer (TDR)	602
	Important Points to Remember	602
	UDP Broadcast	604
	Important Points to Remember	604
26	IPv4 Routing	607
	Overview	607
	Commands	607
27	IPv6 Access Control Lists (IPv6 ACLs)	657
	Overview	657
	Important Points to Remember	657
	IPv6 ACL Commands	657
	IPv6 Route Map Commands	680
28	IPv6 Basics	685
	Overview	685
	Commands	685

29	IPv6 Border Gateway Protocol (IPv6 BGP)	701
	Overview	701
	IPv6 BGP Commands	701
	IPv6 MBGP Commands	761
30	Intermediate System to Intermediate System (IS-IS)	787
	Overview	787
	Commands	787
31	Link Aggregation Control Protocol (LACP)	829
	Overview	829
	Commands	829
32	Layer 2	835
	Overview	835
	MAC Addressing Commands	835
	Virtual LAN (VLAN) Commands	853
33	Link Layer Detection Protocol (LLDP)	863
	Overview	863
	Commands	863
	LLDP-MED Commands	871
34	Multicast Listener Discovery (MLD)	879
	Overview	879
	MLD Commands	879
	MLD Snooping Commands	885
35	Multicast Source Discovery Protocol (MSDP)	891
	Overview	891
	Commands	891
36	Multiple Spanning Tree Protocol (MSTP)	901
	Overview	901
	Commands	901
37	Multicast	915
	Overview	915
	IPv4 Multicast Commands	915
	IPv6 Multicast Commands	924

38	Neighbor Discovery Protocol (NDP)	931
	Overview	931
	Commands	931
39	Object Tracking	939
	Overview	939
	IPv4 Object Tracking Commands	939
	IPv6 Object Tracking Commands	951
40	Open Shortest Path First (OSPFv2 and OSPFv3)	957
	Overview	957
	OSPFv2 Commands	958
	OSPFv3 Commands	1013
41	Policy-based Routing (PBR)	1033
	Overview	1033
	Commands	1033
42	PIM-Dense Mode (PIM-DM)	1041
	Overview	1041
	IPv4 PIM-Dense Mode Commands	1041
43	PIM-Sparse Mode (PIM-SM)	1043
	Overview	1043
	IPv4 PIM-Sparse Mode Commands	1043
	IPv6 PIM-Sparse Mode Commands	1064
44	PIM-Source Specific Mode (PIM-SSM)	1075
	Overview	1075
	IPv4 PIM Commands	1075
	IPv4 PIM-Source Specific Mode Commands	1075
	IPv6 PIM Commands	1077
	IPv6 PIM-Source Specific Mode Commands	1077
45	Power over Ethernet (PoE)	1079
	Overview	1079
	Commands	1079
46	Port Monitoring	1085
	Overview	1085
	Commands	1085

	Important Points to Remember	1085
47	Private VLAN (PVLAN)	1091
	Overview	1091
	Commands	1091
	Private VLAN Concepts	1091
48	Per-VLAN Spanning Tree plus (PVST+)	1101
	Overview	1101
	Commands	1101
49	Quality of Service (QoS)	1113
	Overview	1113
	Global Configuration Commands	1113
	Per-Port QoS Commands	1114
	Policy-Based QoS Commands	1122
	Important Points to Remember—multicast-bandwidth option	1135
	Queue-Level Debugging	1157
50	Router Information Protocol (RIP)	1167
	Overview	1167
	Commands	1167
51	Remote Monitoring (RMON)	1185
	Overview	1185
	Commands	1185
52	Rapid Spanning Tree Protocol (RSTP)	1197
	Overview	1197
	Commands	1197
53	Security	1207
	Overview	1207
	Commands	1207
	AAA Accounting Commands	1207
	Authorization and Privilege Commands	1210
	Authentication and Password Commands	1215
	RADIUS Commands	1226
	TACACS+ Commands	1231
	Port Authentication (802.1X) Commands	1233
	Important Points to Remember	1234

	SSH Server and SCP Commands	1242
	Trace List Commands	1253
	Secure DHCP Commands	1262
54	Service Provider Bridging	1267
	Overview	1267
	Commands	1267
	Important Points to Remember	1267
55	sFlow	1273
	Overview	1273
	Important Points to Remember	1273
	Commands	1274
56	SNMP and Syslog	1283
	Overview	1283
	SNMP Commands	1283
	Important Points to Remember	1284
	Syslog Commands	1300
57	SONET	1311
	Overview	1311
	Commands	1311
58	S-Series Stacking Commands	1329
	Overview	1329
	Commands	1329
59	Storm Control	1337
	Overview	1337
	Commands	1337
	Important Points to Remember	1337
60	Spanning Tree Protocol (STP)	1345
	Overview	1345
	Commands	1345
61	Time and Network Time Protocol (NTP)	1355
	Overview	1355
	Commands	1355

62	VLAN Stacking	1371
	Overview	1371
	Commands	1371
	Important Points to Remember	1371
63	Virtual Routing and Forwarding (VRF)	1381
	Overview	1381
	Commands	1381
64	Virtual Router Redundancy Protocol (VRRP)	1391
	Overview	1391
	IPv4 VRRP Commands	1391
	IPv6 VRRP Commands	1403
65	E-Series ExaScale Debugging and Diagnostics	1407
	Overview	1407
	Diagnostics and Monitoring Commands	1407
	Important Points to Remember	1408
	Offline Diagnostic Commands	1424
	Hardware Commands	1427
66	E-Series Debugging and Diagnostics	1449
	Overview	1449
	Diagnostics and Monitoring Commands	1449
	Important Points to Remember	1450
	Offline Diagnostic Commands	1468
	Hardware Commands	1471
67	ICMP Message Types	1487
68	SNMP Traps	1489
69	Index	1493
70	Command Index	1513

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 Force10 systems supported by FTOS (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 FTOS 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:

Convention	Description
keyword	Keywords are in bold and should be entered in the CLI as listed.
<i>parameter</i>	Parameters are in italics and require a number or word to be entered in the CLI.
{X}	Keywords and parameters within braces must be entered in the CLI.
[X]	Keywords and parameters within brackets are optional.
x y	Keywords and parameters separated by bar require you to choose one.
x y	Keywords and parameters separated by a double bar enables you to choose any or all of them.

Information Symbols

Table 3-1, "Information Symbols," in [About this Guide](#) describes symbols contained in this guide.

Table 3-1. Information Symbols

Symbol	Brief	Description
	Note	This symbol signals important operational information.
	Caution	This symbol indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.
	Warning	This symbol signals information about hardware handling that could result in injury.
	C-Series	This symbol indicates that the selected feature is supported on the C-Series.
	E-Series	This symbol indicates that the selected feature is supported on the E-Series TeraScale AND E-Series ExaScale.
	E-Series TeraScale	This symbol indicates that the selected feature is supported on the E-Series TeraScale platform only.
	E-Series ExaScale	This symbol indicates that the selected feature is supported on the E-Series ExaScale platform only.
	S-Series	This symbol indicates that the selected feature is supported on the S-Series.

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 FTOS version

CLI Basics

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.

The following text is an example of a successful Telnet login session.

```
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 4-2, "Command Prompt and Corresponding Command Mode,"](#) in CLI Basics).

Multiple Configuration Users

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

```
FTOS#conf

% Warning: The following users are currently configuring the system:

User "" on line console0
User "admin" on line vty0 ( 123.12.1.123 )
User "admin" on line vty1 ( 123.12.1.123 )
User "Irene" on line vty3 ( 123.12.1.321 )
```

```
FTOS (conf) #
```

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

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

Navigating the Command Line Interface

The Command Line Interface (CLI) prompt displayed by FTOS is comprised of:

- “hostname”— the initial part of the prompt, “FTOS” by default. You can change it with the **hostname** command, as described in [hostname](#).
- The second part of the prompt, reflecting the current CLI mode, as shown in [Table 4-2, "Command Prompt and Corresponding Command Mode," in CLI Basics](#).

The CLI prompt changes as you move up and down the levels of the command structure. [Table 4-2, "Command Prompt and Corresponding Command Mode," in CLI Basics](#) 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 4-2. Command Prompt and Corresponding Command Mode

Prompt	CLI Command Mode
FTOS>	EXEC
FTOS#	EXEC Privilege
FTOS(conf)#	CONFIGURATION
FTOS(conf-if)#	INTERFACE
FTOS(conf-if-gi-0/0)#	
FTOS(conf-if-te-0/0)#	
FTOS(conf-if-lo-0)#	
FTOS(conf-if-nu-0)#	
FTOS(conf-if-po-0)#	
FTOS(conf-if-vl-0)#	
FTOS(conf-if-so-0/0)#	
FTOS(conf-if-ma-0/0)#	
FTOS(conf-if-range)#	
FTOS(config-ext-nacl)#	IP ACCESS LIST
FTOS(config-std-nacl)#	
FTOS(config-line-aux)#	LINE
FTOS(config-line-console)#	
FTOS(config-line-vty)#	
FTOS(config-ext-macl)#	MAC ACCESS LIST
FTOS(config-std-macl)#	
FTOS(config-mon-sess)#	MONITOR SESSION
FTOS(config-span)#	STP

Table 4-2. Command Prompt and Corresponding Command Mode

Prompt	CLI Command Mode
FTOS(config-mstp)#	MULTIPLE SPANNING TREE
FTOS(config-pvst)#	Per-VLAN SPANNING TREE Plus
FTOS(config-rstp)#	RAPID SPANNING TREE
FTOS(config-gvrp)#	PROTOCOL GVRP
FTOS(config-route-map)#	ROUTE-MAP
FTOS(conf-nprefixl)#	PREFIX-LIST
FTOS(conf-router_rip)#	ROUTER RIP
FTOS(conf-redirect-list)#	REDIRECT
FTOS(conf-router_bgp)#	ROUTER BGP
FTOS(conf-router_ospf)#	ROUTER OSPF
FTOS(conf-router_isis)#	ROUTER ISIS
FTOS(conf-trace-acl)#	TRACE-LIST

Obtaining Help

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

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

The following text describes the results of entering **ip ?** at the prompt.

```

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
pim                  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	SSH 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 interface** 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 FTOS command line. (Table 4-3) defines the key combinations valid at the FTOS command line.

Table 4-3. Short-cut Keys and their Actions

Shortcut	Action
CNTL-A	Moves the cursor to the beginning of the command line.
CNTL-B	Moves the cursor back one character.
CNTL-D	Deletes character at cursor.
CNTL-E	Moves the cursor to the end of the line.
CNTL-F	Moves the cursor forward one character.
CNTL-I	Completes a keyword.
CNTL-K	Deletes all characters from the cursor to the end of the command line.
CNTL-L	Re-enters the previous command.
CNTL-N	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key
CNTL-P	Recalls commands, beginning with the last command
CNTL-R	Re-enters the previous command.
CNTL-U	Deletes the line.
CNTL-W	Deletes the previous word.
CNTL-X	Deletes the line.
CNTL-Z	Ends continuous scrolling of command outputs.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Esc D	Deletes all characters from the cursor to the end of the word.

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



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

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

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

- `show run | grep Ethernet` 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. Refer to 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 4-4, "Interface prompts," in CLI Basics](#).

Table 4-4. Interface prompts

Prompt	Interface Type
FTOS(conf-if)#	INTERFACE mode
FTOS(conf-if-gi-0/0)#	Gigabit Ethernet interface followed by slot/port information
FTOS(conf-if-te-0/0)#	Ten Gigabit Ethernet interface followed by slot/port information
FTOS(conf-if-lo-0)#	Loopback interface number.
FTOS(conf-if-nu-0)#	Null Interface followed by zero
FTOS(conf-if-po-0)#	Port-channel interface number
FTOS(conf-if-vl-0)#	VLAN Interface followed by VLAN number (range 1 to 4094)
FTOS(conf-if-so-0/0)#	SONET interface followed by slot/port information.
FTOS(conf-if-ma-0/0)#	Management Ethernet interface followed by slot/port information
FTOS(conf-if-range)#	Designated interface range (used for bulk configuration; refer to interface range).

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 change 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.

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. Refer to [Chapter 10, 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. Refer to [Chapter 10, 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 41, 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 60, 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 48, 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 52, 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 36, 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 22, 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 40, 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 50, 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 13, 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 FTOS 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 FTOS. 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 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 \(S-Series management unit\)](#)
- [upgrade fpga-image](#)

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

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 ([copy running-config startup-config](#) or [write](#)).

Dell Force10 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

[show bootvar](#) Display the variable settings for the E-Series boot parameters.

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

C **E** Set the location of the configuration file in a remote network.

Syntax `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

C **E** Tell the system where to access the FTOS image used to boot the system.

Syntax `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.

primary After entering **rpm0** or **rpm1**, enter the keyword **primary** to configure the boot parameters used in the first attempt to boot FTOS.

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**

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) and reload system.

Related Commands

- [change bootflash-image](#) Change the primary, secondary, or default boot image configuration.
- [boot system gateway](#) Specify the IP address of the default next-hop gateway for the management subnet.

boot system gateway

C E Specify the IP address of the default next-hop gateway for the management subnet.

Syntax **boot system gateway** *ip-address*

Parameters *ip-address* Enter an IP address in dotted decimal format.

Command Modes CONFIGURATION

Usage Information Saving the address to the startup configuration file preserves the address in NVRAM in case the startup configuration file is deleted.

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

Related Commands [change bootflash-image](#) Change the primary, secondary, or default boot image configuration.

cd

C E S

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

C E

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. FTOS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the *hostip* field).

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

Parameters

file-url

Enter the following location keywords and information:

- To copy a file from the internal FLASH, enter **flash://** followed by the filename.
- To copy a file on an FTP server, enter **ftp://user:password@hostip/filepath**
- To copy a file from the internal FLASH on RPM0, enter **rpm0flash://filepath**
- To copy a file from the external FLASH on RPM0, enter **rpm0slot0://filepath**
- To copy a file from the internal FLASH on RPM1, enter **rpm1flash://filepath**
- To copy a file from the external FLASH on RPM1, enter **rpm1slot0://filepath**
- To copy the running configuration, enter the keyword **running-config**.
- To copy the startup configuration, enter the keyword **startup-config**.
- To copy using Secure Copy (SCP), enter the keyword **scp**: (If **scp**: is entered in the source position, then enter the target URL; If **scp**: is entered in the target position, first enter the source URL; refer to the text below for examples.)
- To copy a file on the external FLASH, enter **slot0://** followed by the filename.
- To copy a file on a TFTP server, enter **tftp://hostip/filepath**

ExaScale only

- To copy a file from a USB drive on RPM0, enter **rpm0usbflash://filepath**
- To copy a file from an external USB drive, enter **usbflash://filepath**

Command Modes

EXEC Privilege

Command History

Version 8.4.1.0	Added IPv6 addressing support for FTP, TFTP, and SCP.
Version 8.2.1.0	Added usbflash and rpm0usbflash commands on E-Series ExaScale
Version 7.6.1.0	Introduced on S-Series and added SSH port number to SCP prompt sequence on all systems.
Version 7.5.1.0	Introduced on C-Series
E-Series original Command	

Usage Information

FTOS 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 FTOS 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 FTOS prompts you for the rest of the information.

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

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

When you use the **copy running-config startup-config** command to copy the running configuration (the startup configuration file amended by any configuration changes made since the system was started) to the startup configuration file, FTOS creates a backup file on the internal flash of the startup configuration.

FTOS supports copying the running-configuration to a TFTP server or to an FTP server:

copy running-config tftp:

copy running-config ftp:

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

cd

Change working directory.


copy (Streamline Upgrade)

(C) (E) 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

<i>source-url</i>	Enter the source file in url format. The source file is a valid Dell Force10 release image. Image validation is automatic.
<i>target-url</i>	Enter the local target file in url format.
boot-image	Enter the keyword boot-image to designate this copy command as a streamline update.
synchronize-rpm	Enter the keyword synchronize-rpm to copy the new image file to the peer RPM.
external	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

Defaults	No default behavior
Command Modes	CONFIGURATION
Command History	<p>Version 8.4.1.0 Added IPv6 addressing support for FTP, TFTP, and SCP.</p> <p>Version 7.5.1.0 Introduced on C-Series</p> <p>Version 6.1.1.0 Introduced</p>
Usage Information	<p>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.</p> <p>FTOS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP.</p> <p> Note: The keywords boot-image, synchronize-rpm, and external can be used on the Primary RPM only.</p>

copy running-config startup-config

  Copy running configuration to the startup configuration.

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

Command Modes EXEC Privilege

Command History




Version 7.5.1.0 Introduced on C-Series

Version 6.3.1.0 Introduced

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, FTOS 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 FTOS 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

C **E** **S** 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

E-Series original Command

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

C **E** 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

E-Series original Command

Usage Information Starting with FTOS 7.7.1.0, the functions of this command are incorporated into the **upgrade** command.

For software upgrade details, refer to the FTOS 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

E Download an alternate FTOS image to the chassis.

Syntax **download alt-full-image** *file-url*

Command Modes EXEC Privilege

Command History

Version 7.7.1.0	Removed form E-Series
Version 6.5.1.0	Introduced

Usage Information Starting with FTOS 7.7.1.0, the functions of this command are incorporated into the **upgrade** command.

For software upgrade details, refer to the FTOS Release Notes.

Related Commands

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

download alt-system-image

E 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

Version 7.7.1.0	Removed from E-Series
Version 6.5.1.0	Introduced

Usage Information Starting with FTOS 7.7.1.0, the functions of this command are incorporated into the **upgrade** command.

For software upgrade details, refer to the FTOS Release Notes.

Related Commands

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

format (C-Series and E-Series)

C **E** 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:

- The startup-config is erased.
- All cacheboot data files are erased and you must reconfigure cacheboot to regain it.
- All generated SSH keys are erased and you must recreate them.
- All archived configuration files are erased.
- All trace logs, crash logs, core dumps, and call-home logs are erased.
- 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	copy	Copy the current configuration to either the startup-configuration file or the terminal.
	show file	Display contents of a text file in the local filesystem.
	show file-systems	Display information about the file systems on the system.

logging coredump

C **E** Enable coredump.

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

Parameters	cp	Enable coredump for the CP.
	linecard	Enable coredump for a linecard.
	rps	Enable coredump for RP 1 and 2.

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	Version 7.7.1.0	Restructured command to accommodate core dumps for CP. Introduced on C-Series and S-Series
	Version 6.5.1.0	Application coredump naming convention enhanced to include application.
	Version 6.1.1.0	Introduced

Usage Information The Kernel core dump can be large and may take up to 5 to 30 minutes to upload. FTOS 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. FTOS completes the coredump process and wait until the upload is complete before rebooting the system.

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

logging coredump server



Designate a server to upload core dumps.

Syntax `logging coredump server { ipv4-address | ipv6-address } username name password [type] password`

Parameters

<code>{ ipv4-address ipv6-address }</code>	Enter the server IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).
<code>name</code>	Enter a username to access the target server.
<code>type</code>	Enter the password type: <ul style="list-style-type: none"> • Enter 0 to enter an unencrypted password. • Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.
<code>password</code>	Enter a password to access the target server.


Defaults Crash kernel files are uploaded to flash by default.

Command Modes CONFIGURATION

Command History

Version 8.4.1.0	Added support for IPv6.
Version 7.7.1.0	Restructured command to accommodate core dumps for CP. Introduced on C-Series and S-Series.
Version 6.1.1.0	Introduced

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

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

Example

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

Related Commands `cd` Change directory.

rename

C E S 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

C E 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:
=====
```

Type	Boot Type	A	B
CP	DOWNLOAD BOOT	invalid	invalid
RP1	DOWNLOAD BOOT	invalid	invalid

```

RP2          DOWNLOAD BOOT invalid          invalid
linecard 0 is not present.
linecard 1   DOWNLOAD BOOT invalid          invalid
linecard 2   DOWNLOAD BOOT 4.7.5.387       6.5.1.8
linecard 3   DOWNLOAD BOOT invalid          invalid
linecard 4   DOWNLOAD BOOT invalid          invalid
linecard 5 is not present.

```

Peer RPM:

```
=====
```

Type	Boot Type	A	B
CP	DOWNLOAD BOOT	invalid	invalid
RP1	DOWNLOAD BOOT	invalid	invalid
RP2	DOWNLOAD BOOT	invalid	invalid

show bootvar

C **E** 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#

```

Related Commands

boot config	Set the location of configuration files on local devices.
boot host	Set the location of configuration files from the remote host.
boot network	Set the location of configuration files from a remote network.

- [boot system](#) Set the location of FTOS image files.
- [boot system gateway](#) Specify the IP address of the default next-hop gateway for the management subnet.

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://:@\
!
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

- [format \(C-Series and E-Series\)](#) Erase all existing files and reformat a filesystem on the E-Series or C-Series platform.
- [format flash \(S-Series\)](#) Erase all existing files and reformat the filesystem in the internal flash memory on and S-Series.

[show file-systems](#)

Display information about the file systems on the system.

show file-systems



Display information about the file systems on the system.

Syntax `show file-systems`**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: **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:
FTOS#

```

show file-systems Command Output Fields

Field	Description
size(b)	Lists the size in bytes of the storage location. If the location is remote, no size is listed.
Free(b)	Lists the available size in bytes of the storage location. If the location is remote, no size is listed.
Feature	Displays the formatted DOS version of the device.
Type	Displays the type of storage. If the location is remote, the word network is listed.
Flags	Displays the access available to the storage location. The following letters indicate the level of access: <ul style="list-style-type: none"> 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

C **E** View the current linecard status.

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

Parameters

number	Enter a number to view information on that linecard. Range: 0 to 6.
all	(OPTIONAL) Enter the keyword all to view a table with information on all present linecards.
boot-information	(OPTIONAL) Enter the keyword boot-information to view cache boot information of all line cards in table format.

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**

#	Status	CurType	Serial number	Booted from	Next boot	Cache boot	Boot flash
0	-						
1	online	EXW10SH	FX000049121	8-4-1-317	8-4-1-317	A: 8-4-1-213 B:	A: 2.9.1.1c B: 2.9.2.0E0 [b]
2	-						
3	online	EXW10SJ	FX000097669	8-4-1-317	8-4-1-317	A: 8-4-1-305 B: invalid	A: 2.9.1.1 [b] B: 2.9.1.1
4	online	E90MH	FX000046835	8-4-1-317	8-4-1-317	A: 8-4-1-213 B: invalid	A: 2.9.1.1 B: 2.9.1.1 [b]
5	-						
6	online	E90MH	FX000044725	8-4-1-317	8-4-1-317	A: 8-4-1-213 B: invalid	A: 2.9.1.1 [b] B: 2.9.1.1

show os-version

C **E** **S** 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 `show os-version [file-url]`

Parameters

file-url (OPTIONAL) Enter the following location keywords and information:

- For a file on the internal Flash, enter **flash://** followed by the filename.
- For a file on an FTP server, enter **ftp://user:password@hostip/filepath**
- For a file on 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

Usage Information

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         route processor  passed
runtime           7.5.1.0         terascale linecard passed
boot flash        2.4.1.1         control processor passed
boot flash        2.4.1.1         route processor  passed
boot flash        2.3.1.3         terascale linecard passed
boot selector     2.4.1.1         control processor passed
boot selector     2.4.1.1         route processor  passed
boot selector     2.3.1.3         terascale 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 (OPTIONAL) Enter one of the keywords listed below to display that entity's current (non-default) configuration. Note that, if nothing is configured for that entity, nothing is displayed and the prompt returns:

- **aaa** for the current AAA configuration
- **acl** for the current ACL configuration
- **arp** for the current static ARP configuration
- **as-path** for the current AS-path configuration
- **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
- **fehd** 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
- **mac-address-table** for the current MAC configuration
- **management-route** for the current Management port forwarding configuration
- **mroute** for the current Mroutes configuration
- **ntp** for the current NTP configuration
- **ospf** for the current OSPF configuration
- **pim** for the current PIM configuration
- **policy-map-input** for the current input policy map configuration
- **policy-map-output** for the current output policy map configuration
- **prefix-list** for the current prefix-list configuration
- **privilege** for the current privilege configuration
- **radius** for the current RADIUS configuration
- **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
- **snmp** for the current SNMP configuration
- **spanning-tree** for the current spanning tree configuration
- **static** for the current static route configuration
- **tacacs+** for the current TACACS+ configuration
- **tftp** for the current TFTP configuration
- **trace-group** for the current trace-group configuration
- **trace-list** for the current trace-list configuration
- **users** for the current users configuration
- **wred-profile** for the current wred-profile configuration

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

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

Command Modes EXEC Privilege

Command History

Version 7.8.1.0	Added hardware-monitor option
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 include last configuration change and start-up last updated (date and time) and who made the change
Version 6.5.4.0	Added status option

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
!
...
```

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

```
FTOS#show running-config status

running-config checksum 0xB4B9BF03
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 (show sfm)

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

```
Switch Fabric State: up
Switch Mode: SFM3

-- SFM card 0 --
Status          : active (Older version of SFM for Exascale)
Card Type       : SFM3 - Switch Fabric Module
Up Time        : 18 hr, 40 min
Last Restart   : remote-off
Temperature     : 42C
Power Status    : AC
Serial Number   : VC074300030
Part Number    : 7520020001 Rev 03
Vendor Id      : 04
Date Code      : 01402006
Country Code   : 01
Piece Part ID  : CN-0RVY43-75412-123-0030
PPID Revision  : 003
Service Tag    : SVCTG00
Expr Svc Code  : 628 458 860 16
FPGA          : 0x0.0.3
Booting from   : EEPROM0
```

Table 5-5. show sfm Command Output Fields

Field	Description
Switch Fabric State:	States that the Switch Fabric is up (8 SFMs are online and operating).
Status	Displays the SFM's active status.
Card Type	States the type of SFM.
Up Time	Displays the number of hours and minutes since the RPM's last reboot.
Temperature	Displays the temperature of the RPM. Minor alarm status if temperature is over 65° C.

Table 5-5. show sfm Command Output Fields

Field	Description
Power Status	Displays power status: absent, down, or up
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

Command output example (show sfm all)

```
Switch Fabric State: up
Switch Mode: SFM3

-- Switch Fabric Modules --
Slot  Status
-----
  0   active          (Older version of SFM for Exascale)
  1   active          (Older version of SFM for Exascale)
  2   active          (Older version of SFM for Exascale)
  3   active          (Older version of SFM for Exascale)
  4   not present
```

show startup-config

CES Display the startup configuration.

Syntax **show startup-config**

Command Modes EXEC Privilege

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	Expanded to include last configuration change and start-up last updated (date and time) and who made the change.

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 FTOS version information on the system.

Syntax `show version`

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

E-Series Example Command output example on E-Series: `show version`

```
FTOS#show version
FTOS Networks Real Time Operating System Software
FTOS Operating System Version: 1.0
FTOS Application Software Version: 5.3.1.0
Copyright (c) 1999-2004 by Dell Force10 Networks, Inc.
Build Time: Sun May 9 00:57:03 PT 2004
Build Path: /local/local0/Release/5-4-1/SW/Bsp/Diag
FTOS 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 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

Lines beginning with	Description
FTOS Network...	Name of the operating system
FTOS Operating...	OS version number
FTOS Application...	Software version

show version Command Fields

Lines beginning with	Description
Copyright (c)...	Copyright information
Build Time...	Software build's date stamp
Build Path...	Location of the software build files loaded on the system
FTOS uptime is...	Amount of time the system has been up
System image...	Image file name
Chassis Type:	Chassis type (E1200, E600, E600i, E300, C300, C150)
Control Processor:...	Control processor information and amount of memory on processor.
Route Processor 1:...	E-Series route processor 1 information and the amount of memory on that processor.
Route Processor 2:...	E-Series route processor 2 information and the amount of memory on that processor.
128K bytes...	Amount and type of memory on system.
1 Route Processor...	Hardware configuration of the system, including the number and type of physical interfaces available.

S-Series ExampleCommand output example on an S50V: **show version**

```

FTOS#show version
FTOS Networks Real Time Operating System Software
FTOS Operating System Version: 1.0
FTOS Application Software Version: E7-8-1-13
Copyright (c) 1999-2008 by Dell 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
FTOS 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)

- E** 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 <i>linecard-slot</i>	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
rpm	Enter the keyword rpm to upgrade the bootflash/boot selector image on all processors on the RPM.
booted	Enter this keyword to upgrade using the image packed with the currently running FTOS image.
file-url	Enter the following location keywords and information to upgrade using an FTOS image other than the one currently running: Enter the transfer method and file location: flash://filename ftp://userid:password@hostip/filepath slot0://filename tftp://hostip/filepath

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 system](#) 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.
linecard number	Enter the keyword linecard followed by the line card slot number. Range: E1200, E1200i AC/DC: 0-12 E600, E600i: 0-6 E300: 0-5 C300: 0-7 C150: 0-3
rpm	Enter the keyword rpm to upgrade the system image of a selector image on all processors on the RPM.
repair	Enter this keyword to upgrade a line card newly inserted into an already upgraded chassis. This option is only available with the system-image keyword.
booted	Upgrade the bootflash or bootselector image using the currently running FTOS image.
file-url	Enter the following location keywords and information to upgrade using an FTOS image other than the one currently running: <ul style="list-style-type: none"> To specify an FTOS image on the internal flash, enter flash:// file-path/ filename. To specify an FTOS image on an FTP server, enter ftp:// user:password@ hostip/ filepath To specify an FTOS image on the external flash on the primary RPM, slot0:// file-path/ filename To copy a file on a TFTP server, enter tftp:// hostip/ filepath/ filename

Defaults FTOS 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 fpga-image

E 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]`

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

Version 8.3.1.0	Added rpm option
Version 7.5.1.0	Introduced on E-Series

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

show sfm	Display the SFM status.
upgrade (E-Series version)	Upgrade the E-Series.

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

rpm	Enter rpm to upgrade an RPM FPGA.
linecard	Enter linecard to upgrade a line card FPGA.
number	Enter the line card or RPM slot number. C-Series Line Card Range: 0-7, RPM Range: 0-1

Defaults None.

Command Mode EXEC Privilege

Command History

Version 7.7.1.0	Renamed keyword primary-fpga-flash to fpga-image .
Version 7.5.1.0	Introduced on C-Series

Example Command example: **restore fpga-image**

```
FTOS#restore fpga-image linecard 4

Current FPGA information in the system:
=====
Card                      FPGA Name                Current Version    New Version
-----
LC4                        48 Port 1G LCM FPGA      A: 3.6             restore


*****
* Warning - Upgrading FPGA is inherently risky and should          *
* only be attempted when necessary. A failure at this upgrade may  *
* cause a board RMA. Proceed with caution !                         *
*****

Restore fpga image for linecard 4 [yes/no]: yes
FPGA restore in progress. Please do NOT power off the card.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upgrade result :
=====
Linecard 4 FPGA restore successful.
```

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} [system-fpga | link-fpga] | 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 C300, 0-3 on the C150

all Enter the keyword **all** to upgrade all RPM and linecard FPGAs. Enter the keyword **all** after the keyword **rpm** to upgrade all FPGAs on all RPMs.
Enter the keyword **all** after the keyword **linecard** to upgrade all FPGAs on all linecards.

system-fpga (OPTIONAL) Enter **system-fpga** to upgrade only the system FPGA on a fiber linecard. Contact the Dell Force10 TAC before using this keyword.

link-fpga (OPTIONAL) Enter **link-fpga** to upgrade only the link FPGA on a fiber linecard. Contact the Dell Force10 TAC before using this keyword.

booted Upgrade the FPGA image using the currently running FTOS image.

file-url Enter the following location keywords and information to upgrade the FPGA using an FTOS image other than the one currently running:

- To specify an FTOS image on the internal flash, enter **flash:// file-path/filename**.
- To specify an FTOS image on an FTP server, enter **ftp://user:password@hostip/ filepath**
- To specify an FTOS image on the external flash on the primary RPM, **slot0://file-path/ filename**
- To copy a file on a TFTP server, enter **tftp://hostip/filepath/filename**

Defaults None.

Command Mode EXEC Privilege

Command History

Version 7.7.1.0 Renamed the **primary-fpga-flash** keyword to **fpga-image**. Added support for upgrading using a remote FTOS image.

Version 7.6.1.0 Added support for the **all** keyword

Version 7.5.1.0 Introduced on C-Series

Example Command example: **upgrade fpga-image**

```
FTOS#conf
FTOS(conf)# upgrade primary-fpga-flash rpm
Proceed to upgrade primary fpga flash for rpm 0 [confirm yes/no]: yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
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.

BOOT_USER Mode

Overview

All commands in this chapter are in the BOOT_USER mode except for **format**, which is in the BOOT_ADMIN mode. Command support on Dell Force10 platforms is indicated by the characters that appear below each command heading:

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

To access this mode in the C-Series and E-Series, enter a control break sequence (**Ctrl^**, which is **Ctrl Shift-6**) when the following line appears on the console during a system boot:

Send the Break Signal to stop Operating System auto-boot...

On the S-Series, the following is displayed twice. Press any key when the following line is displayed the second time:

Hit any key to break into BOOT_USER mode

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.
Note: Instead, enter **help**.

boot change



Change the primary, secondary, or default FTOS boot configuration.

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

Parameters

- primary** Enter the keyword **primary** to configure the boot parameters used in the first attempt to boot FTOS.
- 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 location should always be the internal flash device (flash:), and a verified image should be stored there.

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**, and 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. Refer to the command [interface management ethernet ip address](#).

The example below 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**.

Example 1
(1st field in boot change)

```
BOOT_USER # boot change primary

'.' = clear field; '-' = clear non-essential field

boot device                : ftp
```

Example 2
(Completed boot change)

The following example shows the completed command:

```
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.

Related Commands

- | | |
|-------------------------------------|---|
| boot system | Set the location of FTOS image files. |
| boot zero | Remove the primary, secondary, or default boot image configuration. |
| show boot selection | Display the current Boot Flash image selected. |
| show bootvar | Display boot configuration information. |

boot messages

C **E** 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

C **E** 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

C **E** **S** 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.

```
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 #

```

**Related
Commands**

[boot change](#) Change the primary, secondary or default boot image configuration
[show boot selection](#) Display the current Boot Flash image selected.

default-gateway

C **E** **S** 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

C **E** 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.

Defaults Not configured.

Command Modes BOOT_USER

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

```
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
  8807825       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
  7819238       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 #
```

enable



Change the privilege level of user access to FTOS commands.

Syntax `enable {user | admin}`

Parameters

admin

Used only by Dell Force10 TAC personnel.

user

Used only by Dell Force10 TAC personnel.

Defaults

Not configured.

Command Modes

BOOT_USER

Usage Information

Only Dell Force10 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 FTOS.

[show running-config](#)

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

ignore startup-config

S 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

C **E** **S** 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

S Assign a MAC address to the Management Ethernet interface.

Syntax `interface management ethernet mac-address mac-address`

Parameters `mac-address` Enter a MAC address in standard format (xx:xx:xx:xx:xx:xx).

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 FTOS 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

S Assign a port to be the Management Ethernet interface.

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

C **E** Configure speed, duplex, and negotiation settings for the management interface.

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

Parameters	half-duplex	Enter the keyword half-duplex to set the Management interface to half-duplex mode.
	full-duplex	Enter the keyword full-duplex to set the Management interface to full-duplex mode.
	10m	Enter the keyword 10m to set the speed on the Management interface to 10 Mb/s.
	100m	Enter the keyword 100m to set the speed of the Management interface to 100 Mb/s.
	auto-negotiation	Enter the keyword auto-negotiation to enable negotiation on the Management interface.
	no auto-negotiation	Enter the keyword no auto-negotiation to disable auto-negotiation on the Management interface.
	show	Enter the keyword show to display the settings on the Management interface.

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

C **E** **S** Exit from this mode and reload FTOS.

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



Rename a file.

Syntax `rename 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 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 Force10 platforms is that, on the S-Series, FTOS 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 FTOS.
- [write](#) Save the running configuration to the startup configuration file.

show boot selection

C **E** Display the current FTOS boot image.

Syntax **show boot selection**

Command Modes BOOT_USER

Example BOOT_USER # show boot selection

```
ROM BOOTSTRAP SELECTOR PARMETERS:
=====
Current ROM bootstrap selection set to Bootflash partition B.

Last ROM bootstrap occurred from Bootflash partition B.

BOOT_USER #
```

**Related
Commands**

[boot change](#)

Change the primary, secondary or default boot image configuration

[boot selection](#)

Change the boot flash image on the internal Flash.

show bootflash

C **E** Display information on the boot flash.

Syntax **show bootflash**

Command Modes BOOT_USER

Example BOOT_USER # show bootflash

```
GENERAL BOOTFLASH INFO
=====
Bootflash Partition A:
  Dell Force10 Networks System Boot
  Copyright 1999-2011 Dell 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:
  Dell Force10 Networks System Boot
  Copyright 1999-2011 Dell 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:
  Dell Force10 Networks System Boot
  Copyright 1999-2011 Dell 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

C **E** **S** Display boot configuration information.

Syntax **show bootvar**

Command Modes BOOT_USER

Command History Version 7.8.1.0 Introduced on S-Series

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
Server IP address    : 10.16.1.209
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

- [boot change](#) Change the primary, secondary or default boot image configuration.
- [boot zero](#) Erase the configured primary, secondary, or default boot image parameters.

show default-gateway

C **E** **S** Display the IP address configured for the default gateway.

Syntax **show default-gateway**

Command Mode BOOT_USER

Command History Version 7.8.1.0 Introduced on S-Series

Example BOOT_USER # show default-gateway

```
Gateway IP address: 10.1.1.1

BOOT_USER #
```

**Related
Commands**

[default-gateway](#)
[interface management ethernet ip address](#)

Configure the IP address for the default gateway.
 Assign an IP address to the Management Ethernet interface.

show interface management ethernet



Display 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

```
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
(S-Series)**

```
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](#)
[interface management port config](#)

Assign an IP address to the Management Ethernet interface.
 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

audible cut-off	show chassis
banner exec	show command-history
banner login	show command-tree
banner motd	show console lp
cam-audit linecard	show cpu-traffic-stats
clear alarms	show debugging
clear command history	show environment (C-Series and E-Series)
clear line	show environment (S-Series)
configure	show inventory (C-Series and E-Series)
debug cpu-traffic-stats	show inventory (S-Series)
debug ftpserver	show linecard
disable	show linecard boot-information
do	show memory (C-Series and E-Series)
enable	show memory (S-Series)
enable xfp-power-updates	show processes cpu (C-Series and E-Series)
end	show processes cpu (S-Series)
epoch	show processes ipc flow-control
exec-banner	show processes memory (C-Series and E-Series)
exec-timeout	show processes memory (S-Series)
exit	show rpm
ftp-server topdir	show software ifm
ftp-server username	show switch links
hostname	show system (S-Series)
ip ftp password	show tech-support (C-Series and E-Series)
ip ftp source-interface	show tech-support (S-Series)
ip ftp username	show util-threshold cpu
ip telnet server enable	show util-threshold mem
ip telnet source-interface	ssh-peer-rpm

ip tftp source-interface	telnet
line	telnet-peer-rpm
linecard	terminal length
module power-off	terminal xml
motd-banner	traceroute
ping	undebg all
power-off	util-threshold cpu (C- and E-Series)
power-on	util-threshold cpu (S-Series)
reload	util-threshold mem (C- and E-Series)
reset	util-threshold mem (S-Series)
rpm <slot> location-led	upload trace-log
send	virtual-ip
service timestamps	write
show alarms	

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

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

line Enter a text string for your banner message ending the message with your delineator. In the example below, the delineator is a percent character (%); the banner message is “testing, testing”.

Defaults No banner is displayed.

Command Modes CONFIGURATION

Command History

Version 8.1.1.0 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 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(conf)#banner exec ?
LINE c banner-text c, where 'c' is a delimiting character
FTOS(conf)#banner exec %
Enter TEXT message. End with the character '%'.
This is the banner%
FTOS(conf)#end
FTOS#exit
4d21h5m: %RPM0-P:CP %SEC-5-LOGOUT: Exec session is terminated for user on
line console

This is the banner

FTOS 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	banner login	Sets a banner for login connections to the system.
	banner motd	Sets a Message of the Day banner.
	exec-banner	Enable the display of a text string when the user enters the EXEC mode.
	line	Enable and configure console and virtual terminal lines to the system.

banner login

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

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

Parameters	keyboard-interactive	Enter this keyword to require a carriage return (CR) to get the message banner prompt.
	c	Enter a delineator character to specify the limits of the text banner. In the example below, the % character is the delineator character.
	line	Enter a text string for your text banner message ending the message with your delineator. In the example in the example below, the delineator is a percent character (%). Ranges: <ul style="list-style-type: none">• maximum of 50 lines• up to 255 characters per line

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

Command Modes CONFIGURATION**Command History**

Version 8.2.1.0 Introduced **keyboard-interactive** keyword
 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

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

```
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

FTOS 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

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

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



Enable audit of the IPv4 forwarding table on all line cards.

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** Enter the keyword **interval** followed by the frequency in minutes of the CAM audit.
- time-in-minutes** Range: 5 to 1440 minutes (24 hours)
Default: 60 minutes

Defaults Disabled

Command Modes CONFIGURATION

Command History

- Version 7.4.1.0 Introduced on E-Series

Usage Information

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

clear alarms

C **E** **S**

Clear alarms on the system.

Syntax **clear alarms**

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

Usage Information

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

clear command history

C **E** **S**

Clear the command history log.

Syntax **clear command history**

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

[show command-history](#) Display a buffered log of all commands entered by all users along with a time stamp.

clear line

C **E** **S**

Reset a terminal line.

Syntax **clear line** { *line-number* | **aux 0** | **console 0** | *vtty 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.

vtty number Enter the keyword vty followed by a number to clear a Terminal line.
Range: 0 to 9

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	

configure

C **E** **S**

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	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	

Example
 FTOS#configure
 FTOS (conf) #

debug cpu-traffic-stats

C **E** **S**

Enable the collection of CPU traffic statistics.

Syntax **debug cpu-traffic-stats**


Defaults Disabled

Command Modes EXEC Privilege

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 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 trigger (turn on) the collection of CPU traffic statics. The following message is an indication that collection of CPU traffic is automatically turned on. Use the [show cpu-traffic-stats](#) to view the traffic statistics.

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 Force10 recommends that you disable debugging (**no debug cpu-traffic-stats**) once troubleshooting is complete.

Related Commands

[show cpu-traffic-stats](#)

Display cpu traffic statistics

debug ftpserver

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

Syntax `debug ftpserver`

Command Modes EXEC Privilege

Command History

Version 8.1.1.0	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	

disable

Return to the EXEC mode.

Syntax `disable [level]`

Parameters

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

Defaults 1

Command Modes EXEC Privilege

Command History

Version 8.1.1.0	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	

do

C **E** **S**

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

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 on E-Series

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

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

Example

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

enable

C **E** **S**

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

Syntax `enable [level]`

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

Defaults 15

Command Modes EXEC

Command History	Version 8.1.1.0	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	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

C **E** **S** 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

interval seconds Enter the keyword **interval** followed by the polling interval in seconds.
Range: 120 to 6000 seconds
Default: 300 seconds (5 minutes)

Defaults Disabled

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 and E-Series

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

C **E** **S** 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	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	exit	Return to the lower command mode.
-------------------------	----------------------	-----------------------------------

epoch

E Set the epoch scheduling time for the chassis.

Syntax `epoch {2.4 | 3.2 | 10.4}`

Parameters

- 2.4** Enter the keyword **2.4** 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.
- 3.2** Enter the keyword **3.2** 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 supports this setting with FTOS 8.3.1.0 and later.
- 10.4** Enter the keyword **10.4** to set the epoch to 10.4 micro-seconds. This is the default setting and is available on the E300, E600/E600i, and E1200.

Defaults 10.4

Command Modes CONFIGURATION

Command History

Version 8.3.1.0	Added 2.4 micro-seconds option. ExaScale supports only 10.4 microseconds and 2.4 microseconds with FTOS 8.3.1.0 and later.
Version 8.1.1.2	Introduced on E-Series ExaScale E600i
Version 8.1.1.0	Introduced on E-Series ExaScale E1200i
Version 6.2.1.1	Support for E300 introduced (10.4 only)
Version 6.1.1.0	Values changed as described above

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 Force10 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 FTOS version 8.3.1.0 and later. The 10.4 setting is supported on all ExaScale FTOS versions. The 3.2 setting is only supported on FTOS versions 8.2.1.0 and earlier.

exec-banner

C **E** **S**

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

C **E** **S**

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.
seconds (OPTIONAL) Enter the number of seconds
Range: 0 to 2147483
Default: 0 seconds

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

Command Modes LINE

Command History

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

Usage Information

To remove the time interval, enter **exec-timeout 0 0**.

Example

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

exit

C **E** **S**

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

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

end Return to the EXEC Privilege command mode.

ftp-server enable

C **E** **S**

Enable FTP server functions on the system.

Syntax **ftp-server enable**

Defaults Disabled.

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

Example

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

```
226 Transfer complete
329 bytes received in 0.018 seconds (17.95 Kbytes/s)
ftp>
```

Related Commands

[ftp-server topdir](#) Set the directory to be used for incoming FTP connections to the E-Series.

[ftp-server username](#) Set a username and password for incoming FTP connections to the E-Series.

ftp-server topdir

C **E** **S** 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

E-Series original Command

Usage Information

After you enable FTP server functions with the [ftp-server enable](#) command, Dell Force10 recommends that you specify a top-level directory path. Without a top-level directory path specified, the FTOS directs users to the flash directory when they log in to the FTP server.

Related Commands

[ftp-server enable](#) Enables FTP server functions on the E-Series.

[ftp-server username](#) Set a username and password for incoming FTP connections to the E-Series.

ftp-server username

C **E** **S** 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 *password* Enter the keyword **password** followed by a string up to 40 characters long as the password.

Without specifying an encryption type, the password is unencrypted.

encryption-type (OPTIONAL) After the keyword **password** enter one of the following numbers:

- 0 (zero) for an unencrypted (clear text) password
- 7 (seven) for hidden text password.

Defaults Not enabled.

Command Modes CONFIGURATION

Command History

Version 8.1.1.0	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

hostname

C **E** **S** 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

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 The hostname is used in the prompt.

ip ftp password

C **E** **S** Specify a password for outgoing FTP connections.

Syntax **ip ftp password** [*encryption-type*] *password*

Parameters *encryption-type* (OPTIONAL) Enter one of the following numbers:

- 0 (zero) for an unencrypted (clear text) password
- 7 (seven) for hidden text password

password Enter a string up to 40 characters as the password.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 8.1.1.0	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

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 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 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 8.2.1.0 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
 E-Series original Command

Related Commands

copy Copy files from and to the switch.

ip ftp username

C **E** **S** Assign a user name for outgoing FTP connection requests.

Syntax **ip ftp username** *username*

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

Defaults No user name is configured.

Command Modes CONFIGURATION

Command History

Version 8.1.1.0	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 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

C **E** **S** 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

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
Version 6.1.1.0	Introduced on E-Series

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

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 the SONET interfaces, enter the keyword **sonet** followed by 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 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 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 8.2.1.0	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
E-Series original Command	

Related Commands

[telnet](#) Telnet to another device.

ip tftp source-interface

C **E** **S** 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 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 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 8.2.1.0	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
E-Series original Command	

lag-audit enable

E Enable audit functions for the LAG (port channel) egress port table.

Syntax `lag-audit enable {interval 1-100}`

Parameters *interval* Enter the amount of time, in seconds, indicating how often the egress port table will be audited.

Note: The amount of time selected will be in multiples of 5 seconds, i.e., 1 = 5 seconds; 10 = 50 seconds.
Range: 1 to 100
Default: 1 (audit will occur every 5 seconds)

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 8.3.1.0	Introduced on E-Series ExaScale
-----------------	---------------------------------

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>.
- vtty number** Enter the keyword **vtty** followed by a number from 0 to 9 to configure a virtual terminal line for Telnet sessions.
 The system supports 10 Telnet sessions.
- end-number** (OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure.
 You can configure multiple lines at one time.

Defaults Not configured

Command Modes CONFIGURATION

Command History

- Version 8.1.1.0 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

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

<i>number</i>	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.
<i>card-type</i>	Enter the line card ID (refer to the Supported Hardware section in the Release Notes).

Defaults Not configured

Command Modes CONFIGURATION

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

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).

Example

```
FTOS#show linecard 3

-- Line card 11 --
Status           : not present

FTOS#linecard 3 ?
E46TB           36-port GE 10/100/1000Base-T with RJ45 - 8-port FE/GE with SFP -
2-port 10GE with SFP+
E46VB           36-port GE 10/100/1000Base-T with RJ45 and PoE - 8-port FE/GE with
SFP - 2-port 10GE with SFP+
E48PB           48-port FE/GE line card with SFP optics (CB)
E48TB           48-port GE 10/100/1000Base-T line card with RJ45 interfaces (CB)
E48VB           48-port GE 10/100/1000Base-T line card with RJ45 interfaces and PoE
(CB)
EX4PB           4-port 10GE LAN PHY line card with XFP optics (CB)
EX8PB           8-port 10GE LAN PHY line card with XFP optics (CB)
FTOS#linecard 3 EX4PB
FTOS#show linecard 3

-- Line card 11 --
Status           : not present
Required Type   : EX4PB - 4-port 10GE LAN PHY line card with XFP optics (CB)
FTOS#
```



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

Related Commands [show linecard](#) Display the line card(s) status.

module power-off

C **E** Turn off power to a line card at next reboot.

Syntax **module power-off linecard** *number*

Parameters **linecard** *number* Enter the keyword **line card followed** by the line card slot number
C-Series Range: 0-7
E-Series Range: 0 to 13 on a E1200/1200i, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

Defaults Not configured.

Command Modes CONFIGURATION

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	

motd-banner

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

Syntax **motd-banner**

Defaults Enabled on all lines.

Command Modes LINE

Command History

Version 8.1.1.0	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	

ping

C **E** **S** 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*] [*ointerface (ip src-ipv4-address) | interface*]

Parameter

<i>vrf</i>	(OPTIONAL) E-Series Only: Enter the VRF Instance name of the device to which you are testing connectivity.
<i>host</i>	(OPTIONAL) Enter the host name of the devices to which you are testing connectivity.

<i>ip-address</i>	(OPTIONAL) Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format.
<i>ipv6-address</i>	(OPTIONAL) E-Series only 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
<i>count</i>	Enter the number of echo packets to be sent. <i>number:</i> 1- 2147483647 <i>Continuous:</i> transmit echo request continuously Default: 5
<i>datagram size</i>	Enter the ICMP datagram size. Range: 36 - 15360 bytes Default: 100
<i>timeout</i>	Enter the interval to wait for an echo reply before timing out. Range: 0 -3600 seconds Default: 2 seconds
<i>source</i>	Enter the IPv4 or IPv6 source ip address or the source interface. For IPv6 addresses, you may enter global addresses only. <ul style="list-style-type: none"> • 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 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 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.
<i>tos</i>	(IPv4 only) Enter the type of service required. Range: 0-255 Default: 0
<i>df-bit</i>	(IPv4 only) Enter Y or N for the “don't fragment” bit in IPv4 header N: Do not set the “don't fragment” bit Y: Do set “don't fragment” bit Default is No.
<i>validate-reply</i>	(IPv4 only) Enter Y or N for reply validation. N: Do not validate reply data Y: Do validate reply data Default is No.
<i>pattern pattern</i>	(IPv4 only) Enter the IPv4 data pattern. Range: 0-FFFF Default: 0xABCD
<i>sweep-min-size</i>	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 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 Refer to parameters above.

Command Modes EXEC
EXEC Privilege

Command History

Version 8.4.1.0	IPv6 ping 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. Refer to [Appendix](#) , for information on the ICMP message codes that return from a ping command.

Example 1 (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#

```

Example 2 (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: 0-7
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

Related Commands

[power-on](#) Power on a line card or standby SFM.

power-on



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

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 E1200/E1200i, 0 to 6 on a E600/E600i, and 0 to 5 on a 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	
Related Commands	power-off	Power off a line card or standby SFM.

reload

C **E** **S** Reboot FTOS.

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, FTOS 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 or a failed SFM (TeraScale and ExaScale).
reset stack-unit	Reset any designated stack member except the management unit

reset

C **E** Reset a line card, RPM, or a failed SFM (TeraScale only).

Syntax **reset** {**linecard** *number* [**hard** | **power-cycle**] | **rpm** *number* [**hard** | **power-cycle**] | **sfm** *slot number*}

Parameters

linecard <i>number</i>	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 <i>number</i>	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 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	<p>The command reset without any options is a soft reset, which means FTOS boots the line card from its runtime image. The hard option reloads the FTOS image on the line card. Use the power-cycle after upgrading an FPGA.</p> <p>When a soft reset is issued on a line card (reset linecard number), FTOS 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.</p>	
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]	
Parameters	rpm slot number	Enter the slot number E1200i: 0-13 E600i: 0-6
	on off	Toggles the LED on the RPM on or off.
Defaults	OFF	
Command Modes	EXEC	
Command History	Version 8.2.1.0	Introduced on the E-Series ExaScale
Usage Information	The LED setting is not saved through power cycles.	

send

C **E** **S**

Send messages to one or all terminal line users.

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

Parameters

***** Enter the asterisk character ***** to send a message to all tty lines.

line Send a message to a specific line.
Range: 0 to 11

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

Command Modes EXEC

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	Introduced on E-Series

Usage Information

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

service timestamps

C **E** **S**

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

C **E** **S** 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

E-Series Example

```
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 --
Alarm Type                               Duration
-----
No major alarms
FTOS#
```

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

Example
FTOS#show chassis brief
Chassis Type : E1200
Chassis Mode : TeraScale
Chassis Epoch : 3.2 micro-seconds

```
-- Line cards --
Slot  Status          NxtBoot   ReqTyp   CurTyp   Version   Ports
-----
  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  online             online    E48PF   E48PF   6.1.1.0   48
 12  not present
 13  not present
      E48PF
```

```
-- Route Processor Modules --
Slot  Status          NxtBoot   Version
-----
  0   active          online    6.1.1.0
  1   not present
```

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

-- Power Entry Modules --
Bay Status
-----
0 up
1 up

-- 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

```

Related Commands

- [show linecard](#) View line card status
- [show rpm](#) View Route Processor Module status.
- [show sfm](#) View Switch Fabric Module status.

show command-history

C **E** **S** 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 Force10 TAC to help identify the root cause of an RPM failover.

Example

```

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 hostname FTOS]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):[enable restricted 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):[protocol spanning-tree pvst]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):[shutdown]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 0/4]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):[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 15:47:23]: CMD-(CLI):[shutdown]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
[11/20 21:17:36]: CMD-(CLI):[exit]by default from console
[11/20 21:19:25]: CMD-(CLI):[show command-history]by default from console
F'TOS#

```

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

count Display the command tree with a usage counter for each command.

no Display all of the commands that may be preceded by the keyword **no**, which is the keyword used to remove a command from the running-configuration.

Defaults None

Command Mode	EXEC EXEC Privilege
Command History	" Version 8.2.1.0 Introduced
Usage Information	Reload the system to reset the command-tree counters.
Example	<pre> FTOS#show command-tree count ! Enable privilege mode: enable command usage:3 <0-15> option usage: 0 exit command usage:1 show command-tree count command usage:9 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 </pre>

show console lp

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

Syntax show console lp *number*

Parameters

<i>number</i>	Enter the line card slot number. Range: 0–7 for the C300 Range: 0–13 for the E1200 Range: 0–6 for the E600 Range: 0–5 for the E300
---------------	--

Defaults None

Command Mode EXEC
EXEC Privilege

Command History

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

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.

show cpu-traffic-stats



View the CPU traffic statistics.

Syntax

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

Parameters

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

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

cp (OPTIONAL) Enter the keyword **cp** to display traffic statistics on the specified CPU.
Note: This option is supported on E-Series only.

linecard (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.

rp1 (OPTIONAL) Enter the keyword **rp1** to display traffic statistics on the RP1.
Note: This option is supported on E-Series only.

rp2 (OPTIONAL) Enter the keyword **rp2** to display traffic statistics on the RP2.
Note: This option is supported on E-Series only.

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

E-Series Example

```
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.
```

```
FTOS#
```

Usage Information

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



Note: After debugging is complete, use the [no debug cpu-traffic-stats](#) command to shut off traffic statistics collection.

Related Commands

[debug cpu-traffic-stats](#)

Enable CPU traffic statistics for debugging

show debugging



View a list of all enabled debugging processes.

Syntax

show debugging

Command Mode

EXEC Privilege

Command History

Version 8.1.1.0 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

Example

```
FTOS#show debug
Generic IP:
  IP packet debugging is on for
  ManagementEthernet 0/0
  Port-channel 1-2
  Port-channel 5
  GigabitEthernet 4/0-3,5-6,10-11,20
  GigabitEthernet 5/0-1,5-6,10-11,15,17,19,21
ICMP packet debugging is on for
  GigabitEthernet 5/0,2,4,6,8,10,12,14,16
FTOS#
```

show environment (C-Series and E-Series)

C **E** 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. Refer to the examples below 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
Version 7.5.1.0 Introduced on C-Series
E-Series original Command

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.

E-Series Example (show environment)

```
-- Fan Status --
Status Temp Fan1 Fan2 Fan3 Serial Num Version
-----
up 32C 6000 RPM 6000 RPM 7500 RPM FX000040889 3.2

-- Power Supplies --
Bay Status
-----
0 absent
1 up
2 up
3 up

-- Line Card Environment Status --
Slot Status Temp Voltage
-----
0 not present
1 online 66C ok
2 not present
3 online 59C ok
4 online 64C ok
5 not present
6 online 59C ok
```

```

-- RPM Environment Status --
Slot  Status      Temp  Voltage
-----
0    active      36C   ok
1    not present

```

```

-- SFM Environment Status --

```

**E-Series Example
(show environment fan)**

```

-- Fan Status --
Status Temp  Fan1      Fan2      Fan3      Serial Num  Version
-----
up    32C   6000 RPM  6000 RPM  6000 RPM  FX000040889  3.2

```

**C-Series
Example (show environment fan)**

```

FTOS#show env fan

```

```

-- Fan Status --

```

```

Tray  0

```

```

-----
FanNumber  Speed  Status
0          4170  up
1          4140  up
2          3870  up
3          4140  up
4          3870  up
5          3810  up

```

```

FTOS#

```

show environment (S-Series)

S 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

The following example shows the output of the **show environment fan** command as it appears prior to FTOS 7.8.1.0.

Example 1 (show environment all)

```
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    up    1234        1
```

Example 2 (show environment fan)

```
FTOS#show environment fan

-- Fan Status --
-----
Unit   TrayStatus  Fan0   Fan1   Fan2   Fan3   Fan4   Fan5
-----
0      up           up     up     up     up     up     up
```

Example 3 (show environment pem)

```
FTOS#show environment pem

-- Power Supplies --
-----
Unit   Bay   Status   Type
-----
0      0     up       AC
0      1     absent
```

Example 4 (show environment stack-unit)

```
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)

C **E** Display the chassis type, components (including media), FTOS version including hardware identification numbers and configured protocols.

Syntax `show inventory [media slot]`

Parameters **media slot** (OPTIONAL) Enter the keyword **media** followed by the 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 [Example \(show inventory media slot \[partial\]\)](#). 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".

C300 Example

```
FTOS# show inventory
Chassis Type      : C300
Chassis Mode      : 1.0
Software Version  : FTOS-EF-7.6.1.0
```

Slot	Item	Serial Number	Part Number	Revision
	C300	TY000001400	7520029999	04
3	LC-CB-GE-48T	FX000020075	7520036700	01
0	LC-CB-RPM	0060361	7520029300	02
0	CC-C-1200W-AC	N/A	N/A	N/A
1	CC-C-1200W-AC	N/A	N/A	N/A
0	CC-C300-FAN			

* - standby

Software Protocol Configured

 OSPF

FTOS#

E-Series Example

Chassis Type : E600i
 Chassis Mode : ExaScale
 Software Version : E8-4-1-317

Slot	Item	Serial Number	Part Number	Rev	Piece	Part ID
Rev	Svc Tag	Exprs	Svc Code			

 --

	E600i	TY000002693	7520023900	03		
	US-0RVY43-76991-82B-0456	1B2 SVCTGCH	628 458 864	65		
1	LC-EH-10GE-10S	FX000049121	7520042807	03	N/A	
	N/A N/A	N/A				
1	LC-PIC0	FX000049647	7490105800	01	N/A	
	N/A N/A	N/A				
1	LC-PIC1	FX000049650	7490105800	01	N/A	
	N/A N/A	N/A				
3	LC-EJ-10GE-10S	FX000097669	7520047602	A	N/A	
	N/A N/A	N/A				
3	LC-PIC0	FX000047055	7490105800	01	N/A	
	N/A N/A	N/A				
3	LC-PIC1	FX000048680	7490105800	02	N/A	
	N/A N/A	N/A				
4	LC-EH-GE-90M	FX000046835	7520041702	01	N/A	
	N/A N/A	N/A				
4	LC-PIC0	FX000046905	7490102401	02	N/A	
	N/A N/A	N/A				
6	LC-EH-GE-90M	FX000044725	7520041702	01	N/A	
	N/A N/A	N/A				
6	LC-PIC0	FX000044256	7490102401	02	N/A	
	N/A N/A	N/A				
0	LC-EH-RPM	FX000056234	7520043401	05	N/A	
	N/A N/A	N/A				
0	CC-E-SFM3	VC074300030	7520020001	03		

```

CN-ORVY43-75412-123-0030 003 SVCTG00 628 458 860 16
 1 CC-E-SFM3          VC074300032 7520020001 03

CN-ORVY43-75412-82B-0456 1B2 SVCTG01 628 458 860 17
 2 CC-E-SFM3          VC074300032 7520020001 03

CN-ORVY43-75412-82B-0456 1B2 SVCTG02 628 458 860 18
 3 CC-E-SFM3          0068166      7520020001 03 N/A

      N/A N/A      N/A
 1 CC-E600-2500W-AC  VC074300032 7520026400 02 N/A

      N/A N/A      N/A
 2 CC-E600-2500W-AC  VC074300087 7520026400 02 N/A

      N/A N/A      N/A
 3 CC-E600-2500W-AC  VC073700046 7520026400 02 N/A

      N/A N/A      N/A
 0 CC-E600-FAN       FX000040889 N/A          N/A N/A

      N/A N/A      N/A
 0 slot0:            110613B1304M2737 - HDX 2.15 N/A

      N/A N/A      N/A

```

* - standby

Software Protocol Configured

```

-----
BGP
MCAST
OSPF
PIM
SNMP

```

Example (show inventory media slot [partial])

```

FTOS#show inventory media 3
Slot Port Type Media          Serial Number    F10Qualified
-----
...
 3    11 SFP  1000BASE-SX      U9600L0         Yes
...

```

Example (show inventory media)

```

Slot Port Type Media          Serial Number    F10Qualified
-----
1     0           Media not present or accessible
1     1           Media not present or accessible
1     2           Media not present or accessible
1     3           Media not present or accessible
1     4           Media not present or accessible
1     5 SFP+  10GBASE-SR      AM70PXW         Yes
1     6           Media not present or accessible
1     7           Media not present or accessible
1     8 SFP+  10GBASE-SR      AM70W84         Yes
1     9           Media not present or accessible

```

3	0	Media not present or accessible
3	1	Media not present or accessible
3	2	Media not present or accessible
3	3	Media not present or accessible
3	4	Media not present or accessible
3	5	Media not present or accessible
3	6	Media not present or accessible
3	7	Media not present or accessible
3	8	Media not present or accessible

Related Commands

[show interfaces](#)

Display a specific interface configuration.

[show interfaces transceiver](#)

Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show inventory (S-Series)

S Display the S-Series switch type, components (including media), FTOS version including hardware identification numbers and configured protocols.

Syntax `show inventory [media slot]`

Parameters

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

Defaults 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 1 (show inventory)

```
FTOS>show inventory
System Type           : S4810
System Mode           : 1.0
Software Version      : 8.3.12.0
```

```
Unit Type           Serial Number      Part Number  Rev  Piece Part ID  Rev  Svc Tag  Exprs Svc Code
-----
* 0 S4810-01-64F    HADL111220134  7590009601  A   N/A             N/A  N/A      N/A
  0 S4810-PWR-AC   H6DL111220150  7590008501  C   N/A             N/A  N/A      N/A
  0 S4810-FAN      N/A             N/A         N/A  N/A N/A             N/A  N/A      N/A
  0 S4810-FAN      N/A             N/A         N/A  N/A N/A             N/A  N/A      N/A
```

* - Management Unit

```
Software Protocol Configured
-----
iSCSI
```

LLDP
MCAST
OSPF
PIM
SNMP

Example 2
(show inventory media)

```

FTOS>show inventory media
Slot   Port   Type   Media   Serial Number
F10Qualified
-----
--
0      0      SFP    1000BASE-SX    P681WK0    Yes
0      1      SFP    1000BASE-SX    PGF3T36    Yes
0      2      SFP    1000BASE-SX    PGF420E    Yes
0      3      SFP    1000BASE-SX    P118HQ2    Yes
0      4      SFP    1000BASE-SX    PGF4244    Yes
0      5      SFP    1000BASE-SX    P5N1BN6    Yes
0      6      SFP    1000BASE-SX    P7529KV    Yes
0      7      SFP    1000BASE-SX    PGC514G    Yes
0      8      SFP    1000BASE-SX    PLE71GD    Yes
0      9      SFP    1000BASE-SX    PLE71N0    Yes
0      10     SFP    1000BASE-SX    PLE71M7    Yes
0      11     SFP    1000BASE-SX    PLE71LL    Yes
0      12     SFP    1000BASE-SX    B320210110  Yes
0      13     SFP    1000BASE-SX    B322237357  Yes
0      14     SFP    1000BASE-SX    P118PGB    Yes
0      15     SFP    1000BASE-SX    PGF425R    Yes
0      16     SFP    1000BASE-SX    PLE71MF    Yes
0      17     SFP    1000BASE-SX    AMEH367    Yes
0      18     SFP    1000BASE-SX    PLE71LZ    Yes
0      19     SFP    1000BASE-SX    PGA531L    Yes
0      20     SFP    1000BASE-SX    PLE71M8    Yes
0      21     SFP    1000BASE-SX    PGC51EM    Yes
0      22     SFP    1000BASE-SX    PLP32BP    Yes
0      23     SFP    1000BASE-SX    AJHG367    Yes
0      24     SFP    1000BASE-SX    P11BWUJ    Yes
0      25     SFP    1000BASE-SX    P741RVM    Yes
0      26     SFP    1000BASE-SX    PGF3T9H    Yes
0      27     SFP    1000BASE-SX    PGC51ZE    Yes
0      28     SFP    1000BASE-SX    PGC525W    Yes
0      29     SFP    1000BASE-SX    B342232045  Yes
0      30     SFP    1000BASE-SX    PGC50YB    Yes
0      31     SFP    1000BASE-SX    U960Y9X    Yes
0      32     SFP    1000BASE-SX    PGF420U    Yes
0      33     SFP    1000BASE-SX    PG35GSR    Yes
0      34     SFP    1000BASE-SX    PGC50M2    Yes
0      35     SFP    1000BASE-SX    PGF3T7X    Yes
0      36     SFP    1000BASE-SX    F54155490074  Yes
0      37     SFP    1000BASE-SX    PGF42MX    Yes
0      38     SFP    1000BASE-SX    PGC51WC    Yes
0      39     SFP    1000BASE-SX    PGC51ES    Yes
0      40     SFP    1000BASE-SX    PGA5341    Yes
0      41     SFP    1000BASE-SX    PLE71MC    Yes
0      42     SFP    1000BASE-SX    PGC50SN    Yes
0      43     SFP    1000BASE-SX    U8E0015    Yes
0      44     SFP    1000BASE-SX    PGA535F    Yes
0      45     SFP    1000BASE-SX    PGA533W    Yes
0      46     SFP    1000BASE-SX    P118WQC    Yes
0      47     SFP    1000BASE-SX    PGF42NZ    Yes
0      48     QSFP   40GBASE-SR4    QB030055    Yes
0      52     QSFP   40GBASE-SR4    QB382222    Yes
0      56     Media not present or accessible
0      60     Media not present or accessible

```

Related Commands

[show interfaces](#)
[show interfaces transceiver](#)

interface configuration.

Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show linecard

C **E** Display the line card(s) status.

Syntax **show linecard** [*number* [**brief**] | **all**]

Parameters

number (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.

all (OPTIONAL) Enter the keyword **all** to view a table with information on all present line cards.

brief (OPTIONAL) Enter the keyword **brief** to view an abbreviated list of line card 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

E-Series Example (show linecard)

```
-- Line card 1 --
Status      : online
Next Boot   : online
Required Type : EXW10SH - 10-port 10GE LAN/WAN PHY line card with

SFP+ options 10M CAM (EH)
Current Type  : EXW10SH - 10-port 10GE LAN/WAN PHY line card with

SFP+ options 10M CAM (EH)
Hardware Rev  : Base - 1.4  PP0 - 02  PP1 - 02
Num Ports    : 10
Up Time      : 18 hr, 42 min
FTOS Version : 8-4-1-317
Jumbo Capable : yes
Boot Flash   : A: 2.9.1.1c      B: 2.9.2.0E0 [booted]
Memory Size  : 1073741824 bytes
Temperature  : 65C
Power Status  : AC
Voltage      : ok
Serial Number : FX000049121
Part Number   : 7520042807 Rev 03
Vendor Id     : 04
Date Code    : 01212010
Country Code  : 01
Piece Part ID : N/A
PPID Revision : N/A
Service Tag   : N/A
Expr Svc Code : N/A
Last Restart  : soft reset
Auto Reboot   : enabled
```

C-Series Example

```
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
FTOS 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  :                Rev
Vendor Id    :
Date Code    :
Country Code :
FTOS#
```

Table 7-6, "Descriptions for show linecard output," in [Control and Monitoring](#) list the definitions of the fields shown in [E-Series Example \(show linecard\)](#).

Table 7-6. Descriptions for show linecard output

Field	Description
Line card	Displays the line card slot number (only listed in show linecard all command output).
Status	Displays the line card's status.
Next Boot	Displays whether the line card is to be brought online at the next system reload.
Required Type	Displays the line card type configured for the slot. The Required Type and Current Type must match. Use the linecard command to reconfigure the line card type if they do not match.
Current Type	Displays the line card type installed in the slot. The Required Type and Current Type must match. Use the linecard command to reconfigure the line card type if they do not match.
Hardware Rev	Displays the chip set revision.
Num Ports	Displays the number of ports in the line card.
Up Time	Displays the number of hours and minutes the card is online.
FTOS Version	Displays the operating software version.
Jumbo Capable	Displays Yes or No indicating if the line card can support Jumbo frames.
Boot Flash Ver	Displays the two possible Bootflash versions. The [Booted] keyword next to the version states which version was used at system boot.
Memory Size	List the memory of the line card processor.
Temperature	Displays the temperature of the line card. Minor alarm status if temperature is over 65° C.

Table 7-6. Descriptions for show linecard output

Field	Description
Power Status	Lists the type of power modules used in the chassis: <ul style="list-style-type: none"> AC = AC power supply DC = DC Power Entry Module (PEM)
Voltage	Displays OK if the line voltage is within range.
Serial Number	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.

**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
FTOS Version    : 6.1.1.0
Jumbo Capable  : yes
FTOS#

```

**Related
Commands**

linecard	Pre-configure a line card in a currently empty slot of the system or a different line card type for the slot.
show interfaces linecard	Display information on all interfaces on a specific line card.
show chassis	View information on all elements of the system.
show rpm	View information on the RPM.
show sfm	View information on the SFM.

show linecard boot-information

E View the line card status and boot information.

Syntax **show linecard boot-information**

Command Modes EXEC
EXEC Privilege

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 6.5.1.4	Introduced on E-Series

Example (show linecard boot-information)

Command Example: show linecard boot-information

```

-- Line cards --
# Status CurType Serial      Booted      Next      Cache      Boot
# Status CurType number      from        boot        boot        flash
-----
0 -
1 online EXW10SH FX000049121 8-4-1-317 8-4-1-317 A: 8-4-1-213 B: A: 2.9.1.1c B:
2.9.2.0E0 [b]
2 -
3 online EXW10SJ FX000097669 8-4-1-317 8-4-1-317 A: 8-4-1-305 B: invalid A: 2.9.1.1 [b] B:
2.9.1.1
4 online E90MH FX000046835 8-4-1-317 8-4-1-317 A: 8-4-1-213 B: invalid A: 2.9.1.1 B:
2.9.1.1 [b]
5 -
6 online E90MH FX000044725 8-4-1-317 8-4-1-317 A: 8-4-1-213 B: invalid A: 2.9.1.1 [b] B:
2.9.1.1

```

Table 7-7, "Descriptions for show linecard boot-information output," in Control and Monitoring defines the fields in Example (show linecard boot-information)

Table 7-7. Descriptions for show linecard boot-information output

Field	Description
#	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.
Status	Indicates if a line card is online, offline, or booting. If a line card is not detected in the slot, a hyphen (-) is displayed.
CurType	Displays the line card identification number, for example EXW4PF.
Serial number	Displays the line card serial number.
Booted from	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 FTOS version number (6.5.1.4).
Next boot	Indicates if the next line card boot is a cache boot or system boot and which image will be used in the boot.
Cache boot	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.
Boot flash	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.

Usage Information

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.

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 FTOS image to the chassis
	download alt-system-image	Download an alternate system image to the chassis

show memory (C-Series and E-Series)

C **E** View current memory usage on the system.

Syntax `show memory [cp | lp slot-number | rp1 | rp2]`

Parameters

cp	(OPTIONAL) Enter the keyword cp to view information on the Control Processor on the RPM.
lp <i>slot-number</i>	(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 E600/E600i, and 0 to 5 on a E300.
rp1	(OPTIONAL) Enter the keyword rp1 to view information on Route Processor 1 on the RPM. Note: This option is supported on the E-Series only.
rp2	(OPTIONAL) Enter the keyword rp2 to view information on Route Processor 2 on the RPM. Note: This option is supported on the E-Series only.

Command Modes

EXEC
EXEC Privilege

Command History

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

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 C-Series' and E-Series' LP.

In FTOS 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 FTOS 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

```
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 7-8, "Descriptions for show memory output," in *Control and Monitoring* defines the fields displayed in the example above..

Table 7-8. Descriptions for show memory output

Field	Description
Lowest	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.
Largest	The current largest available. This relates to block size and is not related to the amount of memory on the system.

show memory (S-Series)

S 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 (sysd1p) of the system. The Sysd1p is an aggregate task that handles all the tasks running on the S-Series' CPU.

Example

```

FTOS#show memory stack-unit 0
Statistics On Unit 0 Processor
=====
Total(b)      Used(b)      Free(b)      Lowest(b)    Largest(b)
268435456    4010354     264425102   264375410   264425102

```

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

C **E** 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.
rp2	(OPTIONAL) Enter the keyword rp2 to view CPU usage of the Route Processor 2. Note: This option is supported on the E-Series only.
lp linecard [1-99]	(OPTIONAL) Enter the keyword lp followed by the line card number to display the CPU usage of that line card. The optional 1-99 variable sets the number of tasks to display in order of the highest CPU usage in the past five (5) seconds.
lp all	(OPTIONAL) Enter the keyword lp all to view CPU utilization on all active line cards.
lp summary	(OPTIONAL) Enter the keyword lp summary to view a summary of the line card CPU utilization.

Command Modes

EXEC
EXEC Privilege

Command History

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

Example 1 (partial)

```

FTOS#show processes cpu
      CPU Statistics On  CP Processor
      =====

CPU utilization for five seconds: 4%/2%; one minute: 2%; five minutes: 2%
PID          Runtime(ms)   Invoked    uSecs    5Sec    1Min    5Min  TTY    Process
0xd02e4e8    1498633      89918     16666    3.00%   2.67%   2.67%  0      KP
0xd9d4c70         0           0          0     0.00%   0.00%   0.00%  0      tLogTask
0xd9cd200         0           0          0     0.00%   0.00%   0.00%  0      soc_dpc
0xd9bf588         0           0          0     0.00%   0.00%   0.00%  0      tARL
0xd9bd2f8         0           0          0     0.00%   0.00%   0.00%  0      tBCMLink
0xd9bb0e0         700         42     16666    0.00%   0.00%   0.00%  0      tBcmTask
0xd9798d0    106683      6401     16666    0.00%   0.00%   0.00%  0      tNetTask
0xd3368a0         0           0          0     0.00%   0.00%   0.00%  0      tWdbTask
0xd3329b0         166         10     16600    0.00%   0.00%   0.00%  0      tWdtTask
0xd32a8c8    102500      6150     16666    0.00%   0.00%   0.00%  0      tme
0xd16b1d8    12050       723     16666    0.00%   0.00%   0.00%  0      ipc
0xd1680c8         33          2     16500    0.00%   0.00%   0.00%  0      irc
0xd156008         116          7     16571    0.00%   0.00%   0.00%  0      RpmAvailMgr
0xd153ab0         216         13     16615    0.00%   0.00%   0.00%  0      ev
-more-

```

Example 2
(cpu rp1)

```

FTOS#show processes cpu rp1
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID      Runtime(ms)   Invoked    uSecs    5Sec    1Min    5Min  TTY    Process
0x0000007c    60           6         10000    0.00%   0.00%   0.00%  0      ospf
0x00000077   460          46        10000    0.00%   0.00%   0.00%  0      dsm
0x00000074   100          10        10000    0.00%   0.00%   0.00%  0      ipml
0x0000006e   180          18        10000    0.00%   0.00%   0.00%  0      rtm
0x0000006b   100          10        10000    0.00%   0.00%   0.00%  0      rip
0x00000068   120          12        10000    0.00%   0.00%   0.00%  0      acl
0x00000064   690          69        10000    0.00%   0.00%   0.00%  0      sysdl
0x00000062    20           2         10000    0.00%   0.00%   0.00%  0      sysmon
0x00000024   880          88        10000    0.00%   0.00%   0.00%  0      sshd
0x00000022    0            0          0         0.00%   0.00%   0.00%  0      inetd
0x00000020  2580         258       10000    0.00%   0.00%   0.00%  0      mount_mfs
0x00000013    0            0          0         0.00%   0.00%   0.00%  0      mount_mfs
0x00000006    80           8         10000    0.00%   0.00%   0.00%  0      sh
0x00000005    30           3         10000    0.00%   0.00%   0.00%  0      aiodoned
0x00000004   840          84        10000    0.00%   0.00%   0.00%  0      ioflush
0x00000003   250          25        10000    0.00%   0.00%   0.00%  0      reaper
0x00000002    0            0          0         0.00%   0.00%   0.00%  0      pagedaemon
0x00000001   160          16        10000    0.00%   0.00%   0.00%  0      init
0x00000000   700          70        10000    0.00%   0.00%   0.00%  0      swapper
0x00000088   260          26        10000    0.00%   0.00%   0.00%  0      bgp

```

Example 3
(cpu rp2)

```

FTOS#show processes cpu rp2
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID      Runtime(ms)   Invoked    uSecs    5Sec    1Min    5Min  TTY    Process
0x00000090   140          14        10000    0.00%   0.00%   0.00%  0      vrrp
0x0000008d   120          12        10000    0.00%   0.00%   0.00%  0      fvrp
0x00000088   360          36        10000    0.00%   0.00%   0.00%  0      xstp
0x00000084    60           6         10000    0.00%   0.00%   0.00%  0      span
0x00000083   180          18        10000    0.00%   0.00%   0.00%  0      pim
0x00000080    80           8         10000    0.00%   0.00%   0.00%  0      igmp
0x0000007b   130          13        10000    0.00%   0.00%   0.00%  0      ipm2
0x00000078   700          70        10000    0.00%   0.00%   0.00%  0      mrtm
0x00000074   100          10        10000    0.00%   0.00%   0.00%  0      l2mgr
0x00000070    80           8         10000    0.00%   0.00%   0.00%  0      l2pm
0x0000006c    80           8         10000    0.00%   0.00%   0.00%  0      arpm
0x00000068    60           6         10000    0.00%   0.00%   0.00%  0      acl2
0x00000064   750          75        10000    0.00%   0.00%   0.00%  0      sysd2
0x00000062    0            0          0         0.00%   0.00%   0.00%  0      sysmon
0x00000024   880          88        10000    0.00%   0.00%   0.00%  0      sshd
0x00000022    0            0          0         0.00%   0.00%   0.00%  0      inetd
0x00000020  2250         225       10000    0.00%   0.00%   0.00%  0      mount_mfs
0x00000013    0            0          0         0.00%   0.00%   0.00%  0      mount_mfs
0x00000006   100          10        10000    0.00%   0.00%   0.00%  0      sh
0x00000005    0            0          0         0.00%   0.00%   0.00%  0      aiodoned
0x00000004   960          96        10000    0.00%   0.00%   0.00%  0      ioflush
0x00000003   140          14        10000    0.00%   0.00%   0.00%  0      reaper
0x00000002    0            0          0         0.00%   0.00%   0.00%  0      pagedaemon
0x00000001   160          16        10000    0.00%   0.00%   0.00%  0      init
0x00000000   700          70        10000    0.00%   0.00%   0.00%  0      swapper
0x00000098   140          14        10000    0.00%   0.00%   0.00%  0      msdp

```

Usage Information

The CPU utilization for the last five seconds as shown in [Example 1 \(partial\)](#) 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)

S 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 sysdtp). Refer to 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. Refer to Example 2.

Or, as an option of **memory**, this option limits the output of memory statistics to the designated stack member. Refer to Example 5.

summary (OPTIONAL) Enter the keyword **summary** to view a summary view of CPU usage for all members of the stack. Refer to Example 1.

ipc (OPTIONAL) Enter the keyword **ipc** to display inter-process communication statistics.

memory (OPTIONAL) Enter the keyword **memory** to display memory statistics. Refer to 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 (cpu summary, 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
(cpu
management-unit,
S-Series)

```

FTOS#show processes cpu management-unit 0

CPU utilization for five seconds: 1%/0%; one minute: 10%; five minutes: 2%
PID      Runtime(ms)   Invoked    uSecs    5Sec   1Min   5Min   TTY      Process
 272         20             2    10000   0.00%  0.00%  0.00%  0        topoDPC
 271          0             0         0   0.00%  0.00%  0.00%  0        bcmNHOP
 270          0             0         0   0.00%  0.00%  0.00%  0        bcmDISC
 269          0             0         0   0.00%  0.00%  0.00%  0        bcmATP-RX
 268          0             0         0   0.00%  0.00%  0.00%  0        bcmATP-TX
 267         30             3    10000   0.00%  0.00%  0.00%  0        bcmSTACK
 266        380            38    10000   0.00%  0.00%  0.08%  0        bcmRX
 265         30             3    10000   0.00%  0.00%  0.00%  0        bcmLINK.0
 264          0             0         0   0.00%  0.00%  0.00%  0        bcmXGS3AsyncTX
 263          0             0         0   0.00%  0.00%  0.00%  0        bcmTX
 262        160            16    10000   0.00%  0.00%  0.00%  0        bcmCNTR.0
 260          0             0         0   0.00%  0.00%  0.00%  0        bcmDPC
 253       10690          1069   10000   0.00%  10.00%  2.97%  0        sysd
 251       2380           238   10000   0.00%  0.00%  0.50%  0        kfldintr
 58         30             3    10000   0.00%  0.00%  0.00%  0        sh
 36         50             5    10000   0.00%  0.00%  0.00%  0 13 5 3 1
!----- output truncated -----!

```

Example 3
(cpu stack-unit,
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%
PID      Runtime(ms)   Invoked    uSecs    5Sec   1Min   5Min   TTY      Process
 52       8260           826   10000   0.00%  0.00%  0.22%  0        sysd
 124      1160           116   10000   0.00%  0.00%  0.12%  0        KernLrnAgMv
 116         70             7    10000   0.00%  0.00%  0.00%  0        xstp
 109         50             5    10000   0.00%  0.00%  0.00%  0        span
 108         60             6    10000   0.00%  0.00%  0.00%  0        pim
 103         70             7    10000   0.00%  0.00%  0.00%  0        igmp
 100         70             7    10000   0.00%  0.00%  0.00%  0        mrtm
 96         70             7    10000   0.00%  0.00%  0.00%  0        l2mgr
 92        100            10    10000   0.00%  0.00%  0.00%  0        l2pm
 86         30             3    10000   0.00%  0.00%  0.00%  0        arpm
 83         40             4    10000   0.00%  0.00%  0.00%  0        ospf
 80        100            10    10000   0.00%  0.00%  0.00%  0        dsm
 74         60             6    10000   0.00%  0.00%  0.00%  0        rtm
 70         30             3    10000   0.00%  0.00%  0.00%  0        rip
 68        120            12    10000   0.00%  0.00%  0.00%  0        ipml
 64         70             7    10000   0.00%  0.00%  0.00%  0        acl
 63         30             3    10000   0.00%  0.00%  0.00%  0        bcmLINK.1
 62        290            29    10000   0.00%  0.00%  0.00%  0        bcmCNTR.1
 61         50             5    10000   0.00%  0.00%  0.00%  0        bcmRX
 60         40             4    10000   0.00%  0.00%  0.00%  0        bcmLINK.0
 59          0             0         0   0.00%  0.00%  0.00%  0        bcmXGS3AsyncTX
 58          0             0         0   0.00%  0.00%  0.00%  0        bcmTX
 57        340            34    10000   0.00%  0.00%  0.00%  0        bcmCNTR.0
 55          0             0         0   0.00%  0.00%  0.00%  0        bcmDPC
 117        60             6    10000   0.00%  0.00%  0.00%  0        frpp
 28          0             0         0   0.00%  0.00%  0.00%  0        inetd
 21        450            45    10000   0.00%  0.00%  0.00%  0        mount_mfs
 18        130            13    10000   0.00%  0.00%  0.00%  0        mount_mfs
 11          0             0         0   0.00%  0.00%  0.00%  0        syslogd
 6          30             3    10000   0.00%  0.00%  0.00%  0        sh
 5         10             1    10000   0.00%  0.00%  0.00%  0        aiodoned
 4          0             0         0   0.00%  0.00%  0.00%  0        ioflush
 3         20             2    10000   0.00%  0.00%  0.00%  0        reaper

```

```

2          0          0          0    0.00%  0.00%  0.00%  0          pagedaemon
1          0          0          0    0.00%  0.00%  0.00%  0          init
0          10         1         10000  0.00%  0.00%  0.00%  0          swapper

```

Example 4
(memory,
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: 130596864, CurrentFree: 29634560
SharedUsed : 14261872, SharedFree  : 6709672
PID  Process      ResSize      Size      Allocs      Frees      Max      Current
124 KernLrnAgMv    140410880      0          0          0          0          0
117 frrp           5677056       217088     87650      0          87650     87650
116 xstp          7585792      1536000    551812     49692     518684    502120
109 span          5709824      221184     55386      0          55386     55386
108 pim           5869568      720896     12300      0          12300     12300
103 igmp          5513216      327680     18236     16564     18236     1672
100 mrtm          6905856      516096     72846      0          72846     72846
96  l2mgr         6107136      491520     254858     115948    172038    138910
92  l2pm          5607424      221184     667578     579740    120966    87838
86  arpm          5353472      208896     54528     16564     54528     37964
83  ospf          4210688      475136      0          0          0          0
80  dsm           6057984      552960     22838      0          22838     22838
74  rtm           6311936      577536     574792     298152    376024    276640
70  rip           5001216      249856      528        0          528        528
68  ipml          5292032      339968     67224      0          67224     67224
64  acl           5607424      544768     140086     66256     123522    73830
63  bcmLINK.1    40410880      0          0          0          0          0
62  bcmCNTR.1    140410880      0          0          0          0          0
61  bcmRX        140410880      0          0          0          0          0
60  bcmLINK.0    140410880      0          0          0          0          0
59  bcmXGS3AsyncTX 140410880      0          0          0          0          0
0
58  bcmTX        140410880      0          0          0          0          0
57  bcmCNTR.0    140410880      0          0          0          0          0
55  bcmDPC        140410880      0          0          0          0          0
52  sysd          44650496     22876160    3930856    1358248    2589172    2572608
28  inetd         876544        69632      0          0          0          0
21  mount_mfs     22642688     1953792      0          0          0          0
!----output truncated -----!

```

Example 5
(stack-unit,
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
117 frrp           5677056       217088     87650      0          87650     87650
116 xstp          7585792      1536000    551812     49692     518684    502120
109 span          5709824      221184     55386      0          55386     55386
108 pim           5869568      720896     12300      0          12300     12300
103 igmp          5513216      327680     18236     16564     18236     1672
100 mrtm          6905856      516096     72846      0          72846     72846
96  l2mgr         6107136      491520     254858     115948    172038    138910

```



```

92 l2pm          5607424      221184      667578      579740      120966      87838
86 arpm          5353472      208896      54528       16564       54528       37964
83 ospf          4210688      475136      0            0            0            0
80 dsm           6057984      552960      22838       0            22838       22838
74 rtm           6311936      577536      574792      298152      376024      276640
70 rip           5001216      249856      528         0            528         528
68 ipm1          5292032      339968      67224       0            67224       67224
!----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 hardware system-flow	Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.
show interfaces stack-unit	Display information on all interfaces on a specific S-Series stack member.
show processes memory (S-Series)	Display CPU usage information based on processes running in an S-Series

show processes ipc flow-control

C **E** **S** 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. Refer to [Example 5 \(ipc flow-control, S-Series\)](#).

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
(ipc flow-control,
C-Series)

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

Q Statistics on CP Processor
  TxProcess    RxProcess    Cur    High    Time    Retr    Msg    Ack    Aval    Max
              Len        Mark   Out    ies    Sent    Rcvd  Retra  Retra
              0        0      0     0     0     0     0     0     10   10
    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     0     2     2     50   50
    CFG0    CFGDATASYNC0  0         2      0     0     7     7    255  255
    DHCP0      ACL0          0         1      0     0     9     9     25   25
    DHCP0      IFMGR0         0         0      0     0     0     0     25   25
    RTM0      ARPMGR0        0         1      0     0     1     1    136  136
    ACL20      IGMP0          0         0      0     0     0     0     50   50
    LACP0      IFMGR0         0         2      0     0     4     4     25   25
    ARPMGR0    MRTM0          0         0      0     0     0     0    100  100
    ACL20      PIM0           0         0      0     0     0     0     50   50
    MACMGR0    ACL0           0         1      0     0     1     1     25   25
    TCLASSMGR0 ARPMGR0        0         0      0     0     0     0    100  100
    IFMGR0      IPMGR2         0         6      0     0     44    44     8     8

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

Example 2
(ipc flow-control
rp, E-Series)

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

Q Statistics on CP Processor
  TxProcess    RxProcess    Cur    High    Time    Retr    Msg    Ack    Aval    Max
              Len        Mark   Out    ies    Sent    Rcvd  Retra  Retra
              0        1      0     0     6     6     25   25
    DHCP0      ACL0          0         0      0     0     0     0     25   25
    DHCP0      IFMGR0         0         3      0     0     27    27     8     8
    IFMGR0      FEFD0         0         6      0     0     44    44     8     8
    IFMGR0      IPMGR0         0         1      0     0     16    16     8     8
    IFMGR0      SNMP0          0         4      0     0     31    31     8     8
    IFMGR0      SFL_CP0        0         1      0     0     6     6     8     8
    IFMGR0    EVENTITERMLOG0  0         0      0     0     0     0     8     8
    IFMGR0      PORTMIRRO      0         1      0     0     6     6     8     8
    IFMGR0      DHCP0          0         2      0     0     13    13     8     8
    IFMGR0      TCLASSMGR0     0         3      0     0     25    25     8     8
    IFMGR0      VRRP0          0         2      0     0     21    21     8     8
    TCLASSMGR0 ARPMGR0        0         0      0     0     0     0    100  100
    IFMGR0      IPMGR2         0         6      0     0     44    44     8     8

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

Table 7-9, "Description of show processes ipc flow-control cp output," in Control and Monitoring list the definitions of the fields shown in Example 1 (ipc flow-control, C-Series) and Example 2 (ipc flow-control rp, E-Series).

Table 7-9. Description of show processes ipc flow-control cp output

Field	Description
Source QID /Tx Process	Source Service Identifier
Destination QID/Rx Process	Destination Service Identifier
Cur Len	Current number of messages enqueued
High Mark	Highest number of packets in the queue at any point of time
#of to / Timeout	Timeout count
#of Retr /Retries	Number of retransmissions

Table 7-9. Description of show processes ipc flow-control cp output

Field	Description
#msg Sent/Msg Sent/	Number of messages sent
#msg Ackd/Ack Rcvd	Number of messages acknowledged
Retr /Available Retra	Number of retries left
Total/ Max Retra	Number of retries allowed

**Example 3
(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->ipMgr0       0   0   0   0   0     0  25 25
FTOS#
```

**Example 4
(ipc flow-control
lp)**

```
FTOS#show processes ipc flow-control lp 10
Q Statistics on LP 10
      TxProcess  RxProcess      Cur   High  Time  Retries  Msg   Ack   Aval  Max
              Len   Mark   Out   Retries  Sent  Rcvd  Retra  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
IFAGT10       IFMGRO         0     1     0     0         1     1     8     8
LPDMACAGENT10 MACMGRO        0     0     0     0         0     0     25    25
FTOS#
```

**Example 5
(ipc flow-control,
S-Series)**

```
FTOS#show processes ipc flow-control
Q Statistics on CP Processor
      TxProcess  RxProcess      Cur   High  Time  Retr  Msg   Ack  Aval  Max
              Len   Mark   Out  ies   Sent  Rcvd  Retra  Retra
-----
ACL0          RTM0           0     0     0     0     0     0    10    10
ACL0          DIFFSERVO     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
LACP0         IFMGRO        0     0     0     0     0     0    25    25
RTM0          ARPMGRO       0     0     0     0     0     0   136   136
MACMGRO       ACL0          0     0     0     0     0     0    25    25
ARPMGRO       MRTM0         0     0     0     0     0     0   100   100
DHCP0         ACL0          0     1     0     0     1     1    25    25
DHCP0         IFMGRO        0     0     0     0     0     0    25    25
L2PM0         SPANMGRO      0     2     0     0    14    14    25    25
ARPMGRO       FIBAGT0       0     1     0     0     1     1   100   100
SPANMGRO      MACMGRO       0     0     0     0     0     0    25    25
SPANMGRO      IPMGRO        0     0     0     0     0     0    25    25
SPANMGRO      L2PM0         0     0     0     0     0     0    25    25
STP0          L2PM0         0     0     0     0     0     0    25    25
```

```

          RTM0          FIBAGT0          0          2          0          0          4          4          255          255
          L2PM0          STP0            0          5          0          0          5          5          25          25
ACL_AGENT0          PIM0            0          0          0          0          0          0          20          20
ACL_AGENT0          PIM0            0          0          0          0          0          0          20          20
          FRRP0          L2PM0          0          0          0          0          0          0          25          25
          L2PM0          FRRP0          0          1          0          0          13         13          25          25
          ACL0          ACL_AGENT0        0          4          0          0          7          7          90          90
          ACL0          MACAGENT0        0          0          0          0          0          0          90          90
          IFMGR0        EVENTTERMLG0      0          1          0          0          1          1          8          8
          IFMGR0          SNMP0            0          1          0          0          1          1          8          8
          IFMGR0          IPMGR0           0          7          0          0          9          9          8          8
          IFMGR0          DIFFSERVO        0          2          0          0          3          3          8          8
          DIFFSERVO     ACL_AGENT0        0          0          0          0          0          0          100         100
!-----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 queue³ for a receiving task and waits for an acknowledgement.
- If no response is received within a defined period of time, the SWP timeout mechanism resubmits the message at the head of the FIFO queue.
- After retrying a defined number of times, the following timeout message is generated:

SWP-2-NOMORETIMEOUT

- In the display output in [Example 5 \(ipc flow-control, S-Series\)](#), 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)

C **E** 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

- cp** (OPTIONAL) Enter the keyword **cp** to view memory usage of the Control Processor.
- 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 E600/E600i, 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

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
Version 7.4.1.0	Added lp all and lp summary options
Version 6.5.1.0	For rp1 and rp2 only, the output displays memory consumption of all the processes including a summary (refer to Example 2 (memory rp1) and Example 3 (memory rp2)).

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 FTOS 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 FTOS 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 1

```
FTOS#show processes memory
Memory Statistics On CP Processor (bytes)
=====
Total: 452689184, MaxUsed: 64886986, CurrentUsed: 64873866, Current
TaskName TotalAllocated TotalFreed MaxHeld CurrentHolding
tRootTask 39083408 1395840 38143920 37687568
tARL 64 0 64 64
tBcmTask 256 0 256 256
tPortmapd 18560 0 18560 18560
tShell 3440 0 3440 3440
tPingTmo0 0 1088 0 0
tExcTask 0 592864 0 0
tme 4002494 192 4002302 4002302
ipc 34060 192 34060 33868
irc 943436 0 943436 943436
RpmAvailMgr 9376 32 9344 9344
ev 133188 0 133188 133188
evterm 26752 0 26752 26752
evhdlr 2528 8064 2528 0
dlm 7556256 7366960 1239104 189296
dla 416 0 416 416
tsm 15136 0 15136 15136
fmg 766560 0 766560 766560
fileProc 416 0 416 416
sysAdmTsk 42028 0 42028 42028
```

Example 2 (memory rp1)

```
FTOS#show processes memory rp1
Total      : 954650624, MaxUsed      : 114135040 [3/8/2006 15:1:42]
CurrentUsed: 114135040, CurrentFree: 840515584
SharedUsed : 7849096, SharedFree : 13122448

PID Process ResSize Size Allocs Frees Max Current
```

124	ospf	3215360	425984	0	0	0	0
119	dsm	7749632	1859584	797026	0	797026	797026
114	ipml	3821568	229376	297324	0	297324	297324
112	rtm	4722688	421888	925008	0	925008	925008
107	rip	3731456	253952	198216	0	198216	198216
104	acl	4734976	430080	1127524	0	1127524	1127524
100	sysdl	11636736	2019328	965798	0	965798	965798
98	sysmon	528384	94208	0	0	0	0
36	sshd	1286144	430080	0	0	0	0
34	inetd	663552	98304	0	0	0	0
32	mount_mfs	42397696	2514944	0	0	0	0
19	mount_mfs	364544	2449408	0	0	0	0
6	sh	446464	737280	0	0	0	0
5	aiodoned	76529664	0	0	0	0	0
4	ioflush	76529664	0	0	0	0	0
3	reaper	76529664	0	0	0	0	0
2	pagedaemon	76529664	0	0	0	0	0
1	init	139264	2375680	0	0	0	0
0	swapper	76529664	0	0	0	0	0

**Example 3
(memory rp2)**

FTOS#show processes memory rp2

```
Total      : 953700352, MaxUsed      : 149417984 [3/8/2006 12:33:6]
CurrentUsed: 149417984, CurrentFree: 804282368
SharedUsed : 7847200, SharedFree : 13124344
```

PID	Process	ResSize	Size	Allocs	Frees	Max	Current
145	vrrp	3870720	266240	297324	0	297324	297324
141	fvrp	4472832	204800	797010	0	797010	797010
138	xstp	10764288	7155712	367534	0	367534	367534
133	span	4136960	167936	565810	0	565810	565810
132	pim	6664192	516096	2812528	0	2812528	2812528
128	igmp	4112384	344064	627684	0	627684	627684
124	ipm2	3923968	237568	363396	0	363396	363396
120	mrtm	25567232	593920	697790	0	697790	697790
116	l2mgr	4579328	520192	830098	0	830098	830098
112	l2pm	3874816	225280	367446	32948	367446	334498
108	arpm	3702784	208896	268420	0	268420	268420
104	acl2	3485696	94208	132144	0	132144	132144
100	sysd2	11657216	1679360	998834	0	998834	998834
98	sysmon	528384	94208	0	0	0	0
36	sshd	1286144	430080	0	0	0	0
34	inetd	663552	98304	0	0	0	0
32	mount_mfs	41791488	2514944	0	0	0	0
19	mount_mfs	364544	2449408	0	0	0	0
6	sh	446464	737280	0	0	0	0
5	aiodoned	76967936	0	0	0	0	0
4	ioflush	76967936	0	0	0	0	0
3	reaper	76967936	0	0	0	0	0
2	pagedaemon	76967936	0	0	0	0	0
1	init	139264	2375680	0	0	0	0
0	swapper	76967936	0	0	0	0	0

FTOS#

Table 7-10, "Descriptions of show processes memory rp1/rp2 output," in Control and Monitoring defines the fields that appear in the **show processes memory** output.

Table 7-10. Descriptions of show processes memory rp1/rp2 output

Field	Description
Total:	Total system memory available
MaxUsed:	Total maximum memory used ever (history indicated with time stamp)
CurrentUsed:	Total memory currently in use
CurrentFree:	Total system memory available
SharedUsed:	Total used shared memory
SharedFree:	Total free shared memory
PID	Process ID
Process	Process Name
ResSize	Actual resident size of the process in memory
Size	Process test, stack, and data size
Allocs	Total dynamic memory allocated
Frees	Total dynamic memory freed
Max	Maximum dynamic memory allocated
Current	Current dynamic memory in use

show processes memory (S-Series)

S 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

- Version 7.7.1.0 Modified: Added management-unit option
- Version 7.6.1.0 Introduced on S-Series

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 FTOS processes are counted.

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

Example 1 (show processes memory)

```
FTOS#show processes memory stack-unit 0
Total: 268435456, MaxUsed: 2420244, CurrentUsed: 2420244, Current-
Free: 266015212
```

TaskName	TotalAllocated	TotalFreed	MaxHeld	CurrentHolding
tme	435406	397536	54434	37870
ipc	16652	0	16652	16652
timerMgr	33304	0	33304	33304
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 2 (show processes management-unit)

```
FTOS#show processes management-unit
Total      : 151937024, MaxUsed      : 111800320 [2/25/2008 4:18:53]
CurrentUsed: 98848768, CurrentFree: 53088256
SharedUsed : 13007848, SharedFree  : 7963696
```

PID	Process	ResSize	Size	Allocs	Frees	Max	Current
337	KernLrnAgMv	117927936	0	0	0	0	0
331	vrrp	5189632	249856	50572	0	50572	50572
323	frrp	5206016	241664	369238	0	369238	369238
322	xstp	7430144	2928640	38328	0	38328	38328
321	pim	5267456	823296	62168	0	62168	62168
314	igmp	4960256	380928	18588	16564	18588	2024
313	mrtm	6742016	1130496	72758	0	72758	72758
308	l2mgr	5607424	552960	735214	380972	619266	354242
301	l2pm	5001216	167936	1429522	1176044	286606	253478
298	arpm	4628480	217088	71092	33128	71092	37964
294	ospf	5468160	503808	724204	662560	78208	61644
288	dsm	6778880	1159168	39490	16564	39490	22926
287	rtm	5713920	602112	442280	198768	376024	243512
284	rip	4562944	258048	528	0	528	528
281	lACP	4673536	266240	221060	0	221060	221060
277	ipml	4837376	380928	83788	0	83788	83788
273	acl	5005312	512000	239564	149076	123616	90488
272	topoDPC	117927936	0	0	0	0	0
271	bcmNHOP	117927936	0	0	0	0	0
270	bcmDISC	117927936	0	0	0	0	0
269	bcmATP-RX	117927936	0	0	0	0	0
268	bcmATP-TX	117927936	0	0	0	0	0
267	bcmSTACK	117927936	0	0	0	0	0
266	bcmRX	117927936	0	0	0	0	0
265	bcmLINK.0	117927936	0	0	0	0	0

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

Table 7-11, "Descriptions of show processes memory output," in Control and Monitoring defines the fields that appear in the **show processes memory** output.

Table 7-11. Descriptions of show processes memory output

Field	Description
Total:	Total system memory available
MaxUsed:	Total maximum memory used ever (history indicated with time stamp)
CurrentUsed:	Total memory currently in use
CurrentFree:	Total system memory available
SharedUsed:	Total used shared memory
SharedFree:	Total free shared memory
PID	Process ID
Process	Process Name
ResSize	Actual resident size of the process in memory
Size	Process test, stack, and data size
Allocs	Total dynamic memory allocated
Frees	Total dynamic memory freed
Max	Maximum dynamic memory allocated
Current	Current dynamic memory in use

show processes switch-utilization

E 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 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

E-Series Example

```
-- RPM card 0 --
Status      : active
Next Boot   : online
Card Type   : RPM - Route Processor Module (LC-EH-RPM)
Hardware Rev : 3.1
Num Ports   : 1
Up Time     : 18 hr, 48 min
Last Restart : reset by user
FTOS Version : 8-4-1-317
Jumbo Capable : yes
CP Boot Flash : A: 2.5.1.0 [booted] B: 2.5.1.0
RP1 Boot Flash: A: 2.5.1.0 [booted] B: 2.5.1.0
RP2 Boot Flash: A: 2.5.1.0 [booted] B: 2.5.1.0
CP Mem Size  : 1073741824 bytes
RP1 Mem Size : 1073741824 bytes
RP2 Mem Size : 1073741824 bytes
MMC Mem Size : 3566329856 bytes
External MMC : 128180224 bytes
USB Mem Size : n/a
Temperature  : 36C
Power Status : AC
Voltage      : ok
Serial Number : FX000056234
Part Number  : 7520043401 Rev 05
Vendor Id    : 04
Date Code    : 01072010
Country Code : 01
Piece Part ID : N/A
PPID Revision : N/A
Service Tag   : N/A
Expr Svc Code : N/A
```

Table 7-12, "Descriptions of show rpm output," in Control and Monitoring defines the fields displayed in the example above.

Table 7-12. Descriptions of show rpm output

Field	Description
Status	Displays the RPM's status.
Next Boot	Displays whether the RPM is to be brought online at the next system reload.
Card Type	Displays the RPM catalog number.
Hardware Rev	Displays the E-Series chipset hardware revision level: 1.0 (non-Jumbo); 1.5 (Jumbo-enabled); 2.0 (or above is TeraScale).
Num Ports	Displays the number of active ports.
Up Time	Displays the number of hours and minutes since the RPM's last reboot.
Last Restart	States the reason for the last RPM reboot. C-Series possible values: <ul style="list-style-type: none"> • "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: <ul style="list-style-type: none"> • "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)
FTOS 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.
RP2 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

clients	Enter the keyword clients to display IFM client information.
summary	(OPTIONAL) Enter the keyword summary to display brief information about IFM clients.
ifagt number	Enter the keyword ifagt followed by the number of an interface agent to display software pipe and IPC statistics.
ifcb interface	Enter the keyword ifcb followed by one of the following interface IDs followed by the slot/port information to display interface control block information for that interface: <ul style="list-style-type: none"> For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet. For a Port Channel interface, enter the keyword port-channel followed by a number: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 E-Series Range: 1 to 255 for TeraScale and 1 to 512 for ExaScale. For a 10G Ethernet interface, enter the keyword TenGigabitEthernet. C-Series options also include: <ul style="list-style-type: none"> fastethernet for a Fast Ethernet interface loopback for a Loopback interface managementethernet for a Management Ethernet interface null for a Null interface vlan for a VLAN interface (Range: 1–4094, 1-2094 for ExaScale)
stack-unit unit-ID	Enter the keyword stack-unit followed by the stack member number to display IFM information for that unit. Range: 0-1 Note: This option is only available on S-Series.
trace-flags	Enter the keyword trace-flags to display IFM information for internal trace flags.

Defaults None

Command Mode EXEC
EXEC Privilege

Command History Version 7.6.1.0 Introduced for C-Series and S-Series

S-Series Example

```
FTOS#show software ifm clients summary
ClntType  Inst      svcMask  subSvcMask  tlvSvcMask  tlvSubSvc  swp
IPM       0         0x00000000 0x00000000 0x90ff71f3 0x021e0e81 31
RTM       0         0x00000000 0x00000000 0x800010ff 0x01930000 43
VRRP     0         0x00000000 0x00000000 0x803330f3 0x00400000 39
```


```

L2PM      0      0x00000000 0x00000000 0x87ff79ff 0x0e032200 45
ACL       0      0x00000000 0x00000000 0x867f50c3 0x000f0218 44
OSPF      0      0x00000dfa 0x00400098 0x00000000 0x00000000 0
PIM       0      0x000000f3 0x00030000 0x00000000 0x00000000 0
IGMP      0      0x000e027f 0x00000000 0x00000000 0x00000000 0
SNMP      0      0x00000000 0x00000000 0x800302c0 0x00000002 30
EVTTERM   0      0x00000000 0x00000000 0x800002c0 0x00000000 29
MRTM      0      0x00000000 0x00000200 0x81f7103f 0x00000000 38
DSM       0      0x00000000 0x00000000 0x80771003 0x00000000 32
LACP      0      0x00000000 0x00000000 0x8000383f 0x00000000 35
DHCP      0      0x00000000 0x00000000 0x800000c2 0x0000c000 37
V6RAD     0      0x00000433 0x00030000 0x00000000 0x00000000 0
Unidentified Client0      0x006e0002 0x00000000 0x00000000 0x00000000 0

FTOS#

```

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

Example FTOS# show switch links backplane

Switch fabric backplane link status:

```

                SFM0 Links Status                SFM1 Links Status
LC SlotID  Port0 | Port1 | Port2 | Port3 | Port4 | Port5 | Port6 | Port7
0          up   up     up     up     down  down  down  down
1          not present
2          not present
3          not present
4          not present
5          not present
6          up   up     up     up     down  down  down  down
7          not present
up - Both ends of the link are up
down - Both ends of the link are down
up / down - SFM side up and LC side down
down / up - SFM side down and LC side up
FTOS#

```

show system (S-Series)

S 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

[Example 1](#) shows the output from the **show system brief** command.

[Example 2](#) shows the output from the **show system stack-unit** command.

Example 1 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 2

```

FTOS#
FTOS#show system stack-unit 0
-- Unit 0 --
Unit Type      : Management Unit
Status         : online
Next Boot      : online
Required Type  : Z9000 - 32-port TE/FG (ZB)
Current Type   : Z9000 - 32-port TE/FG (ZB)
Master priority : 0
Hardware Rev   : 3.0
Num Ports      : 128
Up Time        : 8 min, 50 sec
FTOS Version   : 8.3.11.3b
Jumbo Capable  : yes
POE Capable    : no
Boot Flash     : 3.0.1.1
BIOS version   : 3.0.0.0
Memory Size    : 3472461824 bytes
Temperature    : 44C
Voltage        : ok
Serial Number   : Z8FX113100308
Part Number    : 7520052401 Rev E
Vendor Id      : 04
Date Code      : 06312011
Country Code   : 01
Piece Part ID  : N/A
Version        : N/A
Service Tag    : N/A
Auto Reboot    : disabled
Burned In MAC  : 00:01:e8:a0:bf:eb
No Of MACs     : 3

```

-- Power Supplies --

Unit	Bay	Status	Type	Temperature(deg C)	FanSpeed(rpm)
0	0	up	AC	45	16853
0	1	absent		0	0

-- Fan Status --

Unit	Bay	TrayStatus	Fan0	Speed	Fan1	Speed
0	0	up	up	2700	up	2700
0	1	up	up	2700	up	2700
0	2	up	up	2700	up	2700
0	3	up	up	2700	up	2700

Speed in RPM

Related Commands

show version	Display the FTOS version.
show processes memory (S-Series)	Display memory usage based on running processes.
show system stack-ports	Display information about the stack ports on all switches in the S-Series stack.
show hardware stack-unit	Display the data plane and management plane input and output statistics of a particular stack member.
stack-unit priority	Configure the ability of an S-Series switch to become the management unit of a stack.

show tech-support (C-Series and E-Series)

C **E** Display, or save to a file, a collection of data from other show commands, the information necessary for Dell Force10 technical support to perform troubleshooting.

Syntax `show tech-support [linecard 0-6 | page] | { display | except | find | grep | no-more | save }`

Parameters

linecard 0-6	(OPTIONAL) Enter the keyword linecard followed by the linecard number to view information relating to a specific linecard.
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.
display, except, find, grep, no-more	If you use the pipe command (), then enter one of these keywords to filter command output. Refer to Chapter 4, CLI Basics 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))

Command Modes EXEC Privilege

Command History

Version 7.8.1.0	Introduced save to file options
Version 7.5.1.0	Introduced on C-Series
Version 6.5.4.0	Show clock included in display on E-Series

C-Series Example

```
FTOS#show tech-support page
----- show version -----
Dell Force10 Networks Real Time Operating System Software
Dell Force10 Operating System Version: 1.0
Dell Force10 Application Software Version: FTOS 7.5.1.0
Copyright (c) 1999-2011 by Dell Inc.
Build Time: Tue Sep 12 15:39:17 IST 2012
Build Path: /sites/maa/work/sw//C-SERIES/SW/SRC
FTOS 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 mem-
ory.
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----

```

E-Series Example

```

FTOS#show tech-support ?
linecard          Line card
page              Page through output
|                Pipe through a command
<cr>

FTOS#show tech-support linecard 3 | ?
display          Display additional information
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 linecard 3 | save ?
flash:          Save to local file system (flash://filename (max 20
chars) )
slot0:         Save to local file system (slot0://filename (max 20
chars) )

FTOS#show tech-support linecard 3 | save flash://LauraSave
Start saving show command report .....

FTOS#dir
Directory of flash:

  1  drwx      32768   Jan 01 1980 00:00:00 +00:00 .
  2  drwx       512   Aug 22 2008 14:21:13 +00:00 ..
  3  drwx      8192   Mar 30 1919 10:31:04 +00:00 TRACE_LOG_DIR
  4  drwx      8192   Mar 30 1919 10:31:04 +00:00 CRASH_LOG_DIR
  5  drwx      8192   Mar 30 1919 10:31:04 +00:00 NVTRACE_LOG_DIR
  6  drwx      8192   Mar 30 1919 10:31:04 +00:00 CORE_DUMP_DIR
  7  d---      8192   Mar 30 1919 10:31:04 +00:00 ADMIN_DIR
  8  -rwx    33059550  Jul 11 2007 17:49:46 +00:00 FTOS-EF-7.4.2.0.bin
  9  drwx      8192   Jan 01 1980 00:18:28 +00:00 diag

```

```

10 -rwx 29555751 May 12 2008 17:29:42 +00:00 FTOS-EF-4.7.6.0.bin
11 -rwx 27959813 Apr 04 2008 15:05:12 +00:00 FTOS-EF-7.5.1.0.bin
12 -rwx 4693 May 12 2008 17:24:36 +00:00 config051508
13 -rwx 29922288 Jan 11 2008 14:58:36 +00:00 FTOS-EF-7.6.1.0.bin
14 -rwx 6497 Aug 22 2008 14:18:56 +00:00 startup-config
15 -rwx 5832 Jul 25 2008 11:13:36 +00:00 startup-config.bak
16 -rwx 29947358 Jul 25 2008 11:04:26 +00:00 FTOS-EF-7.6.1.2.bin
17 -rwx 10375 Aug 25 2008 10:55:18 +00:00 LauraSave

```

```

flash: 520962048 bytes total (40189952 bytes free)
FTOS#

```

Usage Information

Without the **linecard** or **page** option, the command output is continuous, use **CNTL-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 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**

Related Commands

show version	Display the FTOS version.
show linecard	Display the line card(s) status.
show environment (C-Series and E-Series)	Display system component status.
show processes memory (C-Series and E-Series)	Display memory usage based on running processes.

show tech-support (S-Series)

S 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.
When using the pipe command (|), enter one of these keywords to filter command output. Refer to [Chapter 4, CLI Basics](#) for details on filtering commands.

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

Command Modes EXEC Privilege

Command History

Version 7.8.1.0	Introduced save to file options
Version 7.6.1.0	Expanded to support S-Series switches

Example 1 (show tech-support save)

```
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#

```

Example 2
(show
tech-support)

```

FTOS#show tech-support stack-unit 0
----- show version -----
Dell Force10 Networks Real Time Operating System Software
Dell Force10 Operating System Version: 1.0
Dell Force10 Application Software Version: FTOS 7.6.1.0
Copyright (c) 1999-2011 by Dell Inc.
Build Time: Tue Sep 12 15:39:17 IST 2012
Build Path: /sites/maa/work/sw/purushothaman/cser-latest/depot/main/Dev/
Cyclone/Force10 uptime is 18 minutes
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)
----- show clock -----
12:03:01.695 UTC Wed Nov 21 2007

----- show running-config -----
Current Configuration ...
! Version E_MAIN4.7.5.414
! Last configuration change at Wed Nov 21 11:42:19 2007 by default
!
service timestamps log datetime
!
hostname FTOS
!
enable password 7 xxxxxxxx
!
username admin password 7 xxxxxxxx
!
enable restricted 7 xxxxxxxx
!
interface GigabitEthernet 0/1
  no ip address
  shutdown
!
interface GigabitEthernet 0/2
  no ip address
  shutdown
!
!----- output truncated -----!

```

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**

show version	Display the FTOS version.
show system (S-Series)	Display the current switch status.
show environment (S-Series)	Display system component status.
show processes memory (S-Series)	Display memory usage based on running processes.

show util-threshold cpu

C **E** **S** Display the set CPU utilization threshold values.

Syntax show util-threshold cpu

Defaults None

Command Modes EXEC PRIVILEGE

Command History Version 8.4.1.0 Introduced on C-Series, E-Series, S25 and S50

Usage Information For C- and E-Series, this command displays all the CPU thresholds of the type of processor that is busy.

For S-Series, this command displays all the CPU thresholds of the management, standby and stack-units.

**Related
Commands**

util-threshold cpu (C- and E-Series)	Set the CPU utilization threshold values for C- and E-Series platforms
util-threshold cpu (S-Series)	Set the CPU utilization threshold values for S50 and S25 platforms
util-threshold mem (C- and E-Series)	Set the memory utilization threshold values for C- and E-Series platforms
util-threshold mem (S-Series)	Set the memory utilization threshold values for S50 and S25 platforms

show util-threshold mem

C **E** **S** Display the set memory utilization threshold values.

Syntax show util-threshold memory

Defaults None

Command Modes EXEC PRIVILEGE

Command History Version 8.4.1.0 Introduced on C-Series, E-Series, S25 and S50

Usage Information For C- and E-Series, this command displays all the memory utilization thresholds of the type of processor that is busy.

For S-Series, this command displays all the memory utilization thresholds of the management, standby or stack-units.

Related Commands

util-threshold cpu (C- and E-Series)	Set the CPU utilization threshold values for C- and E-Series platforms
util-threshold cpu (S-Series)	Set the CPU utilization threshold values for S50 and S25 platforms
util-threshold mem (C- and E-Series)	Set the memory utilization threshold values for C- and E-Series platforms
util-threshold mem (S-Series)	Set the memory utilization threshold values for S50 and S25 platforms

ssh-peer-rpm

C **E** 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 Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.5.1.0 Introduced on C-Series
Version 6.3.1.0 Introduced on E-Series

Usage Information This command is not available when the peer RPMs are running different FTOS releases.

telnet



Connect through Telnet to a server. The Telnet client and server in FTOS 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 } [/source-interface]`

Parameters

<i>host</i>	Enter the name of a server.
<i>ip-address</i>	Enter the IPv4 address in dotted decimal format of the server.
<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X format followed by the prefix length in the /x format.
<i>prefix-length</i>	Range: /0 to /128 Note: The :: notation specifies successive hexadecimal fields of zeros
<i>vrf instance</i>	(Optional) E-Series Only: Enter the keyword vrf followed by the VRF Instance name.
<i>source-interface</i>	(OPTIONAL) Enter the keywords /source-interface followed by the interface information to include the interface's IP address. Enter the following keywords and slot/port or number information: <ul style="list-style-type: none">• 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 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 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 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 Not configured.

Command Modes EXEC
EXEC Privilege

Command History

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 Telnet to link-local addresses is not supported.

telnet-peer-rpm

C **E** Open a Telnet connection to the peer RPM.

Syntax **telnet-peer-rpm**

Defaults Not configured.

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
Version 6.2.1.1	Introduced on E-Series

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

C **E** **S** Configure the number of lines displayed on the terminal screen.

Syntax **terminal length** *screen-length*

To return to the default values, enter **terminal no length**.

Parameters

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

Defaults 24 lines

Command Modes EXEC
EXEC Privilege

Command History

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	

terminal xml

C **E** Enable XML mode in Telnet and SSH client sessions.

Syntax **terminal xml**

To exit the XML mode, enter **terminal no xml**.

Defaults Disabled

Command Modes EXEC
EXEC Privilege

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.7.1.0	Introduced on C-Series
Version 6.5.1.0	Introduced for E-Series

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 *FTOS Configuration Guide*.

traceroute

C **E** **S** View a packet's path to a specific device.

Syntax **traceroute** {*host* | *vrf instance* | *ip-address* | *ipv6-address*}

Parameters

<i>host</i>	Enter the name of device.
<i>vrf instance</i>	(Optional) E-Series Only : Enter the keyword vrf followed by the VRF Instance name.
<i>ip-address</i>	Enter the IP address of the device in dotted decimal format.
<i>ipv6-address</i>	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 tracerouting 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 1 (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
-----
```

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

```
FTOS#
```

The following text contains examples of the IPv6 **traceroute** command with both a compressed IPv6 address and uncompressed address.

Example 2 (IPv6)

```
FTOS#traceroute 100::1
```

```
Type Ctrl-C to abort.
```

```
-----
Tracing the route to 100::1, 64 hops max, 60 byte packets
-----
```

Hops	Hostname	Probe1	Probe2	Probe3
1	100::1	000.000 ms	000.000 ms	000.000 ms

```
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
-----
```

Hops	Hostname	Probe1	Probe2	Probe3
1	3ffe:501:ffff:100:201:e8ff:fe00:4c8b	000.000 ms	000.000 ms	000.000 ms

```
FTOS#
```

Related Commands

[ping](#) Test connectivity to a device.

undebug all

C **E** **S** Disable all debug operations on the system.

Syntax **undebug all**

Defaults No default behavior or values

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	

upload trace-log

C **E** 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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.5.1.0	Introduced on C-Series and expanded to support command history, hardware trace, and software trace logs
Version 6.1.1.0	Introduced on E-Series

Usage Information The log information is uploaded to flash:/TRACE_LOG_DIR

util-threshold cpu (C- and E-Series)



Configure the high or low CPU utilization thresholds for SNMP traps.

Syntax

```
util-threshold cpu {5sec | 1min | 5min} {rp1 | rp2 | cp | lp slot-id | all} {high {0-100} | {low [0-100]}}
```

To return to the default settings, use the **no util-threshold cpu** command syntax.

Parameters

<i>cpu utilization time</i>	Indicate the length of time in which the cpu has been busy. <ul style="list-style-type: none"> 5sec 1min 5min
<i>processor type</i>	Indicate the type of processor to be used to configure the CPU utilization information. <ul style="list-style-type: none"> rp1 = route processor1 rp2 = route processor2 cp = control processor lp <i>slot-id</i> = the line card slot-id all = use all of the processors to configure the CPU utilization information.
<i>utilization threshold in %</i>	Indicate the high or low values for the CPU utilization thresholds in percentage format. <ul style="list-style-type: none"> high. Range: 0 - 100 low. Range: 0 - 100 <p>Note: A threshold level of 0 will disable the syslog and SNMP trap.</p>

Example

```
util-threshold cpu 5sec cp high 50
```

In this example, the low threshold value is not specified so it will take the value set for the high threshold value. In all other instances, the low threshold value must be equal to or less than that of the high threshold value.

Defaults

High CPU utilization threshold: 1min = 85%, 5min = 80%

Low CPU utilization threshold: 1min = 75%, 5min = 70%

Command Modes

CONFIG

Command History

Version 8.4.2.3	Introduced on C-Series, S25 and S50
Version 8.4.2.0	Introduced on E-Series TeraScale
Version 8.4.1.0	Introduced on E-Series ExaScale

Usage Information

When the total CPU utilization exceeds the configured threshold for a given time, a threshold notification is sent as a SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value. The system will generate a SYSLOG and SNMP Trap each time the configured threshold is crossed.

Note: The 5sec util-threshold cpu command is disabled by default on all platforms. To enable the command, enter `util-threshold cpu 5sec all high {value greater than zero}`. To disable the SYSLOG and traps for the 5sec cpu utilization thresholds, enter `util-threshold cpu 5sec all high 0` or `no util-threshold cpu 5sec {rp1 | rp2 | cp | lp slot-id | all}`

Related Commands

show util-threshold cpu	Display the set values of the cpu utilization thresholds
show util-threshold mem	Display the set values of the memory utilization thresholds

util-threshold cpu (S-Series)

S Configure the high or low CPU utilization thresholds for SNMP traps.

Syntax util-threshold cpu {5sec | 1min | 5min} {Management-unit | standby | stack-unit *unit-number* | all} {high {0-100} | {low [0-100]}}

To return to the default setting, enter **no util-threshold cpu**.

Parameters

- cpu utilization time* Enter the keyword that indicates the amount of threshold time to configure the CPU utilization thresholds.
- 5sec
 - 1min
 - 5min
- unit* Indicate the unit where you want to configure the CPU utilization thresholds.
- Management-unit
 - standby
 - stack-unit *unit-number* = select the number of the unit in the stack
 - all = use all of the units to configure the cpu utilization information.
- utilization threshold in %* Indicate the high or low values for the CPU utilization threshold in percentage format.
- high. Range: 0 - 100
 - low. Range: 0 - 100
- Note:** A threshold level of 0 will disable the syslog and SNMP trap.

Defaults High threshold cpu default = 92%
Low threshold cpu default = 82%

Command Modes CONFIG

Command History

Version 8.4.2.2	Introduced on C-Series, S25 and S50
Version 8.4.2.0	Introduced on E-Series TeraScale
Version 8.4.1.0	Introduced on E-Series ExaScale

Usage Information When the total CPU utilization exceeds the configured threshold for a given time, a threshold notification is sent as a SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value. The system will generate a SYSLOG and SNMP Trap each time the configured threshold is crossed.

Related Commands

show util-threshold cpu	Display the set values of the cpu utilization thresholds
show util-threshold mem	Display the set values of the memory utilization thresholds

util-threshold mem (C- and E-Series)

C **E** Configure the high or low memory utilization thresholds for SNMP traps.

Syntax util-threshold mem {rp1 | rp2 | cp | lp *slot-id* | all} {high {0-100} | {low [0-100]}}

To return to the default setting, use the **no util-threshold mem** command syntax.

Parameters

<i>processor type</i>	Indicate the type of processor that will be used to configure the memory utilization information. <ul style="list-style-type: none"> rp1 = route processor1 rp2 = route processor2 cp = control processor lp <i>slot-id</i> = the line card slot-id all = use all of the processors to configure the memory utilization information.
<i>utilization threshold in %</i>	Indicate the high or low values for the memory utilization threshold in percentage format. <ul style="list-style-type: none"> high. Range: 0 - 100 low. Range: 0 - 100 <p>Note: A threshold level of 0 will disable the syslog and SNMP trap.</p>

Defaults High threshold default = 92%
Low threshold default = 82%

Command Modes CONFIG

Command History	Version 8.4.2.2	Introduced on C-Series, S25 and S50
	Version 8.4.2.0	Introduced on E-Series TeraScale
	Version 8.4.1.0	Introduced on E-Series ExaScale

Usage Information When the total memory utilization exceeds the configured threshold for a given time, a threshold notification is sent as a SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value.

To return the memory thresholds to the default values, enter **no util-threshold mem rp1 | rp2 | cp | lp *number* | all**

Related Commands	show util-threshold cpu	Display the set values of the cpu utilization thresholds
	show util-threshold mem	Display the set values of the memory utilization thresholds

util-threshold mem (S-Series)

S Configure the high or low memory utilization thresholds for SNMP traps.

Syntax `util-threshold mem {Management-unit | standby | stack-unit unit-number | all} {high {0-100} | {low [0-100]}}`

To return to the default setting, enter the **no util-threshold mem** command syntax.

Parameters

unit Indicate the unit where you want to configure the memory utilization thresholds.

- Management-unit
- standby
- stack-unit *unit-number* = select the number of the unit in the stack
- all = use all of the units to configure the memory utilization information.

utilization threshold in % Indicate the high or low values for the memory utilization in percentage format.

- high. Range: 0 - 100
- low. Range: 0 - 100

Note: A threshold level of 0 will disable the syslog and SNMP trap.

Defaults High threshold default = 92%
Low threshold default = 82%

Command Modes CONFIG

Command History

Version 8.4.2.2	Introduced on C-Series, S25 and S50
Version 8.4.2.0	Introduced on E-Series TeraScale
Version 8.4.1.0	Introduced on E-Series ExaScale

Usage Information

When the total memory utilization exceeds the configured threshold for a given time, a threshold notification is sent as a SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value.

Related Commands

show util-threshold cpu	Display the set values of the cpu utilization thresholds
show util-threshold mem	Display the set values of the memory utilization thresholds

virtual-ip

C **E**

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: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
	E-Series original Command	
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 <code>no virtual-ip</code> command now takes an address/prefix-length argument, so that the desired address only is removed. If <code>no virtual-ip</code> is entered without any specified address, then both IPv4 and IPv6 virtual addresses are removed.	
Example	<pre>FTOS#virtual-ip 10.11.197.99/16 FTOS#virtual-ip fdaa:bbbb:cccc:1004::60/64</pre>	

write



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

Syntax `write {memory | terminal}`

Parameters

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

Command Modes EXEC Privilege

Command History	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 [save](#) Save configurations created in BOOT_USER mode (BLI).

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.

802.1ah

Overview

802.1ah 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

S 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)

S 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)

S 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* | min-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

S 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

S Set the frame error thresholds and window.

Syntax ethernet oam link-monitor frame threshold {high {*frames* | none} | low *frames* | window *frames*}

Parameters

high { <i>frames</i> none}	Specify the high threshold value for frame errors, or disable the high threshold. Range: 1-65535 Default: None
low <i>frames</i>	Specify the low threshold for frame errors. Range: 0-65535 Default: 1
window <i>frames</i>	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

S 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 { <i>milliseconds</i> none }	Specify the high threshold value for frame error seconds per time period, or disable the high threshold. Range: 1-900 Default: None
low <i>milliseconds</i>	Specify the low threshold for frame error seconds per time period. Range: 1-900 Default: 1
window <i>milliseconds</i>	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

S Disable 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

- S** 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

- S** 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

- S** Set the symbol error thresholds and window.

Syntax ethernet oam link-monitor symbol-period threshold {high { *symbols* | none} | low *symbols* | window *symbols*}

Parameters

high { <i>symbols</i> none }	Specify the high threshold value for symbol errors, or disable the high threshold. Range: 1-65535 Default: None
low <i>symbols</i>	Specify the low threshold for symbol errors. Range: 0-65535 Default: 10
window <i>symbols</i>	Specify the time period for symbol errors per second condition. Range: 1-65535 (times 1,000,000 symbols) Default: 10 (10,000,000 symbols)

Defaults	As above	
Command Mode	INTERFACE	
Command History	Version 8.4.1.0	Introduced on S-Series

ethernet oam mode

S Set the transmission mode to active or passive.

Syntax ethernet oam mode {active | passive}

Parameters active | passive Choose either active or passive mode for the interface.

Defaults Active

Command Mode INTERFACE

Command History Version 8.4.1.0 Introduced on S-Series

ethernet oam remote-failure

S 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

critical-event	An unspecified critical event occurred.
dying-gasp	An unrecoverable local failure condition occurred.
link-fault	A fault occurred in the receive direction of the local peer.
error-block-interface	Block the interface if the specified fault occurs.
error-disable-interface	Disable the interface if the specified fault occurs.

Defaults Disabled

Command Mode INTERFACE

Command History Version 8.4.1.0 Introduced on S-Series

ethernet oam remote-loopback

S Start or stop loopback operation on a local interface with a remote peer.

Syntax ethernet oam remote-loopback {start | stop} interface *interface*

Parameters

start stop	Start or stop a loopback operation with a remote peer.
interface <i>interface</i>	Specify the interface on which remote-loopback starts/stops, for example gigabitethernet 0/1.

Defaults Enabled

Command Mode EXEC Privilege

Command History Version 8.4.1.0 Introduced on S-Series

ethernet oam remote-loopback (interface)

S Enable support for OAM loopback on an interface and configure a timeout value.

Syntax ethernet oam remote-loopback {supported | timeout *seconds*}

Parameters

supported	Start or stop a loopback operation on a peer.
timeout <i>seconds</i>	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 Version 8.4.1.0 Introduced on S-Series

ethernet oam timeout

S Specify the amount of time that the system waits to receive an OAMPDU from a peer before considering it non-operational.

Syntax ethernet oam timeout *value*

Parameters

<i>value</i>	Enter a timeout value in seconds. Range: 2-30 seconds
--------------	--

Defaults 5 seconds

Command Mode INTERFACE

Command History Version 8.4.1.0 Introduced on S-Series

show ethernet oam discovery

S Display the OAM discovery status.

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 Version 8.4.1.0 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

S 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 Version 8.4.1.0 Introduced on S-Series

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 x: 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
FTOS OAMPDU Tx:: 10
FTOS 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 Gasps:: 2
Time Stamp: 00:40:23
Total dying Gasps:: 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

S 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

S Display Link Layer OAM sessions.

Syntax show ethernet oam summary

Defaults None

Command Mode EXEC Privilege

Command History Version 8.4.1.0 Introduced on S-Series

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 AddressOUI ModeCapability
Gi6/1/10023.84ac.b8000000DactiveL R
```


802.1X

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-suplicants`
- `dot1x port-control`
- `dot1x quiet-period`
- `dot1x reauthentication`
- `dot1x reauth-max`
- `dot1x server-timeout`
- `dot1x supplicant-timeout`
- `dot1x tx-period`
- `show dot1x cos-mapping interface`
- `show dot1x interface`

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

FTOS supports RADIUS and Active Directory environments using 802.1X Port Authentication.



Important Points to Remember

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

- 802.1X is supported on C-Series, E-Series, 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	<code>all</code>	Enable all 802.1X debug messages.
	<code>errors</code>	Display information about all 802.1X errors.
	<code>packets</code>	Display information about all 802.1X packets.
	<code>state-machine</code>	Display information about all 802.1X packets.
	<code>interface <i>interface</i></code>	Restricts the debugging information to an interface.

Defaults Disabled

Command Modes EXEC Privilege

Command History 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)

C **E** **S** 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 \(Interface\)](#)

dot1x authentication (Interface)

C **E** **S** 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 \(Configuration\)](#)

dot1x auth-fail-vlan

C **E** **S** 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

<i>vlan-id</i>	Enter the VLAN Identifier. Range: 1 to 4094
max-attempts <i>number</i>	(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](#)
[dot1x guest-vlan](#)
[show dot1x interface](#)

dot1x auth-server

C **E** **S** 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

<i>vlan-id</i>	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](#)
- [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-suplicant authentication.

Defaults single-host

Command Modes INTERFACE

Command History	Version 8.4.1.0	The multi-auth option was introduced on the C-Series and S-Series.
	Version 8.3.2.0	The single-host and multi-host options were introduced on the C-Series, E-Series TeraScale, and S-Series
Usage Information	<ul style="list-style-type: none"> • 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-suppliant mode authenticates every device attempting to connect to the network on through the authenticator port. 	
Related Commands	show dot1x interface	

dot1x mac-auth-bypass

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

Syntax dot1x mac-auth-bypass

Defaults Disabled

Command Modes INTERFACE

Command History Version 8.4.1.0 Introduced on C-Series and S-Series

Usage Information To disable MAC authentication bypass on a port, enter the **no dot1x mac-auth-bypass** command.

Related Commands [dot1x auth-type mab-only](#)

dot1x max-eap-req

C **E** **S** 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

C **E** **T** **S**

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

<i>number</i>	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

C **E** **S**

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

C **E** **S**

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

C **E** **S**

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

dot1x reauth-max

C **E** **S**

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

C **E** **S** Configure the amount of time after which exchanges with the server time out.

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

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

Defaults 30 seconds

Command Modes INTERFACE

Command History
Version 7.6.1.0 Introduced on C-Series and S-Series
Version 7.4.1.0 Introduced on E-Series

dot1x supplicant-timeout

C **E** **S** 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

<i>seconds</i>	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

<i>interface</i>	Enter one of the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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.
<i>mac-address</i>	(Optional) MAC address of an 802.1X-authenticated supplicant.

Defaults No default values or behavior

Command Modes EXEC
EXEC privilege

Command History

Version 8.4.2.1	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-supplicant authentication modes.

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

C **E** **S** Display the 802.1X configuration of an interface.

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

Parameters

interface

Enter one of the following keywords and slot/port or number information:

- For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information.
- For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information.
- For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

mac-address (Optional) MAC address of a supplicant.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 8.4.2.1 Introduced **mac-address** option on the C-Series and S-Series
 Version 7.6.1.0 Introduced on C-Series, E-Series, and S-Series

Usage 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-supplicant authentication is enabled on a port, additional 802.1X configuration details (port authentication status, untagged VLAN ID, authentication PAE state, and backend state) are displayed for each supplicant as shown in [Example 3](#).

Example 1

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

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

Auth PAE State:       Initialize
Backend State:        Initialize

FTOS#
```

Example 2

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

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



```
Re-Auth Interval:      60 seconds
Max-EAP-Req:          2
Host Mode:            MULTI_AUTH
Max-SupPLICANTS:     128
```

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

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

Example 3

```
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   

FTOS 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 [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

C **E** **S**

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

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

remark

C **E** **S**

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

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 6.4.1.0	Introduced for E-Series

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

```
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

[show config](#) Display the current ACL configuration.

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

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 6.2.1.1	Introduced

Example

```
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.

C and **S** platforms support Ingress IP ACLs only.

Ingress and Egress IP ACL are supported on platform: **E** **S**

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

C **E** **S** 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	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 6.2.1.1	Introduced

clear counters ip access-group

C **E** **S** 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	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 6.2.1.1	Introduced

ip access-group

C **E** **S** Assign an IP access list (IP ACL) to an interface.

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

Parameters	<i>access-list-name</i>	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 <i>vlan-id</i>	(OPTIONAL) Enter the keyword vlan followed by the ID numbers of the VLANs. Range: 1 to 4094, 1-2094 for ExaScale (can used IDs 1-4094)

Defaults Not enabled.

Command Modes INTERFACE

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 6.2.1.1	Introduced

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

C **E** **S**

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]`

Parameters

access-list-name

Enter the name of a configured IP 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: 1-128

E-Series Range: 1 to 255 for TeraScale and 1 - 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.

in | out

Identify whether ACL is applied on ingress or egress side.

Command Modes EXEC Privilege

Command History

Version 8.4.1.0

Introduced

show ip accounting access-list

C **E** **S**

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

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

Parameters

access-list-name

Enter the name of the ACL to be displayed.

cam_count

List the count of the CAM rules for this ACL.

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 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.

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 6.2.1.1	Introduced

Example 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 10-13, "show ip accounting access-lists Command Example Field," in Access Control Lists (ACL) defines the information in the example above.



Table 10-13. show ip accounting access-lists Command Example Field

Field	Description
"Extended IP..."	Displays the name of the IP ACL.
"seq 5..."	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.
"order 4"	Displays the QoS order of priority for the ACL entry.

Standard IP ACL Commands

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

 and  platforms support Ingress IP ACLs only.

Ingress and Egress IP ACL are supported on platform:  

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

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
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 (discontiguous).
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 only.
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 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 <i>FTOS Configuration Guide</i> .
fragments	Enter the keyword fragments to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-STANDARD-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	Added support for S-Series
Version 7.5.1.0	Added support for C-Series
Version 7.4.1.0	Added support for non-contiguous mask and added the monitor option.
Version 6.5.1.0	Expanded to include the optional QoS order priority for the ACL entry.

Usage Information

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

The **order** option is relevant in the context of the Policy QoS feature only. See the "Quality of Service" chapter of the *FTOS 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 46, 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**

[ip access-list standard](#) Configure a standard ACL.
[permit](#) Configure a permit filter.

ip access-list standard



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

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

Parameters

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

Defaults

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

Command Modes

CONFIGURATION

**Command
History**

Version 8.1.1.0	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	Added support for S-Series
Version 7.5.1.0	Added support for C-Series
Version 7.4.1.0	Added support for non-contiguous mask and added the monitor option.
Version 6.5.1.0	Expanded to include the optional QoS order priority for the ACL entry.

**Usage
Information**

FTOS supports one ingress and one egress IP 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.

Example

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

**Related
Commands**

[ip access-list extended](#) Create an extended access list.
[show config](#) Display the current configuration.

permit



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

Syntax

permit { *source* [*mask*] | **any** | **host** *ip-address* } [**count** [**byte**] | **log**] [**dscp** *value*] [**order**] [**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** { *source* [*mask*] | **any** | **host** *ip-address* } command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
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 <i>ip-address</i>	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.
dscp	(OPTIONAL) Enter the keyword dscp to match to the IP DCSCP values.
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 <i>FTOS Configuration Guide</i> .

Defaults Not configured.

Command Modes CONFIGURATION-STANDARD-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	Added support for S-Series
Version 7.5.1.0	Added support 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 *FTOS 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 46, 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

- [deny](#) Assign a IP ACL filter to deny IP packets.
- [ip access-list standard](#) Create a standard ACL.

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: 1 - 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

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

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

StartingSeqNum Enter the starting sequence number to resequence.
Range: 1 – 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 8.1.1.0 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 Added support for S-Series

Version 7.5.1.0 Added support 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 prefix list.

Prior to 7.8.1.0, names are up to 16 characters long.

Related Commands

[resequence access-list](#) Resequence an access-list

seq

C **E** **S**

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

Syntax `seq sequence-number { deny | permit } { source [mask] | any | host ip-address } [count [byte] | 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 <i>ip-address</i>	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 DSCP 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 <i>FTOS Configuration Guide</i> .
fragments	Enter the keyword fragments to use ACLs to control packet fragments.

Defaults Not configured

Command Modes CONFIGURATION-STANDARD-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	Added support for S-Series
Version 7.5.1.0	Added support 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 **monitor** option is relevant in the context of flow-based monitoring only. See [Chapter 46, 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**

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

Extended IP ACL Commands

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

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

 and  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



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**] [**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

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.
<i>ip-protocol-number</i>	Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword count to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.
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 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 <i>FTOS Configuration Guide</i> .
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	Added support for S-Series
Version 7.5.1.0	Added support 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

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

The **order** option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the *FTOS 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 46, 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

deny tcp	Assign a filter to deny TCP packets.
deny udp	Assign a filter to deny UDP packets.
ip access-list extended	Create an extended ACL.

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

<i>destination-mac-address</i>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format.
<i>mac-address-mask</i>	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 <i>vlan-id</i>	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.
<i>ip-address</i>	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
opcode <i>code-number</i>	Enter the keyword opcode followed by the number of the ARP opcode. Range: 1 to 23.
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 *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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 7.4.1.0 Added **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 *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of flow-based monitoring only. See [Chapter 46, 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.

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 ether-type

E Configure an egress filter that drops specified types of Ethernet packets on egress ACL supported line cards (see your line card documentation).

Syntax **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 { destination-mac-address mac-address-mask | any } vlan vlan-id { source-mac-address mac-address-mask | any }** command.

Parameters

<i>protocol-type-number</i>	Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.
<i>destination-mac-address mac-address-mask</i>	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, 1-2094 for ExaScale (can used IDs 1-4094) To filter all VLAN traffic specify VLAN 1.
<i>source-mac-address mac-address-mask</i>	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: 0-254 (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 <i>FTOS Configuration Guide</i> .

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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 7.4.1.0	Added 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 *FTOS 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 46, 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 syntax 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

<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>destination</i>	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
<i>message-type</i>	(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 10-14, "ICMP Message Type Keywords," in Access Control Lists (ACL)). 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** 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 *FTOS 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 Added **dscp** keyword.
 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 7.4.1.0 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 *FTOS 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 46, 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 10-14, "ICMP Message Type Keywords," in Access Control Lists \(ACL\)](#) lists the keywords displayed in the CLI help and their corresponding ICMP Message Type Name.

Table 10-14. ICMP Message Type Keywords

Keyword	ICMP Message Type Name
administratively-prohibited	Administratively prohibited
alternate-address	Alternate host address
conversion-error	Datagram conversion error
dod-host-prohibited	Host prohibited
dod-net-prohibited	Net prohibited
echo	Echo
echo-reply	Echo reply
general-parameter-problem	Parameter problem

Table 10-14. ICMP Message Type Keywords

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

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

<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>dscp</i>	Enter this keyword to deny a packet based on DSCP value. Range: 0-63
<i>bit</i>	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
<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"> • 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 <i>port</i> command parameter.
<i>port port</i>	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: <ul style="list-style-type: none"> • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>mask</i>	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 *FTOS 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 Added **dscp** keyword.
- 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 Added support for S-Series
- Version 7.5.1.0 Added support for C-Series
- Version 7.4.1.0 Added support for non-contiguous mask and added the **monitor** option. Deprecated **established** keyword.
- 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 *FTOS 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 46, 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:

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111110000000	7936	7999	64
8	0001111101000000	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

- [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 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

- source** Enter the IP address of the network or host from which the packets were sent.
- mask** Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- any** Enter the keyword **any** to specify that all routes are subject to the filter.
- host ip-address** Enter the keyword **host** followed by the IP address to specify a host IP address.
- dscp** Enter this keyword to deny a packet based on DSCP value.
Range: 0-63
- operator** (OPTIONAL) Enter one of the following logical operand:
 - **eq** = equal to
 - **neq** = not equal to
 - **gt** = greater than
 - **lt** = less than
 - **range** = inclusive range of ports

<i>port port</i>	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>mask</i>	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 <i>FTOS Configuration Guide</i> .
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	Added dscp keyword.
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	Added support for S-Series
Version 7.5.1.0	Added support 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 *FTOS 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 46, 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:

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	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

- [deny](#) Assign a deny filter for IP traffic.
- [deny tcp](#) Assign a deny filter for TCP traffic.

ip access-list extended

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

Syntax **ip access-list extended** *access-list-name*

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

Parameters

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

Defaults

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

Command Modes

CONFIGURATION

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 6.2.1.1	Introduced on E-Series

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	Rule#	Data	Mask	From	To	#Covered
	1	0000000000000000	1111110000000000	0	1023	1024
	Total Ports: 1024					

Related Commands		
	ip access-list standard	Configure a standard IP access list.
	show config	Display 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] [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

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.
ip-protocol-number	Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header.
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.
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 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 <i>FTOS Configuration Guide</i> .
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	<p>The order option is relevant in the context of the Policy QoS feature only. See the “Quality of Service” chapter of the <i>FTOS Configuration Guide</i> for more information.</p> <p>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.</p> <p>The C-Series and S-Series cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.</p> <p>The monitor option is relevant in the context of flow-based monitoring only. See the Chapter 46, Port Monitoring.</p> <p> Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.</p>	
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

E

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	<i>destination-mac-address</i>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format.
	<i>mac-address-mask</i>	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 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 <i>vlan-id</i>	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.
	<i>ip-address</i>	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
	opcode <i>code-number</i>	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 <i>FTOS Configuration Guide</i> .
	fragments	Enter the keyword fragments to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version 8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	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 *FTOS 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 46, 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

<i>protocol-type-number</i>	Enter a number from 600 to FFF as the specific Ethernet type traffic to drop.
<i>destination-mac-address</i>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format.
<i>mac-address-mask</i>	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 <i>vlan-id</i>	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.
<i>source-mac-address</i>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format.
<i>mac-address-mask</i>	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 *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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 7.4.1.0 Added **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 *FTOS 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 46, 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

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

<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>dscp</i>	Enter this keyword to deny a packet based on DSCP value. Range: 0-63
<i>message-type</i>	(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 10-14, "ICMP Message Type Keywords," in Access Control Lists (ACL)). 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

Version 8.3.1.0	Added dscp keyword.
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 7.4.1.0	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 *FTOS 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 46, 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

<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>bit</i>	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
<i>dscp</i>	Enter this keyword to deny a packet based on DSCP value. Range: 0-63
<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none">• 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 <i>port</i> parameter.)

<i>port port</i>	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
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>mask</i>	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 <i>FTOS Configuration Guide</i> .
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	Added dscp keyword.
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	Added support for S-Series
Version 7.5.1.0	Added support for C-Series
Version 7.4.1.0	Added support for non-contiguous mask and added the monitor option. Deprecated established keyword.
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 FTOS 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 46, 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:

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111110000000	7936	7999	64
8	0001111101000000	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

- [ip access-list extended](#) Create an extended ACL.
- [permit](#) Assign a permit filter for IP 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 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

- source* Enter the IP address of the network or host from which the packets were sent.
- mask* Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

any	Enter the keyword any to specify that all routes are subject to the filter.
host ip-address	Enter the keyword host followed by the IP address to specify a host IP address.
dscp	Enter this keyword to deny a packet based on DSCP value. Range: 0-63
operator	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"> • 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 <i>port</i> parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword count to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.
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 <i>FTOS Configuration Guide</i> .
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	Added dscp keyword.
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	Added support for S-Series
Version 7.5.1.0	Added support 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 *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See [Chapter 46, 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 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:

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111110000000	7936	7999	64
8	0001111101000000	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

- [ip access-list extended](#) Configure an extended ACL.
- [permit](#) Assign a permit filter for IP packets.
- [permit tcp](#) Assign a permit filter for TCP packets.

resequence access-list



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

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

Parameters	ipv4 mac	Enter the keyword ipv4 , or mac to identify the access list type to resequence.
	<i>access-list-name</i>	Enter the name of a configured IP access list, up to 140 characters.
	<i>StartingSeqNum</i>	Enter the starting sequence number to resequence. Range: 0 - 4294967290
	<i>Step-to-Increment</i>	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 8.1.1.0	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	Added support for S-Series
	Version 7.5.1.0	Added support for C-Series
	Version 7.4.1.0	Introduced for E-Series
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	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	<i>prefix-list-name</i>	Enter the name of configured prefix list, up to 140 characters long.
	<i>StartingSeqNum</i>	Enter the starting sequence number to resequence. Range: 0 – 65535
	<i>Step-to-Increment</i>	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 8.1.1.0	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	Added support for S-Series
Version 7.5.1.0	Added support for C-Series
Version 7.4.1.0	Introduced for E-Series

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

[resequence 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

<i>sequence-number</i>	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.
<i>destination-mac-address mac-address-mask</i>	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 <i>vlan-id</i>	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.
<i>ip-address</i>	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
opcode <i>code-number</i>	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 *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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 7.4.1.0	Added monitor option
Version 6.5.10	Expanded to include the optional QoS order priority for the ACL entry.

Usage Information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See [Chapter 46, 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

- E** 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	<i>sequence-number</i>	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.
	<i>protocol-type-number</i>	Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.
	<i>destination-mac-address</i>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format.
	<i>mac-address-mask</i>	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 <i>vlan-id</i>	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.
	<i>source-mac-address</i>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format.
	<i>mac-address-mask</i>	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 <i>FTOS Configuration Guide</i> .
Defaults	Not configured.	

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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 7.4.1.0	Added monitor option
Version 6.5.10	Expanded to include the optional QoS order priority for the ACL entry.

Usage Information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See [Chapter 46, 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 filters to interfaces in Layer 2 mode.

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

<i>sequence-number</i>	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.
<i>ip-protocol-number</i>	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
icmp	Enter the keyword icmp to configure an ICMP access list filter.
ip	Enter the keyword ip to configure a generic IP access list. The keyword ip specifies that the access list will permit all IP protocols.
tcp	Enter the keyword tcp to configure a TCP access list filter.

udp	Enter the keyword udp to configure a UDP access list filter.
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>operator</i>	(OPTIONAL) Enter one of the following logical operands: <ul style="list-style-type: none"> • 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 <i>port</i> parameter.)
<i>port port</i>	(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: <ul style="list-style-type: none"> • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>message-type</i>	(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 10-14). 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 DSCP values.
order	(OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the order keyword is not used, the ACLs have the lowest order by default (255).
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 <i>FTOS Configuration Guide</i> .
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	Added support for S-Series
Version 7.5.1.0	Added support for C-Series
Version 7.4.1.0	Added support for non-contiguous mask and added the monitor option. Deprecated established keyword
Version 6.5.10	Expanded to include the optional QoS order priority for the ACL entry.

Usage Information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See [Chapter 46, 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

- | | |
|------------------------|--|
| deny | Configure a filter to drop packets. |
| permit | Configure a filter to forward packets. |

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.

 and  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

C **E** **S** Clear counters for all or a specific MAC ACL.

Syntax **clear counters mac access-group** [*mac-list-name*]

Parameters *mac-list-name* (OPTIONAL) Enter the name of a configured MAC access list.

Command Modes EXEC Privilege

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

mac access-group

C **E** **S** Apply a MAC ACL to traffic entering or exiting an interface.

Syntax **mac access-group** *access-list-name* { **in** [**vlan** *vlan-range*] | **out** }

Parameters

<i>access-list-name</i>	Enter the name of a configured MAC access list, up to 140 characters.
vlan <i>vlan-range</i>	(OPTIONAL) Enter the keyword vlan followed a range of VLANs. Note that this option is available only with the in keyword option. Range: 1 to 4094, 1-2094 for ExaScale (can use IDs 1-4094)
in	Enter the keyword in to configure the ACL to filter incoming traffic.
out	Enter the keyword out to configure the ACL to filter outgoing traffic. Not available on S-Series.

Defaults No default behavior or configuration

Command Modes INTERFACE

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

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

mac access-list standard	Configure a standard MAC ACL.
mac access-list extended	Configure an extended MAC ACL.

show mac access-lists

C **E** **S**

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: 1-128
E-Series Range: 1 to 255 for TeraScale and 1 - 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.

in | out

Identify whether ACL is applied on ingress or egress side.

Command Modes EXEC Privilege

Command History

Version 8.4.1.0 Introduced

show mac accounting access-list

C **E** **S**

Display MAC access list configurations and counters (if configured).

Syntax `show mac accounting access-list 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: 1-128
E-Series Range: 1 to 255 for TeraScale and 1 - 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.

in | out

Identify whether ACL is applied ay Ingress (in) or egress (out) side.

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.
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#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

[show mac accounting destination](#)

Display destination counters for Layer 2 traffic (available on physical interfaces only).

Standard MAC ACL Commands

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

 and  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

any	Enter the keyword any to specify that all traffic is subject to the filter.
<i>mac-source-address</i>	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<i>mac-source-address-mask</i>	(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 <i>FTOS Configuration Guide</i> .

Defaults Not enabled.

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
Version 7.4.1.0	Added monitor option
pre-Version 6.1.1.0	Introduced for E-Series



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

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

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 MAC address filter to pass packets.
seq	Configure a MAC address filter with a specified sequence number.

mac access-list standard



Name a new or existing MAC access control list (MAC ACL) and enter the MAC ACCESS LIST mode to configure a standard MAC ACL. See [Commands Common to all ACL Types](#) and [Common MAC Access List Commands](#).

Syntax

mac access-list standard *mac-list-name*

Parameters

<i>mac-list-name</i>	Enter a text string as the name of the standard MAC access list (140 character maximum).
----------------------	--

Defaults	Not configured	
Command Modes	CONFIGURATION	
Command History	Version 8.1.1.0	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	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.	
Example	<pre>FTOS (conf)#mac-access-list access-list standard TestMAC FTOS (config-std-macl)#? deny Specify packets to reject description List description exit Exit from access-list configuration mode no Negate a command or set its defaults permit Specify packets to forward remark Specify access-list entry remark seq Sequence numbers show Show Standard ACL configuration</pre>	

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	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword count to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword byte to count bytes processed by the filter.

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 *FTOS 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
pre-Version 6.1.1.0	Introduced for E-Series



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

deny Configure a MAC ACL filter to drop packets.

seq Configure a MAC ACL filter with a specified sequence number.

seq



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

Syntax

seq *sequence-number* {**deny** | **permit**} {**any** | *mac-source-address* [*mac-source-address-mask*]} [**count** [**byte**]] [**log**] [**monitor**]

Parameters

<i>sequence-number</i>	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.
<i>mac-source-address</i>	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<i>mac-source-address-mask</i>	(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 *FTOS 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
Version 7.4.1.0	Added monitor option
pre-Version 6.1.1.0	Introduced for E-Series



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, the 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

deny	Configure a filter to drop packets.
permit	Configure a filter to forward packets.

Extended MAC ACL Commands

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

and 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**] [**order**] [**monitor**]] [**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 | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask}** command.

Parameters

any	Enter the keyword any to drop all packets.
host mac-address	Enter the keyword host followed by a MAC address to drop 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 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: <ul style="list-style-type: none"> • 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. To count specific packet types, enter one of the following keywords: <ul style="list-style-type: none"> • bytes: Enter the keyword bytes to count bytes processed by the filter. • order: Enter the keyword order to set the QoS order of priority. Range: 0-254 • monitor: Enter the keyword monitor to monitor packets.
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 <i>FTOS Configuration Guide</i> .

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-EXTENDED

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

Version 7.4.1.0 Added **monitor** option
pre-Version 6.1.1.0 Introduced for E-Series



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

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

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

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

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

```
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)#remark 25 IPv6
FTOS(config-ext-macl)#seq 30 permit any any ev2 eq 86dd count bytes
FTOS(config-ext-macl)#seq 40 permit any any 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

[mac access-list standard](#) Configure a standard MAC access list.

[show mac accounting access-list](#) Display MAC access list configurations and counters (if configured).

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 *FTOS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-EXTENDED

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
Version 7.4.1.0	Added monitor option
pre-Version 6.1.1.0	Introduced for E-Series



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, the 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

deny	Configure a filter to drop traffic based on the MAC address.
seq	Configure a filter with specific sequence numbers.

seq

C **E** **S** 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

<i>sequence-number</i>	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.
<i>mac-source-address</i>	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.
<i>mac-source-address-mask</i>	Specify which bits in the MAC address must be matched.

<i>mac-destination-address</i>	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
<i>mac-destination-address-mask</i>	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.
<i>ethertype operator</i>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: <ul style="list-style-type: none"> • 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 <i>FTOS Configuration Guide</i> .

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
	Version 7.4.1.0	Added monitor option
	pre-Version 6.1.1.0	Introduced for E-Series



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, the 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

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

C **E** **S** Reset the number of times traffic met the conditions (“hit” counters) of the configured prefix lists.

Syntax `clear ip prefix-list [prefix-name]`

Parameters *prefix-name* (OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.

Command Modes EXEC Privilege

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

Default Clears “hit” counters for all prefix lists unless a prefix list is specified.

Related Commands [ip prefix-list](#) Configure a prefix list.

deny

C **E** **S** Configure a filter to drop packets meeting the criteria specified.

Syntax `deny ip-prefix [ge min-prefix-length] [le max-prefix-length]`

Parameters

<i>ip-prefix</i>	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.
<i>ge min-prefix-length</i>	(OPTIONAL) Enter the keyword ge followed by the minimum prefix length, which is a number from zero (0) to 32.
<i>le max-prefix-length</i>	(OPTIONAL) Enter the keyword le followed by the maximum prefix length, which is a number from zero (0) to 32.

Defaults Not configured.

Command Modes PREFIX-LIST

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 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	permit	Configure a filter to pass packets.
	seq	Configure a drop or permit filter with a specified sequence number.

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 50, Router Information Protocol \(RIP\)](#). For related OSPF commands supported on all three platforms, see [Chapter 40, 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

C E S

Configure a filter that passes packets meeting the criteria specified.

Syntax `permit ip-prefix [ge min-prefix-length] [le max-prefix-length]`

Parameters

ip-prefix Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.

ge min-prefix-length (OPTIONAL) Enter the keyword **ge** followed by the minimum prefix length, which is a number from zero (0) to 32.

le max-prefix-length (OPTIONAL) Enter the keyword **le** followed by the maximum prefix length, which is a number from zero (0) to 32.

Command Modes PREFIX-LIST

Command History

Version 8.1.1.0 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

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.

seq

C E S

Assign a sequence number to a deny or permit filter in a prefix list while configuring the filter.

Syntax `seq sequence-number {deny | permit} {any} | [ip-prefix /nn {ge min-prefix-length} {le max-prefix-length}] | [bitmask number]`

Parameters

sequence-number Enter a number.
Range: 1 to 65534.

deny Enter the keyword **deny** to configure a filter to drop packets meeting this condition.

permit Enter the keyword **permit** to configure a filter to forward packets meeting this 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

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
Version 6.3.1.0	Added bit mask option

Usage Information 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.
permit	Configure a filter to pass packets.

show config

C **E** **S** Display the current PREFIX-LIST configurations.

Syntax **show config**

Command Modes PREFIX-LIST

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

```
FTOS(conf-nprefixl)#show config
!
ip prefix-list snickers
FTOS(conf-nprefixl)#
```

show ip prefix-list detail

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

show ip prefix-list summary

C **E** **S** Display a summary of the configured prefix lists.

Syntax `show ip prefix-list summary [prefix-name]`

Parameters *prefix-name* (OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters long.

Command Modes EXEC
EXEC Privilege

Command History	Version 8.1.1.0	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#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  
FROS#
```


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 *sequence-number* (OPTIONAL) Enter the route map sequence number.
Range: 1 - 65535
Default: no sequence number

Defaults Not Configured

Command Modes ROUTE-MAP

Command History

Version 8.1.1.0	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	Introduced

Usage Information 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 pre-pended.

Related Commands	set community	Specify a COMMUNITY attribute
	set as-path	Configure a filter to modify the AS path

description

C **E** **S** Add a description to this route map.

Syntax `description { description }`

Parameters *description* Enter a description to identify the route map (80 characters maximum).

Defaults No default behavior or values

Command Modes ROUTE-MAP

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 7.7.1.0	Introduced

Related Commands [route-map](#) Enable a route map

match as-path

C **E** **S** 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

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 [set as-path](#) Add information to the BGP AS_PATH attribute.

match community

C **E** **S** Configure a filter to match routes that have a certain COMMUNITY attribute in their BGP path.

Syntax `match community community-list-name [exact]`

Parameters

<i>community-list-name</i>	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

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 an Community Access list.
set community	Specify a COMMUNITY attribute.
neighbor send-community	Send COMMUNITY attribute to peer or peer group.

match interface

C **E** **S** 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

<i>interface</i>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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 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 used IDs 1-4094).
------------------	--

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 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.
	match tag	Redistribute routes that match a specific tag.

match ip address

C **E** **S** Configure a filter to match routes based on IP addresses specified in an prefix 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

C **E** **S**

Configure a filter to match based on the next-hop IP addresses specified in an IP access list or IP prefix list.

Syntax `match ip next-hop prefix-list prefix-list-name`

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

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 8.1.1.0	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 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 ip route-source

C **E** **S**

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 prefix-list prefix-list-name`

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 8.1.1.0	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 address	Redistribute routes that match an IP address.
	match ip next-hop	Redistribute routes that match the next-hop IP address.
	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

C **E** **S** Configure a filter to match on a specified value.

Syntax `match metric metric-value`

Parameters `metric-value` Enter a value to match.
Range: zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

Version 8.1.1.0	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

C **E** **S** Configure a filter to match routes based on the value found in the BGP path ORIGIN attribute.

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

C **E** **S** 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

C **E** **S** Configure a filter to redistribute only routes that match a specified tag value.

Syntax `match tag tag-value`

Parameters	<i>tag-value</i>	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
	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 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	<i>map-name</i>	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.
	<i>sequence-number</i>	(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

C **E** **S**

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 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 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

C **E** **S**

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
	Version 7.5.1.0	Support added for C-Series
	pre-Version 6.1.1.0	Introduced for E-Series

Related Commands	set level	Specify the OSPF area for route redistribution.
	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 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	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 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

<i>community-number</i>	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 (0xFFFFFFFF03) 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 (0xFFFFFFFF02) 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 (0xFFFFFFFF01) 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 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

C **E** **S**

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 redistributed 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

C **E** **S**

Configure a filter to set the BGP LOCAL_PREF attribute for routers within the local autonomous system.

Syntax `set local-preference value`

Parameters

<i>value</i>	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 [bgp default local-preference](#) Change default LOCAL_PREF attribute for all routes.

set metric

C **E** **S**

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.
<i>metric-value</i>	Enter a number as the new metric value. 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-type	Specify the route type assigned to redistributed routes.
set tag	Specify the tag assigned to redistributed routes.

set metric-type

C **E** **S**

Configure a filter to assign a new route type for routes redistributed to OSPF.

Syntax **set metric-type** {**internal** | **external** | **type-1** | **type-2**}

Parameters

internal	Enter the keyword internal to assign the Interior Gateway Protocol metric of the next hop as the route's BGP MULTI_EXIT_DES (MED) value.
external	Enter the keyword external to assign the IS-IS external metric.
type-1	Enter the keyword type-1 to assign the OSPF Type 1 metric.
type-2	Enter the keyword type-2 to assign the OSPF Type 2 metric.

Defaults Not configured.

Command Modes	ROUTE-MAP	
Command History	Version 8.3.1.0	Implemented internal keyword
	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 tag	Specify the tag assigned to redistributed routes.

set next-hop

C **E** **S** 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

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 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

C **E** **S**

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

C **E** **S**

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

C **E** **S**

Configure a filter to add a non-RFC compliant attribute to the BGP route to assist with route selection.

Syntax `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

C **E** **S**

Display the current route map configuration.

Syntax `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

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

show route-map

C **E** **S** Display the current route map configurations.

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

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

Command Modes EXEC
EXEC Privilege

Command History

Version 8.1.1.0	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#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:

E

The following commands configure AS-Path ACLs.

- [deny](#)
- [ip as-path access-list](#)
- [permit](#)
- [show config](#)
- [show ip as-path-access-lists](#)

deny

- E** 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. 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

Usage Information The regular expression must match part of the ASCII-text in the AS-PATH attribute of the BGP route.

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 6.1.1.0	Introduced for E-Series

ip as-path access-list

- E** 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

```
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	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
Related Commands	match as-path	Match on routes contain a specific AS-PATH.
	neighbor filter-list	Configure filter based on AS-PATH information.

permit

E 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

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 6.1.1.0	Introduced for E-Series

show config

E 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

```
FTOS(config-as-path)#show config
!
ip as-path access-list snickers
deny .3
FTOS(config-as-path)#
```

show ip as-path-access-lists

E 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

```
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: **E**

The commands in this section are.

- [deny](#)
- [ip community-list](#)
- [permit](#)
- [show config](#)
- [show ip community-lists](#)

deny

E

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 (0xFFFFFFFF03) 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 (0xFFFFFFFF02) 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 (0xFFFFFFFF01) 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

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 6.1.1.0	Introduced for E-Series

ip community-list

E 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 *comm-list-name* Enter a text string as the name of the community-list, up to 140 characters.

Command Modes CONFIGURATION

Example
FTOS(conf)#ip community-list TestComList
FTOS(config-community-list)#

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

permit

E 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

<i>community-number</i>	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 (0xFFFFFFFF03) 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 (0xFFFFFFFF02) 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 (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

regex
regular-expression

Enter the keyword **regex** 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 (CNTRL+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

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 6.1.1.0	Introduced for E-Series

show config

E Display the non-default information in the current configuration.

Syntax **show config**

Command Mode COMMUNITY-LIST

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 6.1.1.0	Introduced for E-Series

Example

```
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

E 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

```
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. Refer to [Chapter 15, 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](#)

Refer to other VLAN commands in [Chapter 10, 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 [show acl-vlan-group](#) Display the ACL VLAN groups

description

E 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 [show acl-vlan-group](#) Display the ACL VLAN groups

ip access-group

E 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 [acl-vlan-group](#) Create an ACL VLAN Group and name

member vlan

E 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

E 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.

Example 1 (show acl-vlan group) The following example 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.

```
FTOS#show acl-vlan-group
Group Name                Egress IP Acl          Vlan Members
TestGroupSeventeenTwenty SpecialAccessOnlyExperts 100,200,300
```

```

CustomerNumberIdentifica AnyEmployeeCustomerEleve 2-10,99
HostGroup Group5 1,1000

FTOS#

```

Example 2
(show
acl-vlan-group
group name)

The following example shows the table style display when using the **show acl-vlan-group group-name** option. Note that the access list name is truncated.

```

FTOS#show acl-vlan-group TestGroupSeventeenTwenty
Group Name Egress IP Acl Vlan Members
TestGroupSeventeenTwenty SpecialAccessOnlyExperts 100,200,300

FTOS#

```

Example 3
(show
acl-vlan-group
detail)

The following example shows the line-by-line style display when using the **show acl-vlan-group detail** option. Note that no group or access list names are truncated

```

FTOS#show acl-vlan-group detail

Group Name :
  TestGroupSeventeenTwenty
Egress IP Acl :
  SpecialAccessOnlyExpertsAllowed
Vlan Members :
  100,200,300

Group Name :
  CustomerNumberIdentificationEleven
Egress IP Acl :
  AnyEmployeeCustomerElevenGrantedAccess
Vlan Members :
  2-10,99

Group Name :
  HostGroup
Egress IP Acl :
  Group5
Vlan Members :
  1,1000
FTOS#

```

show acl-vlan-group detail

- E** 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

```
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

E 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

```
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

E 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

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

Example

```
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 FTOS implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03 and supports BFD on all Layer 3 physical interfaces including VLAN interfaces and port-channels.

BFD is supported on the C-Series and E-Series, where indicated by the **C** and **E** characters under command headings.

BFD is supported on E-Series ExaScale **E****X** with FTOS 8.2.1.0 and later.

Commands

- [bfd disable](#)
- [bfd enable \(Configuration\)](#)
- [bfd enable \(Interface\)](#)
- [bfd interval](#)
- [bfd all-neighbors](#)
- [bfd neighbor](#)
- [bfd protocol-liveness](#)
- [clear bfd counters](#)
- [debug bfd](#)
- [ip route bfd](#)
- [isis bfd all-neighbors](#)
- [show bfd counters](#)
- [show bfd neighbors](#)
- [vrrp bfd](#)

bfd disable

C **E**

Disable all VRRP sessions in a VRRP group.

Syntax

`bfd disable`

Re-enable BFD using the command `no bfd disable`.

Defaults

BFD is disabled by default.

Command Modes

INTERFACE VRRP

Command History	Version 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

bfd enable (Configuration)

C **E** Enable BFD on all interfaces.

Syntax `bfd enable`
 Disable BFD using the `no bfd enable` command.

Defaults BFD is disabled by default.

Command Modes CONFIGURATION

Command History	Version 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

bfd enable (Interface)

C **E** Enable BFD on an interface.

Syntax `bfd enable`

Defaults BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.

Command Modes INTERFACE

Command History	Version 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

bfd interval

C **E** 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

<code>interval <i>milliseconds</i></code>	Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range:50-1000 Default:100
---	--

<i>min_rx milliseconds</i>	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
<i>multiplier value</i>	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
<i>role [active passive]</i>	Enter the role that the local system assumes: <ul style="list-style-type: none"> 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 Refer to 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 7.4.1.0	Introduced on E-Series

Example
FTOS(conf-if-gi-0/3)#bfd interval 250 min_rx 300 multiplier 4 role passive
FTOS(conf-if-gi-0/3)#

bfd all-neighbors

C **E** Establish BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.

Syntax bfd all-neighbors [interval *interval* min_rx *min_rx* multiplier *value* role {active | passive}]

Parameters	<i>interval milliseconds</i>	(OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range:50-1000 Default:100
	<i>min_rx milliseconds</i>	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
	<i>multiplier value</i>	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 Refer to Parameters

Command Modes ROUTER OSPF
ROUTER ISIS (Not available on C-Series)

Command History

Version 8.2.1.0	OSPF and ISIS BFD introduced on E-Series ExaScale
Version 7.6.1.0	OSPF BFD introduced on C-Series
Version 7.5.1.0	ISIS BFD introduced on E-Series
Version 7.4.1.0	OSPF BFD introduced on E-Series

Usage Information Any timer values specified in INTERFACE mode using the command [isis bfd all-neighbors](#) override timer values specified in this command. Likewise, using the *no* form of this command will not disable BFD on an interface if BFD is explicitly enabled in INTERFACE mode using the command [isis bfd all-neighbors](#).

Related Commands [show bfd neighbors](#) Display BFD neighbor information on all interfaces or a specified interface.

bfd neighbor

  Establish a BFD session with a neighbor.

Syntax `bfd neighbor ip-address`

Parameters *ip-address* Enter the IP address of the neighbor in dotted decimal format (A.B.C.D).

Defaults None

Command Modes INTERFACE

Command History

Version 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

E 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

C **E** 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 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 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 8.2.1.0 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.

Syntax debug bfd {detail | event / packet} {all | *interface*} [mode] [count *number*]

Parameters

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 the 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.
<i>interface</i>	Enter one of the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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. For a port-channel interface, enter the keyword port-channel followed by a number: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 E-Series Range: 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).
mode	(OPTIONAL) Enter one of the following debug transmission modes: <ul style="list-style-type: none"> 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 <i>number</i>	(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

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

Usage Information

Since BFD can potentially transmit 20 packets per interface, debugging information should be restricted.

ip route bfd

C **E** 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 <i>milliseconds</i>	(OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range:50-1000 Default:100
	min_rx <i>milliseconds</i>	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 <i>value</i>	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: <ul style="list-style-type: none">• 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 Refer to 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

E 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 <i>milliseconds</i>	(OPTIONAL) Enter this keyword to specify non-default BFD session parameters beginning with the transmission interval. Range:50-1000 Default:100

min_rx <i>milliseconds</i>	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 <i>value</i>	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: <ul style="list-style-type: none"> • 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 Refer to 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 `disable` to disable BFD on a specific interface while BFD is configured in from CONFIGURATION mode.

show bfd counters

C **E** Display BFD counter information.

Syntax `show bfd counters [isis | ospf | vrrp | static-route] [interface]`

Parameters

<i>interface</i>	Enter one of the following keywords and slot/port or number information: <ul style="list-style-type: none"> • For a 1-Gigabit Ethernet interface, enter the keyword <code>gigabitethernet</code> followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code> followed by the slot/port information. • For a SONET interface, enter the keyword <code>sonet</code> followed by the slot/port information. • For a port-channel interface, enter the keyword <code>port-channel</code> followed by a number: C-Series and S-Series Range: 1-128 E-Series Range: 1 to 255 for TeraScale, and 1 to 512 for ExaScale • For VLAN interfaces, enter the keyword <code>vlan</code> followed by a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1-2730 (VLAN IDs can be 0-4093).
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.

static-route (OPTIONAL) Enter this keyword to display counter information for BFD sessions established with ISIS neighbors.

vrpp (OPTIONAL) Enter this keyword to display counter information for BFD sessions established with VRRP neighbors.

Defaults None

Command Modes EXEC
EXEC Privilege

Command History

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 BFD for VLAN and port-channel interfaces, ISIS, and VRRP on E-Series
Version 7.4.1.0	Introduced BFD on physical ports, static routes, and OSPF on E-Series

Example FTOS#show bfd counters

```

Interface                Tx          Rx
GigabitEthernet 1/3      522         625
FTOS#

```

show bfd neighbors

C **E** Display BFD neighbor information on all interfaces or a specified interface.

Syntax show bfd neighbors *interface* [detail]

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 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 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 8.2.1.0 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 1

```
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 2 (detail)

```
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[bfd neighbor](#)

Establish a BFD session with a neighbor.

[bfd all-neighbors](#)

Establish BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.

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

- all-neighbors** Establish BFD sessions with all BFD neighbors on an interface.
- neighbor *ip-address*** Enter the IP address of the BFD neighbor.
- 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** 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 Refer to 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.

FTOS version	Platform support	
8.1.1.0	E-Series ExaScale	
7.8.1.0	S-Series	
7.7.1.0.	C-Series	
pre-7.7.1.0	E-Series TeraScale	

For detailed information on configuring BGP, refer to the BGP chapter in the *FTOS Configuration Guide*.

This chapter contains the following sections:

- [BGPv4 Commands](#)
- [MBGP Commands](#)
- [BGP Extended Communities \(RFC 4360\)](#)

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: FTOS Version 7.7.1 supports 2-Byte (16-bit) and 4-Byte (32-bit) format for Autonomous System Numbers (ASNs), where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295.

Note: FTOS Version 8.3.1.0 supports Dotted format as well as the Traditional Plain format for AS Numbers. The dot format is displayed when using the **show ip bgp** commands. To determine the comparable dot format for an ASN from a traditional format, use **ASN/65536**. **ASN%65536**.

For more information about using the 2 or 4-Byte format, refer to the *FTOS Configuration Guide*.

The following commands enable you to configure and enable BGP.

- [address-family](#)
- [aggregate-address](#)
- [bgp add-path](#)
- [bgp always-compare-med](#)

- bgp asnotation
- bgp bestpath as-path ignore
- bgp bestpath 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 add-path
- neighbor advertisement-interval
- neighbor advertisement-start
- neighbor allowas-in
- neighbor default-originate
- neighbor description
- neighbor distribute-list

- neighbor ebgp-multihop
- neighbor fall-over
- neighbor 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
- show ip bgp paths community
- show ip bgp peer-group
- show ip bgp regexp

- [show ip bgp summary](#)
- [show running-config bgp](#)
- [timers bgp](#)

address-family

C **E** **S** Enable the IPv4 multicast or the IPv6 address family.

Syntax `address-family [ipv4 multicast| ipv6unicast]`

Parameters

ipv4 multicast	Enter BGPv4 multicast mode.
ipv6 unicast	Enter BGPv6 mode.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 6.5.1.0	Introduced
-----------------	------------

aggregate-address

C **E** **S** 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

ROUTER BGP ADDRESS FAMILY IPv6

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

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.

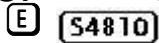
The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the **neighbor distribute-list** command.

In the **show ip bgp** command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

bgp add-path



Allow the advertisement of multiple paths for the same address prefix without the new paths replacing any previous ones.

Syntax

bgp add-path {[send | both] path-count *number* | receive}

Parameters

send	Enter this keyword to indicate that the system will send multiple paths to peers.
receive	Enter this keyword to indicate that the system will accept multiple paths from peers.
both	Enter this keyword to indicate that the system will send and accept multiple paths from peers.
path-count <i>number</i>	Enter the number of paths to advertise. Range: 2-64

Defaults

Disabled

Command Modes

ROUTER BGP

Usage Information

The add-path feature is advertised to BGP neighbors through a capability advertisement. BGP Sessions should be manually flapped for any change in the 'add-path' configuration. The BGP neighbor router should also support Add-Path capability in order to receive multiple paths for the particular address-family.

Command History

Version 8.4.1.5	Introduced on ExaScale.
-----------------	-------------------------

bgp always-compare-med

C **E** **S**

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

C **E** **S**

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 **asnotation**, it is reflected in the running-configuration. If you change the notation type, the running-config is updated dynamically and the new notation is shown.

Related Commands

[bgp four-octet-as-support](#) Enable 4-byte support for the BGP process

Command History

Version 8.3.1.0	Introduced Dynamic Application of AS Notation changes
Version 8.2.1.0	Introduced

Example

```
FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#bgp asnotation asdot
FTOS(conf-router_bgp)#ex
FTOS(conf)#do show run | grep bgp

router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot
```

```
FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#bgp asnotation asdot+
FTOS(conf-router_bgp)#ex
```

```
FTOS(conf)#do show run | grep bgp
router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot+
```

```
FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#bgp asnotation asplain
FTOS(conf-router_bgp)#ex
FTOS(conf)#do show run |grep bgp
router bgp 1
  bgp four-octet-as-support
  bgp asnotation asplain
```

```
FTOS(conf)#
```

bgp bestpath as-path ignore

C **E** **S** Ignore the AS PATH in BGP best path calculations.

Syntax **bgp bestpath as-path ignore**

To return to the default, enter **no bgp bestpath as-path ignore**.

Defaults Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes ROUTER BGP

Usage Information If you enable this command, use the [clear ip bgp ipv4 unicast soft *](#) command to recompute the best path.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

bgp bestpath med confed

C **E** **S** 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 <code>clear ip bgp ipv4 unicast soft *</code> command to recompute the best path.	
Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

bgp bestpath med missing-as-best

C **E** **S** During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

Syntax `bgp bestpath med missing-as-best`

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults Disabled

Command Modes ROUTER BGP

Usage Information The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.

Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series
	Version 6.3.1.0	Introduced

bgp bestpath router-id ignore

C **E** **S** 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.

Command History	Version 8.3.1.0	Introduced
------------------------	-----------------	------------

bgp client-to-client reflection

C **E** **S** 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

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.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

bgp cluster-id

C **E** **S** 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

<i>ip-address</i>	Enter an IP address as the route reflector cluster ID.
<i>number</i>	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

[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 support on C-Series
Added support for 4-Byte format

bgp confederation peers



Specify the Autonomous Systems (ASs) that belong to the BGP confederation.

Syntax `bgp confederation peers as-number [...as-number]`

To return to the default, enter **no bgp confederation peers**.

Parameters

as-number Enter the AS number.
Range: 0-65535 (2-Byte) *or*
1-4294967295 (4-Byte) *or*
0.1-65535.65535 (Dotted format)

...as-number (OPTIONAL) Enter up to 16 confederation numbers.
Range: 0-65535 (2-Byte) *or*
1-4294967295 (4-Byte) *or*
0.1-65535.65535 (Dotted format)

Defaults Not configured.

Command Modes 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

[bgp confederation identifier](#) Configure a confederation ID.
[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 support on C-Series
Added support for 4-byte format

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

<i>half-life</i>	(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
<i>reuse</i>	(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
<i>suppress</i>	(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
<i>max-suppress-time</i>	(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 <i>map-name</i>	(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

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

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

value Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred.
Range: 0 to 4294967295
Default: 100

Defaults 100

Command Modes ROUTER BGP

Usage Information

The `bgp default local-preference` command setting is applied by all routers within the AS. To set the local preference for a specific route, use the `set 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
Version 7.7.1.0 Introduced support for C-Series
Version 7.4.1.0 Introduced

bgp fast-external-fallover

C **E** **S** 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

C **E** **S** 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 *FTOS Configuration Guide*.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced command
	Introduced support on C-Series

bgp graceful-restart

C **E** **S**

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

Version 7.8.1.0 Introduced support on S-Series

Version 7.7.1.0 Introduced support on C-Series

bgp log-neighbor-changes

C **E** **S**

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.

Related Commands

[show logging](#) View logging settings and system messages logged to the system.

Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

bgp non-deterministic-med

C **E** **S** 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	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

bgp recursive-bgp-next-hop

C **E** **S** 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 [clear ip bgp ipv4 unicast soft](#) Clear and reapply policies for IPv4 routes without resetting the TCP connection.

Command History

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

bgp regex-eval-optz-disable

C **E** **S** 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 [show ip protocols](#) View information on all routing protocols enabled and active on the E-Series.

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

Example

```
FTOS(conf-router_bgp)#no bgp regex-eval-optz-disable
FTOS(conf-router_bgp)#do show ip protocols
Routing Protocol is "ospf 22222"
  Router ID is 2.2.2.2
  Area           Routing for Networks
  51             10.10.10.0/00

Routing Protocol is "bgp 1"
  Cluster Id is set to 10.10.10.0
  Router Id is set to 10.10.10.0
  Fast-external-fallover enabled
  Regular expression evaluation optimization enabled
```

```

Capable of ROUTE_REFRESH
For Address Family IPv4 Unicast
  BGP table version is 0, main routing table version 0
  Distance: external 20 internal 200 local 200

FTOS(conf-router_bgp)#

```

bgp retain-ibgp-nexthop

C **E** **S**

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

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.

bgp router-id

C **E** **S**

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

<i>ip-address</i>	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.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

bgp soft-reconfig-backup

C **E** **S**

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

[clear ip bgp ipv4 unicast soft in](#) Activate inbound policies for IPv4 routes without resetting the BGP TCP session.

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

capture bgp-pdu neighbor

C **E** **S**

Enable capture of an IPv4 BGP neighbor packet.

Syntax **capture bgp-pdu neighbor ipv4-address direction { both | rx | tx }**

To disable capture of the IPv4 BGP neighbor packet, use the **no capture bgp-pdu neighbor ipv4-address** command.

Parameters

ipv4-address	Enter the IPv4 address of the target BGP neighbor.
direction { both rx tx }	Enter the keyword direction and a direction— either rx for inbound, tx for outbound, or both .

Defaults Not configured.

Command Modes EXEC Privilege

Related Commands

capture bgp-pdu max-buffer-size	Specify a size for the capture buffer.
show capture bgp-pdu neighbor	Display BGP packet capture information

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

capture bgp-pdu max-buffer-size

C **E** **S**

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

[capture bgp-pdu neighbor](#) Enable capture of an IPv4 BGP neighbor packet.
[capture bgp-pdu neighbor \(ipv6\)](#) Enable capture of an IPv6 BGP neighbor packet.
[show capture bgp-pdu neighbor](#) Display BGP packet capture information for an IPv6 address on the E-Series.

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

C **E** **S**

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)
- `ipv4-neighbor-addr | ipv6-neighbor-addr` Clear and reapply policies for a neighbor.
- `peer-group name` Clear and reapply policies for all BGP routers in the specified peer group.
- `ipv4 unicast` Clear and reapply policies for all IPv4 unicast routes.
- in** Reapply only inbound policies.
Note: If you enter **soft**, without an **in** or **out** option, both inbound and outbound policies are reset.
- out** Reapply only outbound policies.
Note: If you enter **soft**, without an **in** or **out** option, both inbound and outbound policies are reset.

Command Modes EXEC Privilege

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 peer-group

C **E** **S** 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	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

clear ip bgp dampening

C **E** **S** Clear information on route dampening and return suppressed route to active state.

Syntax `clear ip bgp dampening [ip-address mask]`

Parameters *ip-address mask* (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.

Command Modes EXEC Privilege

Usage Information After you enter this command, the software deletes history routes and returns suppressed routes to active state.

Command History	Version 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 [ip-address mask | filter-list as-path-name | regexp regular-expression]`

Parameters

- ip-address mask*** (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.
- filter-list as-path-name*** (OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH list.
- regexp regular-expression*** (OPTIONAL) Enter the keyword **regexp** followed by regular expressions. Use one or a combination of the following:
- `.` = (period) any single character (including a white space)
 - `*` = (asterisk) the sequences in a pattern (0 or more sequences)
 - `+` = (plus) the sequences in a pattern (1 or more sequences)
 - `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
 - `[]` = (brackets) a range of single-character patterns.
 - `()` = (parenthesis) groups a series of pattern elements to a single element
 - `{ }` = (braces) minimum and the maximum match count
 - `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
 - `$` = (dollar sign) the end of the output string.

Command Modes EXEC Privilege

Usage Information If you enter `clear ip bgp flap-statistics` without any parameters, all statistics are cleared.

Related Commands

<code>show debugging</code>	View enabled debugging operations.
<code>show ip bgp flap-statistics</code>	View BGP flap statistics.
<code>undebug all</code>	Disable all debugging operations.

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



Display all information on BGP, including BGP events, keepalives, notifications, and updates.

Syntax `debug ip bgp [ip-address | peer-group peer-group-name] [in | out]`

To disable all BGP debugging, enter **no debug ip bgp**.

Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	peer-group <i>peer-group-name</i>	Enter the keyword peer-group followed by the name of the peer group.
	in	(OPTIONAL) Enter the keyword in to view only information on inbound BGP routes.
	out	(OPTIONAL) Enter the keyword out to view only information on outbound BGP routes.

Command Modes EXEC Privilege

Usage Information To view information on both incoming and outgoing routes, do not include the **in** and **out** parameters in the debugging command. The **in** and **out** parameters cancel each other; for example, if you enter **debug ip bgp in** and then enter **debug ip bgp out**, you will not see information on the incoming routes.

Entering a [no debug ip bgp](#) command removes all configured debug commands for BGP.

Related Commands	debug ip bgp events	View information about BGP events.
	debug ip bgp keepalives	View information about BGP keepalives.
	debug ip bgp notifications	View information about BGP notifications.
	debug ip bgp updates	View information about BGP updates.
	show debugging	View enabled debugging operations.

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 dampening

C **E** **S** Display information on routes being dampened.

Syntax **debug ip bgp dampening [in | out]**

To disable debugging, enter **no debug ip bgp dampening**.

Parameters	in	(OPTIONAL) Enter the keyword in to view only inbound dampened routes.
	out	(OPTIONAL) Enter the keyword out to view only outbound dampened routes.

Command Modes EXEC Privilege

Usage Information Enter [no debug ip bgp](#) command to remove all configured debug commands for BGP.

Related Commands	show debugging	View enabled debugging operations.
	show ip bgp dampened-paths	View BGP dampened routes.

Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

debug ip bgp events

C **E** **S**

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 (OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
peer-group-name
in (OPTIONAL) Enter the keyword **in** to view only events on inbound BGP messages.
out (OPTIONAL) Enter the keyword **out** to view only events on outbound BGP messages.

Command Modes EXEC Privilege

Usage Information

Enter **no debug ip bgp** command to remove all configured debug commands for BGP.

Command History

Version 7.8.1.0 Introduced support on S-Series
 Version 7.7.1.0 Introduced support on C-Series

debug ip bgp keepalives

C **E** **S**

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 (OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
peer-group-name
in (OPTIONAL) Enter the keyword **in** to view only inbound keepalive messages.
out (OPTIONAL) Enter the keyword **out** to view only outbound keepalive messages.

Command Modes EXEC Privilege

Usage Information

Enter **no debug ip bgp** command to remove all configured debug commands for BGP.

Command History

Version 7.8.1.0 Introduced support on S-Series
 Version 7.7.1.0 Introduced support on C-Series

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 (OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
peer-group-name
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

Version 8.4.1.0 Introduced support for IPv4 multicast and IPv6 unicast 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 updates

C **E** **S** Enables you to view information about BGP updates.

Syntax `debug ip bgp updates [in | out | prefix-list prefix-list-name]`

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **updates** [**in** | **out**] command.

Parameters

- 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.
- prefix-list** (OPTIONAL) Enter the keyword **prefix-list** followed by the name of an established prefix list. If the prefix list is not configured, the default is *permit* (to allow all routes).
- prefix-list-name*
- 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 to disable or enable all routers within the peer group.

Command Modes EXEC Privilege

Usage Information Enter **no debug ip bgp** command to remove all configured debug commands for BGP.

Command History Version 7.7.1 Introduced support on C-Series

default-metric

C **E** **S** 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

- number* Enter a number as the metric to be assigned to routes from other protocols. Range: 1 to 4294967295.

Defaults 0

Command Modes ROUTER BGP

Usage Information The [default-metric](#) command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands	bgp always-compare-med	Enable comparison of all BGP MED attributes.
	redistribute	Redistribute routes from other routing protocols into BGP.

Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

description

C **E** **S** 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 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series
	pre-7.7.1.0	Introduced

Related Commands [router bgp](#) Enter ROUTER mode on the switch.

distance bgp

C **E** **S** 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	<i>external-distance</i>	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
	<i>internal-distance</i>	Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200
	<i>local-distance</i>	Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200

Defaults *external-distance* = 20; *internal-distance* = 200; *local-distance* = 200.

Command Modes ROUTER BGP



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

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

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

ebgp	Enter the keyword ebgp to enable multipath support for External BGP routes.
ibgp	Enter the keyword ibgp to enable multipath support for Internal BGP routes.
<i>number</i>	Enter a number as the maximum number of parallel paths. Range: 1 to 16 Default: 1

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.

For optimal configuration, the *number* variable should be set to the highest possible value. Dell Force10 recommends maintaining the default setting of 64.

Command History

Version 8.4.1.5	Modified range and default value.
Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

neighbor activate

C **E** **S**

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

Version 7.8.1.0 Introduced support on S-Series

Version 7.7.1.0 Introduced support on C-Series

neighbor add-path

E

S4810

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

Syntax `neighbor {ip-address | peer-group-name} add-path {[send | both] path-count number | receive}`

Parameters

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

peer-group-name Enter the name of the peer group.

send Enter this keyword to indicate that the system will send multiple paths to peers.

receive Enter this keyword to indicate that the system will accept multiple paths from peers.

both Enter this keyword to indicate that the system will send and accept multiple paths from peers.

path-count Enter the number of paths to advertise.
number Range: 2 to 64

Defaults none

Command Modes ROUTER BGP

Usage Information

The add-path feature is advertised to BGP neighbors through a capability advertisement. BGP Sessions should be manually flapped for any change in the 'add-path' configuration. The BGP neighbor router should also support Add-Path capability in order to receive multiple paths for the particular address-family.

If you enable 'bgp add-path' globally and you are also using 'neighbor add-path,' the neighbor-specific command will override the global configuration.

If you specify a BGP peer-group, all the members will inherit the characteristics configured with this command. If you also configure add-path for a particular member, the command will override peer-group configuration.

Related Commands	bgp add-path	Allow the advertisement of multiple paths for the same address prefix without the new paths implicitly replacing any previous ones.
Command History	Version 8.4.1.5	Introduced on ExaScale.

neighbor advertisement-interval

C **E** **S** 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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	<i>seconds</i>	Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

Defaults *seconds* = 5 seconds (internal peers); *seconds* = 30 seconds (external peers)

Command Modes ROUTER BGP

Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

neighbor advertisement-start

C **E** **S** 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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>seconds</i>	Enter a number as the time interval, in seconds, before BGP route updates are sent. Range: 0 to 3600 seconds.

Defaults	<i>none</i>	
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 allowas-in

C **E** **S** 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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	<i>number</i>	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 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced on C-Series and E-Series

neighbor default-originate

C **E** **S** 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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to set the default route of all routers in that peer group.
	route-map <i>map-name</i>	(OPTIONAL) Enter the keyword route-map followed by the name of a configured route map.

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

C **E** **S** 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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>text</i>	Enter a continuous text string up to 80 characters.

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

C **E** **S** 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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
	<i>prefix-list-name</i>	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

neighbor ebgp-multihop

C **E** **S** Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax **neighbor** { *ip-address* | *peer-group-name* } **ebgp-multihop** [*ttl*]

To disallow and disconnect connections, use the **no neighbor** { *ip-address* | *peer-group-name* } **ebgp-multihop** command.

Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>ttl</i>	(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

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.

Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

neighbor fall-over

E **C** **S** 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	<i>ipv4-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
	<i>as-path-name</i>	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 (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	
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 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

C **E** **S** 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**]

To return to the default, enter the **no bgp graceful-restart** command.

Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
	restart-time <i>seconds</i>	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 <i>seconds</i>	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

C **E** **S** Configure Internal BGP (IBGP) routers to accept *external* routes from neighbors with a local AS number in the AS number path

Syntax **neighbor** { *ip-address* | *peer-group-name* } **local-as** *as-number* [no-prepend]

To return to the default value, use the **no neighbor** { *ip-address* | *peer-group-name* } **local-as** command.

Parameters	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
	<i>as-number</i>	Enter the AS number to reset all neighbors belonging to that AS. Range: 0-65535 (2-Byte) <i>or</i> 1-4294967295 (4-Byte) <i>or</i> 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
		Introduced support on C-Series

neighbor maximum-prefix

C **E** **S** 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	<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>maximum</i>	Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
	<i>threshold</i>	(OPTIONAL) Enter a number to be used as a percentage of the <i>maximum</i> value. When the number of prefixes reaches this percentage of the <i>maximum</i> 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	<i>threshold</i> = 75	
Command Modes	ROUTER BGP	

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 summary command displays (prfxd) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the clear ip bgp ipv4 unicast soft command for the neighbor or the peer group to which the neighbor belongs or you enter neighbor shutdown and neighbor no shutdown commands.	
Related Commands	show ip bgp summary	Displays the current BGP configuration.
Command History	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

neighbor next-hop-self

C **E** **S** 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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	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.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

neighbor password

C **E** **S** Enable Message Digest 5 (MD5) authentication on the TCP connection between two neighbors.

Syntax **neighbor** { *ip-address* | *peer-group-name* } **password** [*encryption-type*] *password*

To delete a password, use the **no neighbor** { *ip-address* | *peer-group-name* } **password** command.

Parameters

<i>ip-address</i>	Enter the IP address of the router to be included in the peer group.
<i>peer-group-name</i>	Enter the name of a configured peer group.

	<i>encryption-type</i>	(OPTIONAL) Enter 7 as the encryption type for the <i>password</i> entered. 7 means that the password is encrypted and hidden.
	<i>password</i>	Enter a text string up to 80 characters long. The first character of the <i>password</i> must be a letter. You cannot use spaces in the password.
Defaults	Not configured.	
Command Modes	ROUTER BGP	
Usage Information	<p>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.</p> <p>Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.</p> <p>If you specify a BGP peer group by using the <i>peer-group-name</i> parameter, all the members of the peer group will inherit the characteristic configured with this command.</p> <p>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:</p> <p>%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address] :179 to [local router's IP address]:65524</p> <p>Also, if you configure different passwords on the two routers, the following message appears on the console:</p> <p>%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from [peer's IP address] : 11502 to [local router's IP address] :179</p>	
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)

C **E** **S** 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)

C **E** **S** 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.

Parameters *peer-group-name* Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information When a peer group is created, it is disabled (shut mode).

Related Commands [neighbor peer-group \(assigning peers\)](#) Assign routers to a peer group.

neighbor remote-as	Assign an indirectly connected AS to a neighbor or peer group.
neighbor shutdown	Disable a peer 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

neighbor peer-group passive

C **E** **S** 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 [match-af]`

To delete a passive peer-group, use the **no neighbor peer-group-name peer-group passive** command.

Parameters	<i>peer-group-name</i>	Enter a text string up to 16 characters long as the name of the peer group.
	match-af	(Optional) Enter the keyword match-af 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.

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.

Related Commands [neighbor soft-reconfiguration inbound](#) Assign a subnet to a dynamically-configured BGP neighbor.

Command History	Version 8.4.2.0	Added support for the match-af keyword
	Version 7.8.1.0	Introduced support on S-Series
	Version 7.7.1.0	Introduced support on C-Series

neighbor remote-as

C **E** **S** 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

<i>ip-address</i>	Enter the IP address of the neighbor to enter the remote AS in its routing table.
<i>peer-group-name</i>	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
<i>number</i>	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 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series Added 4-Byte support.

neighbor remove-private-as

C **E** **S** 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

<i>ip-address</i>	Enter the IP address of the neighbor to remove the private AS numbers.
<i>peer-group-name</i>	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

Usage Information

Applies to EBGp neighbors only.

You must configure your system to accept 4-Byte formats before entering a 4-Byte AS Number.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGp neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535 (2-Byte).

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series Added 4-Byte support.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group.
<i>map-name</i>	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.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

neighbor route-reflector-client

C **E** **S**

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	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

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

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

neighbor send-community

C **E** **S**

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

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	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

C **E** **S**

Disable a BGP neighbor or peer group.

Syntax **neighbor** { *ip-address* | *peer-group-name* } **shutdown**

To enable a disabled neighbor or peer group, use the **neighbor** { *ip-address* | *peer-group-name* } **no shutdown** command.

Parameters

ip-address Enter the IP address of the neighbor in dotted decimal format.
peer-group-name Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes ROUTER BGP

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The [neighbor shutdown](#) command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the [show ip bgp summary](#) command to confirm its status.

Related Commands

[show ip bgp summary](#) Displays the current BGP configuration.
[show ip bgp neighbors](#) Displays the current BGP neighbors.

Command History

Version 7.8.1.0 Introduced support on S-Series
 Version 7.7.1.0 Introduced support on C-Series

neighbor soft-reconfiguration inbound

C **E** **S**

Enable a BGP soft-reconfiguration and start storing inbound route updates.

Syntax **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
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

Version 8.4.1.0	Added support for IPv4 multicast and IPv4 unicast address families
Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series
Version 7.4.1.0	Introduced

neighbor subnet

C **E** **S** 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

<i>subnet-number</i>	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.
<i>mask</i>	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

C **E** **S** 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

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to set the timers for all routers within the peer group.
<i>keepalive</i>	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 History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

neighbor update-source

C **E** **S** 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

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to disable all routers within the peer group.
<i>interface</i>	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

neighbor weight

C **E** **S**

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

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to disable all routers within the peer group.
<i>weight</i>	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

C **E** **S**

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

<i>ip-address</i>	Enter an IP address in dotted decimal format of the network.
<i>mask</i>	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 (OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map.
map-name

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

Usage Information FTOS software resolves the network address configured by the [network](#) command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

Related Commands [redistribute](#) Redistribute routes into BGP.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

network backdoor

C **E** **S** 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

<i>ip-address</i>	Enter an IP address in dotted decimal format of the network.
<i>mask</i>	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).

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information Though FTOS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

redistribute



Redistribute routes into BGP.

Syntax `redistribute { connected | static } [route-map map-name]`

To disable redistribution, use the **no redistribution { **connected** | **static** }** 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

Usage Information

With FTOS version 8.3.1.0 and later, the redistribute command can be used to advertise the IGP cost as the MED on redistributed routes. When the route-map is set with metric-type internal and applied outbound to an EBGp peer/peer-group, the advertised routes corresponding to those peer/peer-group will have IGP cost set as MED.

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

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

redistribute isis

E 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

<i>WORD</i>	ISO routing area tag
level-1	(OPTIONAL) Enter the keyword level-1 to independently redistributed into Level 1 routes only.
level-1-2	(OPTIONAL) Enter the keyword level-1-2 to independently redistributed into Level 1 and Level 2 routes. This is the default.
level-2	(OPTIONAL) Enter the keyword level-2 to independently redistributed into Level 2 routes only
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword metric followed by the metric value used for the redistributed route. Use a metric value that is consistent with the destination protocol. Range: 0 to 16777215 Default: 0
route-map <i>map-name</i>	Enter the keyword route-map followed by the map name that 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 <i>map-name</i> , all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.

Defaults **level-1-2**

Command Modes ROUTER BGP

Example

```
FTOS(conf)#router bgp 1
FTOS(conf-router_bgp)#redistribute isis level-1 metric 44 route-map
rmap-is2bgp
FTOS(conf-router_bgp)#show running-config bgp
!
router bgp 1
redistribute isis level-1 metric 44 route-map rmap-is2bgp
```

Usage Information

With FTOS version 8.3.1.0 and later, the redistribute command can be used to advertise the IGP cost as the MED on redistributed routes. When the route-map is set with metric-type internal and applied outbound to an EBGp peer/peer-group, the advertised routes corresponding to those peer/peer-group will have IGP cost set as MED.

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

C **E** **S** 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	<i>process-id</i>	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 <i>map-name</i>	(OPTIONAL) Enter the keywords route-map followed by the name of a configured Route map.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information With FTOS version 8.3.1.0 and later, the redistribute command can be used to advertise the IGP cost as the MED on redistributed routes. When the route-map is set with metric-type internal and applied outbound to an EBGp peer/peer-group, the advertised routes corresponding to those peer/peer-group will have IGP cost set as MED.

When you enter `redistribute isis process-id` command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. This feature is not supported by an RFC.

Command History	Version 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

C **E** **S**

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

```
FTOS(conf)#router bgp 3
FTOS(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

Usage Information

At least one interface must be in Layer 3 mode for the router bgp command to be accepted. If no interfaces are enabled for Layer 3, an error message appears: **% Error: No router id configured.**

show capture bgp-pdu neighbor

C **E** **S**

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

```
FTOS(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2
```

```
Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using 680 bytes
PDU[1] : len 101, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00650100 00000013 00000000 00000000 419ef06c 00000000
  00000000 00000000 00000000 00000000 0181a1e4 0181a25c 41af92c0 00000000 00000000 00000000
  00000000 00000001 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 40958758, 27 packet(s) captured using 562 bytes
```



```

PDU[1] : len 41, captured 00:34:52 ago
ffffff fffffff fffffff fffffff 00290104 000100b4 14141401 0c020a01 04000100 01020080
00000000
PDU[2] : len 19, captured 00:34:51 ago
ffffff fffffff fffffff fffffff 00130400
PDU[3] : len 19, captured 00:34:50 ago
ffffff fffffff fffffff fffffff 00130400
[. . .]
FTOS#

```

**Related
Commands**

[capture bgp-pdu max-buffer-size](#) Specify a size for the capture buffer.

**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

show config

C **E** **S**

View the current ROUTER BGP configuration.

Syntax

show config

Command Modes

ROUTER BGP

Example

```

FTOS(conf-router_bgp)#show confi
!
router bgp 45
 neighbor suzanne peer-group
 neighbor suzanne no shutdown
 neighbor sara peer-group
 neighbor sara shutdown
 neighbor 13.14.15.20 peer-group suzanne
 neighbor 13.14.15.20 shutdown
 neighbor 123.34.55.123 peer-group suzanne
 neighbor 123.34.55.123 shutdown
FTOS(conf-router_bgp)#

```

**Command
History**

Version 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 [*ipv4 unicast*] [*network* [*network-mask*] [**longer-prefixes**]]

Parameters

ipv4 unicast (OPTIONAL) Enter the **ipv4 unicast** keywords to view information only related to ipv4 unicast routes.

network (OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.

network-mask (OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.

longer-prefixes (OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.

Command Modes

EXEC

EXEC Privilege

Usage Information

When you enable **bgp non-deterministic-med** command, the **show ip bgp** command output for a BGP route does not list the INACTIVE reason.

Example

```
FTOS>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

   Network          Next Hop          Metric      LocPrf   Weight  Path
*> 0.0.0.0/0        63.114.8.33
*   3.0.0.0/8        63.114.8.33
*>
*> 3.3.0.0/16       0.0.0.0           22          32768    ?
                    63.114.8.35
                    0 18508 ?
*> 4.0.0.0/8        63.114.8.33
                    0 18508 701 1 i
*> 4.2.49.12/30     63.114.8.33
                    0 18508 209 i
*   4.17.250.0/24   63.114.8.33
                    0 18508 209 1239 13716 i
*>
*   4.21.132.0/23   63.114.8.33
                    0 18508 209 6461 16422 i
*>
*> 4.24.118.16/30   63.114.8.33
                    0 18508 209 i
*> 4.24.145.0/30    63.114.8.33
                    0 18508 209 i
*> 4.24.187.12/30   63.114.8.33
                    0 18508 209 i
*> 4.24.202.0/30    63.114.8.33
                    0 18508 209 i
*> 4.25.88.0/30     63.114.8.33
                    0 18508 209 3561 3908 i
*> 5.0.0.0/9        63.114.8.33
                    0
                    0 18508 ?
*> 5.0.0.0/10       63.114.8.33
                    0
                    0 18508 ?
*> 5.0.0.0/11       63.114.8.33
                    0
                    0 18508 ?
--More--
```

Table 13-15, "show ip bgp Command Example Fields," in Border Gateway Protocol IPv4 (BGPv4) defines the information displayed in the example above

Table 13-15. show ip bgp Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

**Related
Commands**

[show ip bgp community](#) View BGP communities.
[neighbor maximum-prefix](#) Control number of network prefixes received.

**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 cluster-list

C **E** **S** View BGP neighbors in a specific cluster.

Syntax `show ip bgp [ipv4 unicast] cluster-list [cluster-id]`

Parameters

ipv4 unicast (OPTIONAL) Enter the **ipv4 unicast** keywords to view information only related to ipv4 unicast routes.
cluster-id (OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes

EXEC
 EXEC Privilege

Example

```
FTOS#show ip bgp cluster-list
BGP table version is 64444683, 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
Network          Next Hop          Metric      LocPrf Weight Path
* I 10.10.10.1/32 192.68.16.1      0           100    0 i
* I                192.68.16.1      0           100    0 i
*>I                192.68.16.1      0           100    0 i
* I                192.68.16.1      0           100    0 i
* I                192.68.16.1      0           100    0 i
* I                192.68.16.1      0           100    0 i
* I 10.19.75.5/32 192.68.16.1      0           100    0 ?
* I                192.68.16.1      0           100    0 ?
*>I                192.68.16.1      0           100    0 ?
```

```

* I          192.68.16.1          0          100          0 ?
* I          192.68.16.1          0          100          0 ?
* I          192.68.16.1          0          100          0 ?
* I 10.30.1.0/24 192.68.16.1          0          100          0 ?
* I          192.68.16.1          0          100          0 ?
*>I         192.68.16.1          0          100          0 ?
* I          192.68.16.1          0          100          0 ?
* I          192.68.16.1          0          100          0 ?
* I          192.68.16.1          0          100          0 ?

```

Table 13-16, "show ip bgp cluster-list Command Fields," in Border Gateway Protocol IPv4 (BGPv4) defines the information displayed in the example above.

Table 13-16. show ip bgp cluster-list Command Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

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 community

C **E** **S**

View information on all routes with Community attributes or view specific BGP community groups.

Syntax

show ip bgp [*ipv4 unicast*] **community** [*community-number*] [**local-as**] [**no-export**] [**no-advertise**]

Parameters

ipv4 unicast (OPTIONAL) Enter the **ipv4 unicast** keywords to view information only related to ipv4 unicast routes.

community-number Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
You can specify up to eight community numbers to view information on those community groups.

local-AS Enter the keywords **local-AS** to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED.
All routes with the NO_EXPORT_SUBCONFED (0xFFFFF03) community attribute must not be advertised to external BGP peers.

- no-advertise** Enter the keywords **no-advertise** to view all routes containing the well-known community attribute of NO_ADVERTISE.
All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.
- no-export** Enter the keywords **no-export** to view all routes containing the well-known community attribute of NO_EXPORT.
All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes EXEC

EXEC Privilege

Usage Information To view the total number of COMMUNITY attributes found, use the [show ip bgp](#) summary command. The text line above the route table states the number of COMMUNITY attributes found.

Example

```

FTOS>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
Network          Next Hop          Metric      LocPrf      Weight    Path
* i 3.0.0.0/8      205.171.0.16      100         0          209 701 80 i
*>i 4.2.49.12/30    205.171.0.16      100         0          209 i
* i 4.21.132.0/23   205.171.0.16      100         0          209 6461 16422 i
*>i 4.24.118.16/30  205.171.0.16      100         0          209 i
*>i 4.24.145.0/30   205.171.0.16      100         0          209 i
*>i 4.24.187.12/30  205.171.0.16      100         0          209 i
*>i 4.24.202.0/30   205.171.0.16      100         0          209 i
*>i 4.25.88.0/30    205.171.0.16      100         0          209 3561 3908 i
*>i 6.1.0.0/16      205.171.0.16      100         0          209 7170 1455 i
*>i 6.2.0.0/22      205.171.0.16      100         0          209 7170 1455 i
*>i 6.3.0.0/18      205.171.0.16      100         0          209 7170 1455 i
*>i 6.4.0.0/16      205.171.0.16      100         0          209 7170 1455 i
*>i 6.5.0.0/19      205.171.0.16      100         0          209 7170 1455 i
*>i 6.8.0.0/20      205.171.0.16      100         0          209 7170 1455 i
*>i 6.9.0.0/20      205.171.0.16      100         0          209 7170 1455 i
*>i 6.10.0.0/15     205.171.0.16      100         0          209 7170 1455 i
*>i 6.14.0.0/15     205.171.0.16      100         0          209 7170 1455 i
*>i 6.133.0.0/21    205.171.0.16      100         0          209 7170 1455 i
*>i 6.151.0.0/16    205.171.0.16      100         0          209 7170 1455 i
--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 13-17. Command Example Fields: show ip bgp community

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.

Table 13-17. Command Example Fields: show ip bgp community

Field	Description
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

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 community-list

C **E** **S**

View routes that are affected by a specific community list.

Syntax**show ip bgp** [*ipv4 unicast*] **community-list** *community-list-name* [**exact-match**]**Parameters**

<i>ipv4 unicast</i>	(OPTIONAL) Enter the ipv4 unicast keywords to view information only related to ipv4 unicast routes.
<i>community-list-name</i>	Enter the name of a configured IP community list. (max 16 chars)
exact-match	Enter the keyword for an exact match of the communities.

Command Modes

EXEC

EXEC Privilege

Example

```
FTOS#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop          Metric      LocPrf   Weight  Path
FTOS#
```

The [show ip bgp community-list](#) command without any parameters lists BGP routes matching the Community List and the output is the same as for the [show ip bgp](#) command output.

Table 13-18. show ip bgp community-list Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

**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 dampened-paths

C **E** **S** View BGP routes that are dampened (non-active).

Syntax **show ip bgp** [*ipv4 unicast*] **dampened-paths**

Command Modes EXEC
EXEC Privilege

Example

```
FTOS>show ip bgp damp
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          From           Reuse         Path
FTOS>
```

Table 13-19, "show ip bgp dampened-paths Command Example," in Border Gateway Protocol IPv4 (BGPv4) defines the information displayed in the example above.

Table 13-19. show ip bgp dampened-paths Command Example

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

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 detail

C **E** **S** Display BGP internal information for IPv4 Unicast address family.

Syntax **show ip bgp** [*ipv4 unicast*] **detail**

Defaults none

Command Modes EXEC
EXEC Privilege

Example

```
R2#show ip bgp detail

Detail information for BGP Node
bgpNdp 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPMPPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 : NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP 0x41a19088
```



```

NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25000
: NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP : NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 : NdModCommP
0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 : NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSet 0x41a1a298 : NHopDfrdHdP 0x41a1a3e0 :

NumNhDfrd 0 : CfgHdrAFMsk 1
AFChkNetTmrP 0x41ee705c : AFRtDamp 0 : AlwaysCmpMed 0 : LocrHld 10 : LocrRem
10 : softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : FataIs 0 : ConnExps 0 : HldExps 0 : KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 : TxNotifs 0
BadEvts 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP 0x41a1b6d4 : RxOp-
CodeP 0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP 0x41a1b750 : TxOp-
CodeP 0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP 0x41a1b7b8 : LogN-
brChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl 0 : AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 : CleanRibTmrP
0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP 0x41ee713c :
FastExtFallover 1 : FastIntFallover 0 : EnforcelstAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpiCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 : NonDet 0 : Dfrd-
PathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 : IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 : MaxeorExtInt 361
FixedPartCrt 1 : VarParCrt 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 0x41a0d200 : NdRTMMkrP 0x41a19d28 : NdRTMAFT-
blVer 0 : NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPrefix 0 : NdAfNLRIP 0 : NdAFNLRILen 0 : NdAFWPtrP
0
NdAFWLen 0 : NdAfNH : NdAFRedRttP 0x41a0d400 : NdRecCtxAdd 1101110868
NdRedCtxAddrLen 255 : NdAfRedMkrP 0x41a19e88 : AFAggRttP 0x41a0d600 : AFaggC-
txAddr 1101111028 : AFaggCtxAddrLen 255
AfNumAggrPfx 0 : AfNumAggrASSet 0 : AfNumSuppmap 0 : AfNumAggrValidPfx 0 :
AfMPathRttP 0x41a0d700
MpathCtxAddr 1101111140 : MpathCtxAddrLen 255 : AfEorSet 0x41a19f98 : NumD-
frdPfx 0
AfActPeerHd 0x41a1a3a4 : AfExtDist 1101112312 : AfIntDist 200 : AfLocDist 200
AfNumRRc 0 : AfRR 0 : AfNetRttP 0x41a0d300 : AfNetCtxAddr 1101112392 :
AfNetCtxAddrLen 255
AfNwCtxAddr 1101112443 : AfNwCtxAddrLen 255 : AfNetBKDrRttP 0x41a0d500 :
AfNetBKDRCnt 0 : AfDampHLife 0

```

```
AfDampReuse 0 : AfDampSupp 0 : AfDampMaxHld 0 : AfDampCeiling 0 : AfDampRmapP
0x41a1a508
AfNumDamped 0 : AfNumHist 0 : AfNumTotalHist 0 : AfDfrdRtLstP 0x41a1b5fc :
AfDfrdNodeCnt 0 : softRecfgAf 0x41a1b5b4 : softRecfgCfgAf 0x41a1b5f0
AfCfgCnt 0 : AfRedistCfg 0 : IBGP_Mpath 0 : EBGP_Mpath 0 : DebugInPfList :
DebugOutPfList
```

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

show ip bgp extcommunity-list

C **E** **S**

View information on all routes with Extended Community attributes.

Syntax

show ip bgp [*ipv4 unicast*] **extcommunity-list** [*list name*]

Parameters

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 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

show ip bgp filter-list

C **E** **S**

View the routes that match the filter lists.

Syntax

show ip bgp [*ipv4 unicast*] **filter-list** *as-path-name*

Parameters

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

Example

```
FTOS#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: 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 6.1.5.0/24	192.100.11.2	20000	9999	0	?
* I	192.100.8.2	20000	9999	0	?
* I	192.100.9.2	20000	9999	0	?
* I	192.100.10.2	20000	9999	0	?
*>I	6.1.5.1	20000	9999	0	?
* I	6.1.6.1	20000	9999	0	?
* I	6.1.20.1	20000	9999	0	?
* I 6.1.6.0/24	192.100.11.2	20000	9999	0	?
* I	192.100.8.2	20000	9999	0	?
* I	192.100.9.2	20000	9999	0	?
* I	192.100.10.2	20000	9999	0	?
*>I	6.1.5.1	20000	9999	0	?
* I	6.1.6.1	20000	9999	0	?
* I	6.1.20.1	20000	9999	0	?
* I 6.1.20.0/24	192.100.11.2	20000	9999	0	?
* I	192.100.8.2	20000	9999	0	?
* I	192.100.9.2	20000	9999	0	?
* I	192.100.10.2	20000	9999	0	?

F7OS#

(Table 13-20) defines the information displayed in the example above.

Table 13-20. Command Example fields: show ip bgp filter-list

Field	Description
Path source codes	Lists the path sources shown to the right of the last AS number in the Path column: <ul style="list-style-type: none"> • i = internal route entry • a = aggregate route entry • c = external confederation route entry • n = network route entry • r = redistributed route entry
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

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 flap-statistics



View flap statistics on BGP routes.

Syntax `show ip bgp [ipv4 unicast] flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-expression]`

Parameters

- ipv4 unicast** (OPTIONAL) Enter the **ipv4 unicast** keywords to view information only related to ipv4 unicast routes.
- ip-address** (OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
- mask** (OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
- filter-list as-path-name** (OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH ACL.
- regexp regular-expression** Enter a regular expression then use one or a combination of the following characters to match:
- `.` = (period) any single character (including a white space)
 - `*` = (asterisk) the sequences in a pattern (0 or more sequences)
 - `+` = (plus) the sequences in a pattern (1 or more sequences)
 - `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**
 - `[]` = (brackets) a range of single-character patterns.
 - `()` = (parenthesis) groups a series of pattern elements to a single element
 - `{ }` = (braces) minimum and the maximum match count
 - `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
 - `$` = (dollar sign) the end of the output string.

Command Modes EXEC

EXEC Privilege

Example

```
FTOS>show ip bgp flap
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network                From                Flaps Duration Reuse      Path
FTOS>
```

[Table 13-21, "show ip bgp flap-statistics Command Example Fields," in Border Gateway Protocol IPv4 \(BGPv4\)](#) defines the information displayed in the example above.

Table 13-21. show ip bgp flap-statistics Command Example Fields

Field	Description
Network	Displays the network ID to which the route is flapping.
From	Displays the IP address of the neighbor advertising the flapping route.

Table 13-21. show ip bgp flap-statistics Command Example Fields

Field	Description
Flaps	Displays the number of times the route flapped.
Duration	Displays the hours:minutes:seconds since the route first flapped.
Reuse	Displays the hours:minutes:seconds until the flapped route is available.
Path	Lists all the ASs the flapping route passed through to reach the destination network.

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 inconsistent-as



View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax `show ip bgp [ipv4 unicast] inconsistent-as`

Command Modes EXEC

EXEC Privilege

Example

```
FTOS>show ip bgp inconsistent-as
BGP table version is 280852, 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 ?
*	63.114.8.34		0	18508	209 7018 ?
*	63.114.8.33		0	18508	701 7018 ?
*	63.114.8.33		0	18508	209 7018 ?
*> 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	701 1 i
*	63.114.8.33		0	18508	209 1 i
* 6.0.0.0/20	63.114.8.60		0	18508	209 3549 i
*	63.114.8.34		0	18508	209 3549 i
*>	63.114.8.33	0	0	18508	?
*	63.114.8.33		0	18508	209 3549 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 13-22. show ip bgp inconsistent-as Command Example Fields

Fields	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

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 neighbors

C **E** **S**

Displays routing information exchanged by BGP neighbors.

Syntax

```
show ip bgp [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

ipv4 unicast	(OPTIONAL) Enter the ipv4 unicast keywords to view information only related to IPv4 unicast routes.
<i>ipv4-neighbor-addr</i> <i>ipv6-neighbor-addr</i>	(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 [<i>network</i> [<i>network-mask</i>]]	(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 [<i>network</i> [<i>network-mask</i>]]	(OPTIONAL) Enter the keywords denied-routes followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

Command Modes

EXEC

EXEC Privilege

Command History

Version 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 6.3.1.0	The output is changed to display the total number of advertised prefixes

Example 1 (Partial)

```
FTOS#show ip bgp neighbors

BGP neighbor is 100.10.10.2, remote AS 200, external link
  BGP version 4, remote router ID 192.168.2.101
  BGP state ESTABLISHED, in this state for 00:16:12
  Last read 00:00:12, last write 00:00:03
  Hold time is 180, keepalive interval is 60 seconds
  Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    ROUTE_REFRESH(2)
    GRACEFUL_RESTART(64)
    CISCO_ROUTE_REFRESH(128)

  Route map for incoming advertisements is test
  Maximum prefix set to 4 with threshold 75

  For address family: IPv4 Unicast
  BGP table version 34, neighbor version 34
  5 accepted prefixes consume 20 bytes
  Prefix advertised 0, denied 4, withdrawn 0

  Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer

  Connections established 2; dropped 1
  Last reset 00:18:21, due to Maximum prefix limit reached

  Notification History
  'Connection Reset' Sent : 1  Recv: 0

Local host: 100.10.10.1, Local port: 179
Foreign host: 100.10.10.2, Foreign port: 47496
```

FTOS#

**Example 2
(advertised-routes)**

FTOS>show ip bgp neighbors 192.14.1.5 advertised-routes

BGP table version is 74103, local router ID is 33.33.33.33
 Status codes: s suppressed, S stale, d damped, h history, * valid, > best
 Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>r 1.10.1.0/24	0.0.0.0	5000		32768	?
*>r 1.11.0.0/16	0.0.0.0	5000		32768	?
.....					
*>I 223.94.249.0/24	223.100.4.249	0	100	0	?
*>I 223.94.250.0/24	223.100.4.250	0	100	0	?
*>I 223.100.0.0/16	223.100.255.254	0	100	0	?

Total number of prefixes: 74102

**Example 3
(received-routes)**

FTOS#show ip bgp neighbors 100.10.10.2 received-routes

BGP table version is 13, local router ID is 120.10.10.1
 Status codes: s suppressed, S stale, d damped, h history, * valid, > best
 Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
 n - network, D - denied, S - stale
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
D 70.70.21.0/24	100.10.10.2		0	0 100 200	?
D 70.70.22.0/24	100.10.10.2		0	0 100 200	?
D 70.70.23.0/24	100.10.10.2		0	0 100 200	?
D 70.70.24.0/24	100.10.10.2		0	0 100 200	?
*> 70.70.25.0/24	100.10.10.2		0	0 100 200	?
*> 70.70.26.0/24	100.10.10.2	0	0	0 100 200	?
*> 70.70.27.0/24	100.10.10.2	0	0	0 100 200	?
*> 70.70.28.0/24	100.10.10.2	0	0	0 100 200	?
*> 70.70.29.0/24	100.10.10.2	0	0	0 100 200	?

FTOS#

**Example 4
(denied-routes)**

FTOS#show ip bgp neighbors 100.10.10.2 denied-routes

4 denied paths using 205 bytes of memory
 BGP table version is 34, local router ID is 100.10.10.2
 Status codes: s suppressed, S stale, d damped, h history, * valid, > best
 Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
 n - network, D - denied, S - stale
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
D 70.70.21.0/24	100.10.10.2		0	0 100 200	?
D 70.70.22.0/24	100.10.10.2		0	0 100 200	?
D 70.70.23.0/24	100.10.10.2		0	0 100 200	?
D 70.70.24.0/24	100.10.10.2		0	0 100 200	?

FTOS#

Table 13-23. Command Example fields: show ip bgp neighbors

Lines beginning with	Description
BGP neighbor	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.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: <ul style="list-style-type: none"> 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 Unicast as the address family.
BGP table version	Displays the which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefix 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](#)

View the current BGP routing table.

show ip bgp next-hop

C **E** **S**

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

```
FTOS>show ip bgp next-hop
Next-hop          Via                               RefCount  Cost  Flaps  Time Elapsed
63.114.8.33       63.114.8.33, Gi 12/22           240984    0    0 00:18:25
63.114.8.34       63.114.8.34, Gi 12/22           135152    0    0 00:18:13
63.114.8.35       63.114.8.35, Gi 12/22             1        0    0 00:18:07
63.114.8.60       63.114.8.60, Gi 12/22           135155    0    0 00:18:11
FTOS>
```

Table 13-24. Command Example fields: show ip bgp next-hop

Field	Description
Next-hop	Displays the next-hop IP address.
Via	Displays the IP address and interface used to reach the next hop.
RefCount	Displays the number of BGP routes using this next hop.
Cost	Displays the cost associated with using this next hop.
Flaps	Displays the number of times the next hop has flapped.
Time Elapsed	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.

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

C **E** **S**

View all the BGP path attributes in the BGP database.

Syntax `show ip bgp paths [regexp regular-expression]`

Parameters

regex *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

```
FTOS#show ip bgp path
Total 16 Paths
Address          Hash Refcount Metric Path
0x1efe7e5c       15      10000      32 ?
0x1efe7e1c       71      10000      23 ?
0x1efe7ddc      127      10000      22 ?
0x1efe7d9c      183      10000      43 ?
0x1efe7d5c      239      10000      42 ?
0x1efe7c9c      283         6      {102 103} ?
0x1efe7b1c      287      336 20000      ?
0x1efe7d1c      295      10000      13 ?
0x1efe7c5c      339         6      {92 93} ?
0x1efe7cdc      351      10000      12 ?
0x1efe7c1c      395         6      {82 83} ?
0x1efe7bdc      451         6      {72 73} ?
0x1efe7b5c      491        78         0 ?
0x1efe7adc      883         2      120 i
0x1efe7e9c      983      10000      33 ?
0x1efe7b9c     1003         6         0 i
FTOS#
```

Table 13-25. Command Example fields: show ip bgp paths

Field	Description
Total	Displays the total number of BGP path attributes.
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using this path attribute.
Metric	Displays the MED attribute for this path attribute.
Path	Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces { } are AS_SET information.

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 as-path

C **E** **S** View all unique AS-PATHs in the BGP database

Syntax **show ip bgp paths as-path**

Command Modes EXEC
EXEC Privilege

Example

```

FTOS#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
FTOS#

```

Table 13-26. Command Example fields: show ip bgp paths community

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these AS-Paths.
AS-Path	Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces { } are AS_SET information.

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 community



View all unique COMMUNITY numbers in the BGP database.

Syntax `show ip bgp paths community`

Command Modes EXEC

EXEC Privilege

Example

```
E1200-BGP>show ip bgp paths community
Total 293 Communities
Address          Hash Refcount Community
0x1ec88a5c       3         4 209:209 209:6059 209:31272 3908:900 19092:300
0x1e0f10ec       15        4 209:209 209:3039 209:31272 3908:900 19092:300
0x1c902234       37         2 209:209 209:7193 209:21362 3908:900 19092:300
0x1f588cd4       41        24 209:209 209:6253 209:21362 3908:900 19092:300
0x1e805884       46         2 209:209 209:21226 286:777 286:3033 1899:3033
64675:21092
0x1e433f4c       46         8 209:209 209:5097 209:21362 3908:900 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 3908:900 19092:300
0x1c9f88e4       53         4 209:209 209:3193 209:21362 3908:900 19092:300
0x1f58a944       57         6 209:209 209:2073 209:21362 3908:900 19092:300
0x1ce6be44       80         2 209:209 209:999 209:40832
0x1c6e2374       80         2 209:777 209:41528
0x1f58ad6c       82        46 209:209 209:41528
0x1c6e2064       83         2 209:777 209:40832
0x1f588ecc       85        570 209:209 209:40832
0x1f57cc0c       98         2 209:209 209:21226 286:3031 13646:1044 13646:1124
13646:1154 13646:1164 13646:1184 13646:1194 13646:1204 13646:1214 13646:1224
13646:1234 13646:1244 13646:1254 13646:1264 13646:3000
0x1d65b2ac      117         6 209:209 209:999 209:31272
0x1f5854ac      119        18 209:209 209:21226 286:108 286:111 286:777
286:3033 517:5104
0x1d77b49c      119         2 209:209 209:21226 286:81 286:777 286:3358 790:51
790:61 790:3358
0x1c6e210c      120         2 209:777 209:31272
0x1f588bf4      122       680 209:209 209:31272
0x1f004f64      123        12 209:209 209:21226 286:777 286:3031 5466:20
--More--
```

Table 13-27. Command Example fields: show ip bgp paths community

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these communities.
Community	Displays the community attributes in this BGP path.

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 peer-group



Enables you to view information on the BGP peers in a peer group.

Syntax `show ip bgp [ipv4 unicast] peer-group [peer-group-name [detail | summary]]`

Parameters

- ipv4 unicast* (OPTIONAL) Enter the **ipv4 unicast** keywords to view information only related to ipv4 unicast routes.
- peer-group-name* (OPTIONAL) Enter the name of a peer group to view information about that peer group only.
- detail** (OPTIONAL) Enter the keyword **detail** to view detailed status information of the peers in that peer group.
- summary** (OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group.
The output is the same as that found in [show ip bgp summary](#) command

Command Modes

EXEC
EXEC Privilege

Example

```
FTOS#show ip bgp peer-group
Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
 12.1.1.2*
 12.1.1.3*
 12.1.1.4*
 12.1.1.5*
 12.1.1.6*
 12.2.1.2*
 12.2.1.3*
 12.2.1.4*
 12.2.1.5*
 12.2.1.6*
 12.3.1.2*
 12.3.1.3*
 12.3.1.4*
 12.3.1.5*
 12.3.1.6*
 12.4.1.2*
 12.4.1.3*
 12.4.1.4*
 12.4.1.5*
 12.4.1.6*
```

Table 13-28. Command Example fields: show ip bgp peer-group

Line beginning with	Description
Peer-group	Displays the peer group's name.
Administratively shut	Displays the peer group's status if the peer group is not enabled. If the peer group is enabled, this line is not displayed.
BGP version	Displays the BGP version supported.
Minimum time	Displays the time interval between BGP advertisements.
For address family	Displays IPv4 Unicast as the address family.
BGP neighbor	Displays the name of the BGP neighbor.
Number of peers	Displays the number of peers currently configured for this peer group.
Peer-group members:	Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, a * is displayed next to the IP address.

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 peer-group (multicast)	View information on the BGP peers in a peer group.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series
Version 7.8.1.0	Introduced support on S-Series

show ip bgp regexp

C **E** **S**

Display the subset of BGP routing table matching the regular expressions specified.

Syntax**show ip bgp regexp** *regular-expression* [*character*]**Parameters**

<i>regular-expression</i> [<i>character</i>]	Enter a regular expression then use one or a combination of the following characters to match: <ul style="list-style-type: none"> • . = (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

```

FTOS#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network                Next Hop                Metric      LocPrf Weight Path
*>I 3.0.0.0/8             1.1.1.2                  0           100     0 2914 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 i
*>I 4.19.16.0/23          1.1.1.2                  0           100     0 2914 701
6167 6167 6167 i
*>I 4.21.80.0/22          1.1.1.2                  0           100     0 2914 174
4200 16559 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 8063 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 i
*>I 4.67.64.0/22          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 6.1.0.0/16            1.1.1.2                  0           100     0 2914 701
668 i
*>I 6.2.0.0/22            1.1.1.2                  0           100     0 2914 701
668 i
*>I 6.3.0.0/18            1.1.1.2                  0           100     0 2914 701
668 i

```

Table 13-29. Command Example fields: show ip bgp regexp

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then non-BGP routes exist in the router's routing table.
Metric	Displays the BGP router's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the AS paths the route passed through to reach the destination network.

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 summary

C **E** **S** Enables you to view the status of all BGP connections.

Syntax `show ip bgp [ipv4 unicast] summary`

Command Modes EXEC

EXEC Privilege

Example

```

FTOS#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
*>I 3.0.0.0/8	1.1.1.2	0	100	0	2914 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 i					
*>I 4.19.16.0/23	1.1.1.2	0	100	0	2914 701
6167 6167 6167 i					
*>I 4.21.80.0/22	1.1.1.2	0	100	0	2914 174
4200 16559 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 8063 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 i					
*>I 4.67.64.0/22	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 6.1.0.0/16	1.1.1.2	0	100	0	2914 701
668 i					
*>I 6.2.0.0/22	1.1.1.2	0	100	0	2914 701
668 i					
*>I 6.3.0.0/18	1.1.1.2	0	100	0	2914 701
668 i					

Table 13-30. Command Example fields: show ip bgp summary

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries and route paths and the amount of memory used to process those entries.
paths	Displays the number of paths and the amount of memory used.
denied paths	Displays the number of denied paths and the amount of memory used.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	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.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	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.
Up/Down	Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed. The output format is: Time Established-----Display Example < 1 day ----- 00:12:23 (hours:minutes:seconds) < 1 week ----- 1d21h (DaysHours) > 1 week ----- 11w2d (WeeksDays)
State/Pfxrcd	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.

Command History

Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series

show running-config bgp

C **E** **S** Use this feature to display the current BGP configuration.

Syntax **show running-config bgp**

Defaults No default values or behavior

Command Modes EXEC Privilege

Command History	Version 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

timers bgp

C **E** **S** Adjust BGP Keep Alive and Hold Time timers.

Syntax **timers bgp** *keepalive holdtime*

To return to the default, enter **no timers bgp**.

Parameters	<i>keepalive</i>	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. Range: 1 to 65535 Default: 60 seconds
	<i>holdtime</i>	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	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

MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). FTOS MBGP is implemented as per IETF RFC 1858.

FTOS version 7.8.1.0 and later support MBGP for IPv6 on **E**_T and **C** platforms.

FTOS version 7.8.1.0 and later supports MBGP for IPv4 Multicast only on the **S** platform.

FTOS 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 dampening
- debug ip bgp peer-group updates
- debug ip bgp ipv4 unicast soft-reconfiguration
- debug ip bgp 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
- 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

ipv4 Enter the keyword **ipv4** to specify the address family as IPV4.
multicast Enter the keyword **multicast** to specify multicast as SAFI.

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.

Command History

Version 7.8.1.0 Introduced support on S-Series for MBGP IPv4 Multicast
Version 7.7.1.0 Introduced support on C-Series

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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.</p>				
Command History	<table border="0"> <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> </table>	Version 7.8.1.0	Introduced support on S-Series	Version 7.7.1.0	Introduced support on C-Series
Version 7.8.1.0	Introduced support on S-Series				
Version 7.7.1.0	Introduced support on C-Series				

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)

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

bgp soft-reconfig-backup

C E S

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.

Related Commands

[clear ip bgp ipv4 multicast soft in](#) Activate inbound policies without resetting the BGP TCP session.

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 dampening

C E T S

Clear information on route dampening.

Syntax `clear ip bgp dampening ipv4 multicast network network-mask`

Parameters

dampening	Enter the keyword dampening to clear route flap dampening information.
<i>network</i>	(OPTIONAL) Enter the network address in dotted decimal format (A.B.C.D).
<i>network-mask</i>	(OPTIONAL) Enter the network mask in slash prefix format (/x).

Command Modes 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

clear ip bgp flap-statistics

C **E** **T** **S** Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax `clear ip bgp ipv4 multicast flap-statistics network | filter-list list | regexp regexp`

Parameters

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: <ul style="list-style-type: none"> • . = (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

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

clear ip bgp ipv4 multicast soft

C **E** **T** **S** 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) <i>or</i> 1-4294967295 (4-Byte) <i>or</i> 0.1-65535.65535 (Dotted format)
ipv4-neighbor-addr ipv6-neighbor-addr	Clear and reapply policies for a neighbor.
peer-group name	Clear and reapply policies for all BGP routers in the specified peer group.

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

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 dampening

C **E** **T** **S** View information on routes being dampened.

Syntax **debug ip bgp ipv4 multicast dampening**

To disable debugging, enter **no debug ip bgp ipv4 multicast dampening**

Parameters **dampening** Enter the keyword **dampening** to clear route flap dampening information.

Command Modes EXEC Privilege

Command History	Version 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

debug ip bgp ipv4 multicast soft-reconfiguration

C **E** **S** 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

<i>ipv4-address</i> <i>ipv6-address</i>	Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
<i>peer-group-name</i>	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.	
Command History	Version 8.4.1.0	Introduced support for IPv4 multicast and IPv6 unicast 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 peer-group updates



View information about BGP peer-group updates.

debug 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

peer-group <i>peer-group-name</i>	Enter the keyword peer-group followed by the name of the peer-group.
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.

Command Modes 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

debug ip bgp updates



View information about BGP updates.

debug ip bgp updates [**in** | **out**]

To disable debugging, enter **no debug ip bgp updates** [**in** | **out**] command.

Parameters

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.

Command Modes	EXEC Privilege	
Defaults	Disabled.	
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

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	<i>external-distance</i>	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
	<i>internal-distance</i>	Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200
	<i>local-distance</i>	Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200

Defaults *external-distance* = 20; *internal-distance* = 200; *local-distance* = 200.

Command Modes ROUTER BGP (conf-router_bgp_af)



Caution: Dell 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	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 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

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

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

[address family ipv4 multicast \(MBGP\)](#) Changes the context to SAFI

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 advertisement-interval

C **E** **T** **S**

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 Address Family (conf-router_bgp_af)

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 default-originate

C **E** **T** **S** 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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map <i>map-name</i>	(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

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 distribute-list

C **E** **T** **S** 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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
<i>prefix-list-name</i>	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	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
	Version 7.6.1.0	Introduced IPv6 MGBP support for E-Series

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
<i>access-list-name</i>	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

C **E** **T** **S** 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

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.

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, FTOS 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

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

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 next-hop-self

C **E** **T** **S** 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

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.

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.

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 remove-private-as

C **E** **T** **S** 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	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 route-map

C **E** **T** **S** Apply an established route map to either incoming or outbound routes of a BGP neighbor or c 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	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 route-reflector-client

C **E** **T** **S**

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	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	(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	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 soft-reconfiguration inbound

C **E** **S**

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**

Parameters	<i>ipv4-address</i> <i>ipv6-address</i>	Enter the IP address of the neighbor for which you want to start storing inbound routing updates.
	<i>peer-group-name</i>	Enter the name of the peer group for which you want to start storing inbound routing updates.

Defaults Disabled

Command Modes ROUTER BGP ADDRESS FAMILY (conf-router_bgp_af)

Usage Information This command enables soft-reconfiguration for the specified BGP neighbor. BGP will store all updates for inbound IPv4 multicast 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

Version 8.4.1.0	Added support for IPv4 multicast and IPv4 unicast address families
Version 7.8.1.0	Introduced support on S-Series
Version 7.7.1.0	Introduced support on C-Series
Version 7.4.1.0	Introduced

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 Address Family (conf-router_bgp_af)

Usage Information FTOS 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

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 ospf

C E T S 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 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

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 cluster-list

C E T S

View BGP neighbors in a specific cluster.

Syntax**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**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

C E S

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 (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords no-advertise to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords no-export to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes	EXEC
	EXEC Privilege
Usage Information	To view the total number of COMMUNITY attributes found, use the show ip bgp summary command. The text line above the route table states the number of COMMUNITY attributes found.
	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

C **E** **T** **S** View routes that are affected by a specific community list.

Syntax **show ip bgp ipv4 multicast 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 7.8.1.0 Introduced support on S-Series
	Version 7.7.1.0 Introduced support on C-Series

show ip bgp dampened-paths

C **E** **T** **S** View BGP routes that are dampened (non-active).

Syntax **show ip bgp ipv4 multicast dampened-paths**

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 filter-list



View the routes that match the filter lists.

Syntax `show ip bgp ipv4 multicast filter-list as-path-name`

Parameters *as-path-name* Enter the name of an AS-PATH.

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 flap-statistics



View flap statistics on BGP routes.

Syntax `show ip bgp ipv4 multicast flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-expression]`

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+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

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 inconsistent-as

C **E** **T** **S**

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**

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

show ip bgp ipv4 multicast

C **E** **T** **S**

View the current MBGP routing table for the system.

Syntax **show ip bgp ipv4 multicast [detail | network [network-mask] [length]]**

Parameters	detail	(OPTIONAL) Enter the keyword detail to display BGP internal information for the IPv4 Multicast address family.
	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

Example

```

FTOS#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 145.1.1.0/16      0.0.0.0      0      32768 i
FTOS#
```

Table 13-31. show ip bgp Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

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
 Version 7.6.1.0 Introduced IPv6 MGBP support for E-Series
 Version 7.8.1.0 Introduced support on S-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 (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.
 [network
 [network-mask]

Note: [neighbor soft-reconfiguration inbound](#) must be configured prior to viewing all the information received from the neighbors.

denied-routes [network (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.
 [network-mask]

Command Modes EXEC
 EXEC Privilege

Command History

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

Example FTOS#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 13-32. Command Example fields: show ip bgp ipv4 multicast neighbors

Lines beginning with	Description
BGP neighbor	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.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: <ul style="list-style-type: none"> 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.

Table 13-32. Command Example fields: show ip bgp ipv4 multicast neighbors

Lines beginning with	Description
(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](#)

View the current BGP routing table.

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**

- peer-group-name* (OPTIONAL) Enter the name of a peer group to view information about that peer group only.
- detail** (OPTIONAL) Enter the keyword **detail** to view detailed status information of the peers in that peer group.
- summary** (OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group.
The output is the same as that found in [show ip bgp summary](#) command

Command ModesEXEC
EXEC Privilege**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 peer-group](#) View information on the BGP peers in a peer group.

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
Version 7.5.1.0 Modified: added **detail** option

show ip bgp summary

C **E** **T** **S**

Enables you to view the status of all BGP connections.

Syntax **show ip bgp ipv4 multicast summary**

Command Modes EXEC

EXEC Privilege

Example FTOS#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
#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
211.1.1.129	640	28	6	0	0	0	00:00:21	Active

FTOS#

Table 13-33. Command Example fields: show ip bgp ipv4 multicast summary

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries and route paths and the amount of memory used to process those entries.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	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.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.

Table 13-33. Command Example fields: show ip bgp ipv4 multicast summary

Field	Description
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	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.
Up/Down	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.
State/Pfx	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the <code>neighbor maximum-prefix</code> 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.

Command History

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 7.6.1.0	Introduced IPv6 MGBP support for E-Series

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

C **E** **S**

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

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)

Defaults Not configured

Command Modes CONFIGURATION (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

deny regex

C **E** **S**

This features enables you to specify an extended communities to reject (deny) using a regular expressions (regex).

Syntax **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	<pre>FTOS(conf-ext-community-list)#deny regexp 123 FTOS(conf-ext-community-list)#</pre>	
Related Commands	permit regex	Permit a community using a regular expression
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 `description {line}`

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

Parameters *line* Enter a description (maximum 80 characters).

Defaults Not configured

Command Modes CONFIGURATION (conf-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

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. Refer to the example below.

Example

```
FTOS(conf)#ip extcommunity-list test
FTOS(conf-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

C **E** **S** 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.

Example

```
FTOS(config-route-map)#match extcommunity Freedombird
FTOS(config-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

permit

C **E** **S** 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).

	<i>ASN:NNNN</i>	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
	<i>IPADDR:NN</i>	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value)
Defaults	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 to specify extended communities to forward (permit) using regular expressions (regex).

Syntax	permit regex { <i>regex</i> }	
	To remove, use the no permit regex { <i>regex</i> } command.	
Parameters	<i>regex</i>	Enter a regular expression.
Defaults	Not configured	
Command Modes	CONFIGURATION (conf-ext-community-list)	
Usage Information	Duplicate commands are silently accepted.	
Example	<pre>FTOS(conf-ext-community-list)#permit regexp 123 FTOS(conf-ext-community-list)#</pre>	
Related Commands	deny regex	Deny a community using a regular expression
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

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 <i>ASN4:NN</i>	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).
<i>ASN:NNNN</i>	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
<i>IPADDR:NN</i>	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 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 soo](#) Set extended community site-of-origin in 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

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 <i>ASN4:NN</i>	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).
<i>ASN:NNNN</i>	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).

	<i>IPADDR:NN</i>	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	<p>If the set community rt and soo are in the same route-map entry, we can define the behavior as:</p> <ul style="list-style-type: none"> • 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.
	<i>name</i>	(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 example below.

Example

```
FTOS#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 :
      RT:1111:4278080  SoO:35:4          SoO:36:50529043    SoO:37:50529044
      SoO:38:50529045  SoO:0.0.0.2:33   SoO:506.62106:34   0x0303:254:11223*
```

FTOS#

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

```
FTOS#show ip bgp paths extcommunity
Total 1 Extended Communities

Address          Hash          Refcount      Extended Community
0x41d57024      12272         1             RT:7:200 SoO:5:300 SoO:0.0.0.3:1285
FTOS#
```

Table 13-34. Command Example fields: show ip bgp paths community

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these extended communities.
Community	Displays the extended community attributes in this BGP path.

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

C **E** **S** 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

```
FTOS#show ip extcommunity-list test
ip extcommunity-list test
deny RT:1234:12
permit regexp 123
deny regexp 234
deny regexp 123
FTOS#
```

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 running-config extcommunity-list

C **E** **S** Use this feature to display the current configuration of the extended community lists.

Syntax **show running-config extcommunity-list** [*word*]

Parameters *word* Enter the name of the extended community list you want to view.

Defaults No default values or behavior

Command Modes EXEC Privilege

Example

```
FTOS#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_)$
FTOS#
```

**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

Content Addressable Memory (CAM) for ExaScale

Overview

This chapter discusses CAM commands for the E-Series ExaScale  platform. Refer to [Chapter 15, Content Addressable Memory \(CAM\)](#) for information on the commands for the E-Series TeraScale platform



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

Commands

This chapter includes the following commands:

- [cam-profile template \[10M-CAM\]](#)
- [enable](#)
- [flow](#)
- [layer-2](#)
- [layer-3](#)
- [microcode](#)
- [show cam-profile](#)
- [test cam-profile](#)

Important Points to Remember

- The Default CAM-profile is supported on E-Series ExaScale with FTOS version 8.1.1.0 and later.
- The recommended, pre-defined CAM-profile templates are supported on E-Series ExaScale with FTOS version 8.2.1.0 and later.
- The CAM-profile template is applied to entire system. You must save the running-configuration to enable the change. Saving the running-configuration also ensures that the CAM-profile selected remains in the case of a reboot.
- All components in the chassis must have the same CAM-profile and microcode. The profile and microcode loaded on the primary RPM determines the profile that is required on all other chassis components.
- If a newly installed line card has a profile different from the primary RPM, the card reboots so that it can load the proper profile.
- If the standby RPM has a profile different from the primary RPM, the RPM reboots so that it can load the proper profile.
- Enabling a CAM-profile immediately replaces the existing CAM-profile. You will be prompted to save the running-configuration and reload the system to implement the new CAM-profile.

cam-profile *template* [10M-CAM]



Select a pre-defined CAM-profile template or create a new CAM-profile template.

Syntax `cam-profile template {10M-CAM}`

Parameters

template

Choose one of the following CAM profiles:

- **10M L2** to support IPv4 Layer 2 switching on line cards with 10M CAM.
- **10M L2 IPv6 Switching** to support IPv6 Layer 2 switching on line cards with 10M CAM.
- **40M L2 IPv6-IPv4** to support IPv4 and IPv6 Layer 2 routing on line cards with 40M CAM.
- **40M L2 IPv4Only** to support IPv4 Layer 2 routing on line cards with 40M CAM.
- **VRF** to support Virtual Routing and Forwarding (VRF).
- **MAX-IPv4-FIB** to allocate the maximum space supported for IPv4 FIB support.
- Enter a 16 character string used as a template name to create a new template.

Defaults Default

Command Modes CONFIGURATION

Command History

Version 8.2.1.0 Introduced on E-Series ExaScale

Usage Information

CAM profile changes take effect after the next chassis reboot.

CAM-profile template region allocations are not automatically configured when you select a template. Use the allocations shown in the **Content Addressable Memory for ExaScale** chapter in the *FTOS Configuration Guide* for detailed values supported in each CAM/SRAM region.

enable



Enable CAM-profile template.

Syntax `enable`

Defaults `cam-profile default microcode default`

Command Modes CONFIGURATION-CAM-profile-*template*

Command History

Version 8.2.1.0 Introduced on E-Series ExaScale

Usage Information

You must save the running configuration using the command `copy running-config startup-config` after changing the CAM-profile. CAM-profile template changes take effect after the next chassis reboot.

flow



Configure the Flow region for a CAM-profile template

Syntax **flow** [**ipv4** | **ipv6**] *multicast-fib {value} pbr {value} qos {value} system-flow {value}*

Defaults None

Command Modes CONFIGURATION-CAM-profile-template

Command History
Version 8.2.1.0 Introduced on E-Series ExaScale

Usage Information
You do not need to enter every parameter for a region. You can enter only the ones you need.

User configured CAM-profiles are automatically validated.

Refer to Content Addressable Memory for ExaScale in the FTOS Configuration Guide for detailed values supported in each CAM/SRAM region.

layer-2



Configure the Layer 2 region for a CAM-profile template

Syntax **layer-2 eg-acl** {value} *fib {value} frpp {value} ing-acl {value} learn {value} l2pt {value} qos {value} system-flow {value}*

Defaults None

Command Modes CONFIGURATION-CAM-profile-template

Command History
Version 8.2.1.0 Introduced on E-Series ExaScale

Usage Information
You do not need to enter every parameter for a region. You can enter only the ones you need.

User configured CAM-profiles are automatically validated.

Refer to Content Addressable Memory for ExaScale in the FTOS Configuration Guide for detailed values supported in each CAM/SRAM region.

layer-3



Configure the Layer 3 region for a CAM-profile template

Syntax **layer-3** [*ipv4* | *ipv6*] *eg-acl {value} fib {value} ing-acl {value}*

Defaults None

Command Modes CONFIGURATION-CAM-profile-template

Command History Version 8.2.1.0 Introduced on E-Series ExaScale

Usage Information You do not need to enter every parameter for a region. You can enter only the ones you need.

User configured CAM-profiles are automatically validated.

Refer to Content Addressable Memory for ExaScale in the FTOS Configuration Guide for detailed values supported in each CAM/SRAM region.

microcode



Assign the microcode to the created CAM-profile template

Syntax **microcode** { default | ipv6-switched | lag-hash-align | vrf }

Parameters

default	Distributes CAM space for a typical deployment. <ul style="list-style-type: none"> Applies to the Default CAM-profile and the recommended CAM-profile templates. Recommended for any user-defined CAM-profiles.
vrf	Distributes space to best manage IPv4 and IPv6 VRF packet forwarding <ul style="list-style-type: none"> Applies to the VRF cam-profile template only.
lag-hash-align	
ipv6-switched	

Defaults None

Command Modes CONFIGURATION-CAM-profile-template

Command History Version 8.2.1.0 Introduced on E-Series ExaScale

Usage Information You must assign a microcode to a CAM-profile template.
IPv6 is not supported with VRF microcode on ExaScale.

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

<i>profile</i>	(OPTIONAL) Choose a single CAM profile to display:
<i>summary</i>	(OPTIONAL) Enter this keyword to view a summary listing of the CAM-profile and on the chassis and all line cards.

Defaults None

Command Modes EXEC Privilege

Command History Version 8.2.1.0 Introduced on E-Series ExaScale

Example 1 (summary) FTOS#**show cam-profile summary**
-- Chassis CAM Profile --
CamSize : 40-Meg
 : Current Settings
Profile Name : default
Microcode Name : Default

-- Line card 2 - per Port Pipe --
CamSize : 40-Meg
 : Current Settings
Profile Name : default
Microcode Name : Default
FTOS

Example 2 (profile) FTOS#**show cam-profile**
-- Chassis CAM Profile --
CamSize : 40-Meg
 : Current Settings
Profile Name : default
Microcode Name : Default
L2FIB : 15K entries
 Learn : 1K entries
L2ACL : 5K entries
 System Flow : 102 entries
 Qos : 500 entries
 Frrp : 102 entries
 L2pt : 266 entries
IPv4FIB : 512K 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
MPLS LSP Count : 0K entries
EoMPLS Encap : 0K entries
EoMPLS Decap : 0K entries

-- Line card 2 - per Port Pipe --
CamSize : 40-Meg
 : Current Settings

```

Profile Name      : default
Microcode Name   : Default
L2FIB            : 15K entries
  Learn          : 1K entries
L2ACL            : 5K entries
  System Flow    : 102 entries
  Qos             : 500 entries
  Frrp           : 102 entries
  L2pt           : 266 entries
IPv4FIB          : 512K entries
IPv4ACL          : 16K entries
IPv4Flow         : 24K entries
  Mcast Fib/Acl  : 9K entries
  Pbr            : 1K entries
  Qos            : 10K entries
  System Flow    : 4K entries
-----output truncated-----
FTOS#

```

test cam-profile

E **X** Validate a user-defined CAM-profile template.

Syntax `test cam-profile template`

Parameters `template` Enter the name of the CAM-profile template to validate.

Defaults None

Command Modes CONFIGURATION-CAM-profile-*template*

Command History Version 8.2.1.0 Introduced on E-Series ExaScale

Example





```

FTOS#test cam-profile test
cam-profile 'test' can be applied to the system.
FTOS#test cam-profile Customer002
% Error: 'test cam-profile Customer002 failed. Please check all profile parameters.
FTOS

```

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:    

This chapter includes information relating to the E-Series TeraScale platform. Refer to [Chapter 14, 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 Dell Force10 Technical Assistance Center (TAC) for guidance. For information on contacting Dell Force10 TAC, visit the Dell Force10 website at www.force10networks.com/support

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 FTOS versions 6.3.1.1 and later for the E-Series TeraScale. Refer to [Chapter 14, Content Addressable Memory \(CAM\) for ExaScale](#) for information on the commands for the E-Series ExaScale platform.
- FTOS 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).
- FTOS 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* ipmacacl *number* ecfmacl *number* [vman-qos | vman-dual-qos *number*]

Parameters

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
<i>l2acl number</i> <i>ipv4acl number</i> <i>ipv6acl number</i> , <i>ipv4qos number</i> <i>l2qos number</i> , <i>l2pt number</i> <i>ipmacacl number</i> <i>ecfmacl number</i> [<i>vman-qos</i> <i>vman-dual-qos number</i>]	Allocate space to each CAM region. Enter the CAM profile name followed by the amount to be allotted. The total space allocated must equal 13. The ipv6acl range must be a factor of 2.

Command Modes CONFIGURATION

Command History

Version 8.3.1.0 Added ecfmacl, vman-qos, and vman-dual-qos keywords.

Version 8.2.1.0 Introduced on the S-Series
Version 7.8.1.0 Introduced on the C-Series

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)

C **S** Adjust line card CAM setting to match chassis settings.

This command is deprecated as of FTOS 8.3.1.0

Syntax **cam-acl {chassis |linecard}**

Command Modes EXEC Privilege

Command History
Version 8.3.1.0 COMMAND DEPRECATED
Version 7.8.1.0 Introduced on the C-Series

cam-optimization

C **S** Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

Syntax **cam-optimization [qos]**

Parameters **qos** Optimize CAM usage for Quality of Service (QoS)

Command Modes CONFIGURATION

Defaults Disabled

Command History
Version 8.2.1.0 Introduced on the s-Series
Version 7.8.1.0 Introduced on the C-Series and S-Series

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 *FTOS Configuration Guide* for complete discussion.

cam-profile (Config)

E 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-inacl** 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 IPv6FIB 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 IPv4FIB to IPv4Flow and IPv6FIB.

*microcode *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 bidirectional 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

Command History

Version 8.4.1.0	Added support for l2-switched-pbr microcode.
Version 8.2.1.0	Added support for the ipv4-64k-ipv6 profile.
Version 7.9.1.0	Added support for VRF protocols.
Version 7.5.1.0	Added the l2-ipv4-inacl CAM profile
Version 7.4.2.0	Added the unified-default CAM profile and lag-hash-align microcode
Version 7.4.1.0	Added the lag-hash-mpls microcode
Version 6.5.1.0	Added the eg-default and ipv4-320k CAM profiles
Version 6.3.1.0	Introduced on E-Series

Usage Information

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

Version 7.8.1.0 Introduced on C-Series

Usage Information

The display reflects the settings implemented with the `cam-acl` command.

Example 1 (default)

```
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      :          5
Ipv4Acl    :          6
Ipv6Acl    :          0
Ipv4Qos    :          1
```

**Example 2
(Non-default)**

```

L2Qos      :          1
FTOS#
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-profile

E Display the details of the CAM profiles on the chassis and all line cards.

Syntax `show cam-profile [profile microcode microcode | summary]`

Parameters

- profile* (OPTIONAL) Choose a single CAM profile to display:
- 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-inacl` 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.

- microcode** Choose the microcode to display. 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 bidirectional 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.
 - Enter the keyword **ipv4-64k-ipv6** to specify the CAM profile that provides an alternate to **ipv6-extacl** that redistributes CAM space from the IPv4FIB to IPv4Flow and IPv6FIB.
- 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

Version 8.2.1.0 Added support for **ipv4-64k-ipv6** profile
 Version 7.9.1.0 Added support for VRF protocols.
 Version 6.3.1.0 Introduced on E-Series

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 (summary)

```
FTOS#show cam-profile summary

-- Chassis CAM Profile --
      : Current Settings : Next Boot
Profile Name      : Default           : Default
MicroCode Name   : Default           : Default

      : Current Settings : Next Boot
-- Line card 1 --
Profile Name      : Default           : Default
MicroCode Name   : Default           : Default

      : Current Settings : Next Boot
-- Line card 6 --
Profile Name      : Default           : Default
MicroCode Name   : Default           : Default
FTOS#
```

Example 2 (profile)

```
FTOS#show cam-profile

-- Chassis Cam Profile --

CamSize          : 18-Meg
                  : Current Settings : Next Boot
```

```

Profile Name      : DEFAULT          : DEFAULT
L2FIB            : 32K entries        : 32K entries
L2ACL            : 1K entries          : 1K entries
IPv4FIB          : 256K entries       : 256K entries
IPv4ACL          : 12K entries        : 12K entries
IPv4Flow         : 24K entries        : 24K entries
EgL2ACL         : 1K entries          : 1K entries
EgIPv4ACL        : 1K entries          : 1K entries
Reserved         : 8K entries          : 8K 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
                  : Current Settings : Next Boot
Profile Name      : DEFAULT          : DEFAULT
L2FIB            : 32K entries        : 32K entries
L2ACL            : 1K entries          : 1K entries
IPv4FIB          : 256K entries       : 256K entries
IPv4ACL          : 12K entries        : 12K entries
IPv4Flow         : 24K entries        : 24K entries
EgL2ACL         : 1K entries          : 1K entries
EgIPv4ACL        : 1K entries          : 1K entries
Reserved         : 8K entries          : 8K 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

[E] Display Layer 2, Layer 3, ACL, or all CAM usage statistics.

Syntax show cam-usage [acl | router | switch]

Parameters

- acl (OPTIONAL) Enter this keyword to display Layer 2 and Layer 3 ACL CAM usage.
- router (OPTIONAL) Enter this keyword to display Layer 3 CAM usage.
- switch (OPTIONAL) Enter this keyword to display Layer 2 CAM usage.

Defaults None

Command Modes EXEC Privilege

Command History
Version 6.5.1.0 Introduced on E-Series

Example 1

```

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--

Example 2
(acl)

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	2	1022
		OUT-L3 ACL	1024	0	1024

FTOS#

Example 3
(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
11	1	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 4
(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
11	1	IN-L2 ACL	7152	0	7152
		IN-L2 FIB	32768	1081	31687
		OUT-L2 ACL	0	0	0

```
FTOS#
```

test cam-usage



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.

Range: 0-6 for E-Series, 0-7 for C-Series, 0-7 for S-Series

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. The following examples show some sample output when using the **test cam-usage** command.

**Example 1
(C-Series)**

```
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#
```

```
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#
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 15-35. Output Explanations: test cam-usage (C-Series)

Term	Explanation
Linecard	Lists the line card or line cards that are checked. Entering all shows the status for line cards in the chassis
Portpipe	Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering all shows the status for line cards and port-pipes in the chassis.
CAM Partition	Shows the CAM profile of the CAM
Available CAM	Identifies the amount of CAM space remaining for that profile
Estimated CAM per Port	Estimates the amount of CAM space the listed policy will require.
Status	Indicates whether or not the policy will be allowed in the CAM

Example 2 (S-Series)

```

FTOS#test cam-usage service-policy input LauraIn stack-unit all
Stack-Unit | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port | Status
-----|-----|-----|-----|-----|-----
      0 |      0 | IPv4Flow |      102 |      0 | Allowed
      0 |      1 | IPv4Flow |      102 |      0 | Allowed
FTOS#
!
FTOS#test cam-usage service-policy input LauraIn stack-unit 0 port-set 1
Stack-Unit | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port | Status
-----|-----|-----|-----|-----|-----
      0 |      1 | IPv4Flow |      102 |      0 | Allowed
FTOS#

```

Table 15-36. Output Explanations: test cam-usage (S-Series)

Term	Explanation
Stack-Unit	Lists the stack unit or units that are checked. Entering all shows the status for all stacks.
Portpipe	Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering all shows the status for line cards and port-pipes in the chassis.
CAM Partition	Shows the CAM profile of the CAM
Available CAM	Identifies the amount of CAM space remaining for that profile
Estimated CAM per Port	Estimates the amount of CAM space the listed policy will require.
Status	Indicates whether or not the policy will be allowed in the CAM

CAM IPv4flow Commands

IPv4Flow sub-partitions are supported on E-Series TeraScale platform ET

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 TeraScale. 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)

ET

Configure the amount of CAM space in IPv4flow sub-regions.

This command is deprecated as of FTOS 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)

ET

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

<code>default</code>	Enter the keyword <code>default</code> to reset the IPV4Flow CAM region to its default setting.
<code>multicast-fib <i>value</i></code>	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
<code>pbr <i>value</i></code>	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

qos value Enter the keyword **qos** followed by the number of entries for the QoS sub-region in 1K increments.
Range: 1 to 32 KB
Default: 8 KB

system-flow value Enter the keyword **system-flow** followed by the number of entries for the system-flow sub-region in 1K increments.
Range: 4 to 32 KB
Default: 5 KB

trace-list value Enter the keyword **trace-list** followed by the number of entries for the trace-list sub-region in 1K increments.
Range: 1 to 32 KB
Default: 1 KB

Defaults Refer to Parameters

Command Modes CONFIGURATION

Command History

Version 8.3.1.0	Command deprecated. Replaced by cam-ipv4flow (CONFIGURATION)
Version 6.3.1.0	Introduced on E-Series

Usage Information CAM profile changes take effect after the next chassis reboot.

Related Commands

copy	Save the running configuration.
show cam-ipv4flow	Display the CAM IPv4flow entries.

show cam-ipv4flow

E T Display details about the IPv4Flow sub-regions.

Syntax show cam-ipv4flow

Command Modes EXEC Privilege

Command History

Version 6.3.1.0	Introduced on E-Series
-----------------	------------------------

Example 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*.

Related Commands

[cam-ipv4flow \(CONFIGURATION\)](#)

Configure the amount of CAM space in IPv4flow sub-regions.

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. FTOS 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)

E**T** Re-allocate the amount of space, in percentage, for each Layer 2 ACL CAM sub-partition.

This command is deprecated as of FTOS 8.3.1.0

Syntax cam l2acl {chassis all | linecard *number*} {default | system-flow *percentage* l2acl *percentage* pvst *percentage* qos *percentage* l2pt *percentage* frpp *percentage*}

Command Modes EXEC Privilege

Command History

Version 8.3.1.0	COMMAND DEPRECATED
Version 7.7.1.0	Introduced on E-Series

cam-l2acl (CONFIGURATION)

E**T** 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* frpp *percentage*}

Parameters

default	Enter this keyword to reset the Layer 2 ACL CAM sub-partition space allocations to the default values (Sysflow: 6, L2ACL: 14, PVST: 50, QoS: 12, L2PT: 13, FRRP: 5).
system-flow <i>percentage</i>	Allocate a percentage of the Layer 2 ACL CAM space for system flow entries. Enter the keyword system-flow , and specify the percentage. Range: 5 to 100
l2acl <i>percentage</i>	Allocate a percentage of the Layer 2 ACL CAM space for Layer 2 ACL entries. Enter the keyword l2acl , and specify the percentage. Range: 5 to 95
pvst <i>percentage</i>	Allocate a percentage of the Layer 2 ACL CAM space for PVST+ entries. Enter the keyword pvst and specify the percentage. Range: 5 to 95
qos <i>percentage</i>	Allocate a percentage of the Layer 2 ACL CAM space for QoS entries. Enter the keyword qos , and specify the percentage. Range: 5 to 95
l2pt <i>percentage</i>	Allocate a percentage of the Layer 2 ACL CAM space for L2PT entries. Enter the keyword l2pt , and specify the percentage. Range: 5 to 95
frpp <i>percentage</i>	Allocate a percentage of the Layer 2 ACL CAM space for FRRP entries. Enter the keyword frpp , and specify a percentage. Range: 5 to 95

Command Modes CONFIGURATION

Command History

Version 7.7.1.0	Introduced on E-Series
-----------------	------------------------

Usage Information The PVST sub-partition requires a minimum number of entries when employing PVST+. Refer to the CAM chapter of the FTOS Configuration Guide for the E-Series.

Related Commands [show cam-l2acl](#) Display the percentage of the Layer 2 ACL CAM partition that is allocated to each Layer 2 ACL CAM sub-partition.

show cam-l2acl

E T 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 FTOS 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 FTOS#`show cam-l2acl`

```
-- Chassis Cam L2-ACL --
      Current Settings(in percent)
Sysflow  :      6
L2Acl    :      14
Pvst     :      50
Qos      :      12
L2pt     :      13
Frrp     :      5



-- Line card 1 --
      Current Settings(in percent)
Sysflow  :      6
L2Acl    :      14
Pvst     :      50
Qos      :      12
L2pt     :      13
Frrp     :      5

-- Line card 5 --
      Current Settings(in percent)
Sysflow  :      6
L2Acl    :      14
--More--
```

Related Commands [cam-l2acl \(CONFIGURATION\)](#) Re-allocate the amount of space, in percentage, for each Layer 2 ACL CAM sub-partition.

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

C **E** 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

C **E** Copy an archive file to another location.

Syntax **archive backup** {**flash://CFGARCH_DIR/filename**} {**flash://filepath** | **ftp://userid:password@hostip/filepath**}

Parameters

flash://CFGARCH_DIR/filename	Enter the path directory flash://CFGARCH_DIR/ followed by the name of the file.
flash://filepath	Enter the path flash:// followed by the file path of the local file system to copy your file to the local location.
ftp://userid:password@hostip/filepath	Enter the path ftp:// followed by the FTP remote file system to copy your file to the remote location.

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

C **E** Archive a running configuration.

Syntax **archive config** [**comment comment**]

Parameters	comment <i>comment</i>	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 a acronym for C onfigure A rchive. A maximum of 15 archive files can be stored in this directory.	
Example	<pre>R4_C300#archive config comment 30 characters 3d2h5m: %RPM0-P:CP %CFGARCHIVE-5-RUNNING_CFG_ARCHIVED: Archived running-con- fig as archive_0 configuration archived as archive_0 R4_C300#</pre>	

archive delete

C **E** Delete an archived configuration.

Syntax **archive delete** { *number* | **all** }

Parameters

<i>number</i>	Specify the which archived configuration you want to delete.
all	Enter this keyword to delete all archived configurations.

Defaults None

Command Modes CONFIG ARCHIVE

Command History

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

Example

```
FTOS#archive delete all
Please confirm if you want to proceed [yes/no]:yes
all archives have been removed.
FTOS#
```

configure confirm

C **E** Confirm the replacement of the running configuration when **time** option is used with the **configure replace** command.

Syntax **configure confirm**

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 replace

C **E** 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

configure terminal

C **E** 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
Related Commands	configuration mode exclusive	Enable exclusive configuration.

configuration mode exclusive

  Enable exclusive configuration mode.

Syntax **configuration mode exclusive { auto | manual }**

To negate the configuration, use the **no configuration mode exclusive { auto | manual }** command.

Parameters

auto Enter **auto** to set the exclusive mode to auto.

manual Enter **manual** to set the exclusive mode to manual (the default).

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**

[configure terminal](#)

When configuration is set to manual, use this command to set the exclusive mode.

debug rollback

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

Related Commands [undebug all](#) Disable all debug operations on the system.

maximum number

C E Set the maximum number of archives.

Syntax **maximum {number}**

To return to the default, use the **no maximum {number}** command.

Parameters

<i>number</i>	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 Version 7.6.1.0 Introduced on C-Series and E-Series

Related Commands [show archive](#) Display the archive

show archive

C **E** 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

```
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

C **E** 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

C **E** Show the configuration lock status.

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 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, FTOS 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 FTOS 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

clear line	Reset a terminal line.
configuration mode exclusive	Enable exclusive configuration mode.
send	Send messages to one or all terminal line users.

show run diff

C **E** Display the difference between an archived file and a file.

Syntax **show run diff {flash: | startup-config}**

Parameters

flash:	Enter the archive configuration file using the path [flash://]filename
startup-config	Enter the keywords startup-config to compare the contents of the startup configuration.

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

```

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

C **E**

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 devices 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](#)
- [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 server](#)

clear ip dhcp

  Clear IP address binding from the DHCP server database.

Syntax `clear ip dhcp [binding {address}] | conflict | server statistics]`

Parameters

binding	Enter this keyword to delete all entries in the binding table.
address	Enter the IP address to clear the binding entry for a single IP address.
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

  Identify the clients using a special identifier rather than the hardware address.

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

  Display FTOS debugging messages for DHCP.

Syntax `debug ip dhcp server [events | packets]`

Parameters

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

Command Mode	EXEC Privilege
Default	None
Command History	Version 8.2.1.0 Introduced on C-Series and S-Series.

default-router

C **S** Assign a default gateway to clients based on address pool.

Syntax **default-router** *address* [*address2...address8*]

Parameters *address* Enter the a list of routers that may be the default gateway for clients on the subnet. You may specify up to 8. List them in order of preference.

Command Mode DHCP <POOL>

Default None

Command History Version 8.2.1.0 Introduced on C-Series and S-Series.

disable

C **S** 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

C **S** Assign a DNS server to clients based on address pool.

Syntax **dns-server** *address* [*address2...address8*]



Parameters *address* Enter the a list of DNS servers that may service clients on the subnet. You may list up to 8 servers, in order of preference.

Command Mode DHCP <POOL>

Default None

Command History Version 8.2.1.0 Introduced on C-Series and S-Series.

domain-name

  Assign a domain to clients based on address pool.

Syntax **domain-name** *name*



Parameters *name* Give a name to the group of addresses in a pool.

Command Mode DHCP <POOL>

Default None

Command History Version 8.2.1.0 Introduced on C-Series and S-Series.

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



<i>address</i>	Enter a single address to be excluded from the pool.
<i>low-address</i>	Enter the lowest address in a range of addresses to be excluded from the pool.
<i>high-address</i>	Enter the highest address in a range of addresses to be excluded from the pool.

Command Mode DHCP

Default None

Command History Version 8.2.1.0 Introduced on C-Series and S-Series.

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

C **S** 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.

lease

C **S** Specify a lease time for the addresses in a pool.

Syntax **lease** { *days* [*hours*] [*minutes*] | **infinite** }

Parameters

<i>days</i>	Enter the number of days of the lease. Range: 0-31
<i>hours</i>	Enter the number of hours of the lease. Range: 0-23
<i>minutes</i>	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

C **S** Specify the NetBIOS Windows Internet Naming Service (WINS) name servers, in order of preference, that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients.

Syntax **netbios-name-server** *address* [*address2...address8*]

Parameters *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

C **S** Specify the NetBIOS node type for a Microsoft DHCP client. Dell Force10 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

C **S** 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

C **S** 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

C **S** 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

C **S** Display the DHCP configuration.

Syntax **show ip dhcp configuration [global | pool name]**

Parameters **pool name** Display the configuration for a DHCP pool.
global Display the DHCP configuration for the entire system.

Command Mode EXEC Privilege

Default None

Command History Version 8.2.1.0 Introduced on C-Series and S-Series.

show ip dhcp conflict

C **S** Display the address conflict log.

Syntax `show ip dhcp conflict address`

Parameters *address* Display a particular conflict log entry.

Command Mode EXEC Privilege

Default None

Command History Version 8.2.1.0 Introduced on C-Series and S-Series.

show ip dhcp server

C **S** Display the DHCP server statistics.

Syntax `show ip dhcp server statistics`

Command Mode EXEC Privilege

Default None

Command History Version 8.2.1.0 Introduced on C-Series and S-Series.

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 information-option](#)
- [ip dhcp snooping verify mac-address](#)
- [show ip dhcp snooping](#)

arp inspection

C **E** **S** Enable Dynamic Arp Inspection (DAI) on a VLAN.

Syntax **arp inspection**

Command Modes INTERFACE VLAN

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.

arp inspection-trust

C **E** **S** 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](#) Enable Dynamic ARP Inspection on a VLAN.

clear ip dhcp snooping

C **E** **S** Clear the DHCP snooping 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

C **E** **S** Enable DHCP Snooping globally.

Syntax [no] ip dhcp snooping

Command Modes CONFIGURATION

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 for Layer 2 interfaces.
Version 7.8.1.0	Introduced on C-Series and S-Series on Layer 3 interfaces.

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.

Introduced in FTOS version 7.8.1.0, DHCP Snooping was available for Layer 3 only and dependent on DHCP Relay Agent (ip helper-address). FTOS version 8.2.1.0 extends DHCP Snooping to Layer 2, and you do not have to enable relay agent to snoop on Layer 2 interfaces.

Related Commands

[ip dhcp snooping vlan](#) Enable DHCP Snooping on one or more VLANs.

ip dhcp snooping database

C **E** **S** 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

ip dhcp snooping binding

C **E** **S** Create a static entry in the DHCP binding table.

Syntax **[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number**

Parameters

mac address Enter the keyword **mac** followed by the MAC address of the host to which the server is leasing the IP address.

vlan-id vlan-id Enter the keyword **vlan-id** followed by the VLAN to which the host belongs.
Range: 2-4094

ip ip-address Enter the keyword **ip** followed by the IP address that the server is leasing.

interface type Enter the keyword **interface** followed by the type of interface to which the host is connected.

- For an 10/100 Ethernet interface, enter the keyword **fastethernet**.
- For a Gigabit Ethernet interface, enter the keyword **gigabitethernet**.
- For a SONET interface, enter the keyword **sonet**.
- For a Ten Gigabit Ethernet interface, enter the keyword **tengigabitethernet**.

slot/port Enter the slot and port number of the interface.

lease time Enter the keyword **lease** followed by the amount of time the IP address will be leased.
Range: 1-4294967295

Command Modes EXEC

EXEC Privilege

Default None

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 database renew

C **E** **S** Renew the binding table.

Syntax **ip dhcp snooping database renew**

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

ip dhcp snooping trust

C **E** **S** Configure an interface as trusted.

Syntax [no] ip dhcp snooping trust

Command Modes INTERFACE

Default Untrusted

Command History

Version 8.3.1.0	Introduced on E-Series.
Version 7.8.1.0	Introduced on C-Series and S-Series

ip dhcp source-address-validation

C **E** **S** Enable IP Source Guard.

Syntax [no] ip dhcp source-address-validation [ipmac]

Parameters

ipmac	Enable IP+MAC Source Address Validation (Not available on E-Series).
--------------	--

Command Modes INTERFACE

Default Disabled

Command History

Version 8.3.1.0	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

C **E** **S** Enable DHCP Snooping on one or more VLANs.

Syntax [no] ip dhcp snooping vlan *name*

Parameters

<i>name</i>	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.	
Related Commands	ip dhcp snooping trust	Configure an interface as trusted.

ip dhcp relay information-option

C **E** **S** 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

C **E** **S** 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

C **E** **S**

Validate a DHCP packet's source hardware address against the client hardware address field (CHADDR) in the payload.

Syntax [no] ip dhcp snooping verify mac-address

Command Modes CONFIGURATION

Default Disabled

Command History

Version 8.3.1.0	Introduced on E-Series.
Version 8.2.1.0	Introduced on C-Series and S-Series

Equal Cost Multi-Path

Overview

The characters that appear below command headings indicate support for the associated Dell Force10 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

- E** 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.

Parameters

<i>algorithm-number</i>	Enter the algorithm number. Range: 0 to 47
ecmp <i>hash algorithm value</i>	TeraScale and ExaScale Only: Enter the keyword ecmp followed by the ECMP hash algorithm value. Range: 0 to 47
lag <i>hash algorithm value</i>	TeraScale and ExaScale Only: Enter the keyword lag followed by the LAG hash algorithm value. Range: 0 to 47
nh-ecmp <i>hash algorithm value</i>	(OPTIONAL) Enter the keyword nh-ecmp followed by the ECMP hash algorithm value.
linecard <i>number</i>	(OPTIONAL) TeraScale and ExaScale Only: Enter the keyword linecard 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
ip-sa-mask <i>value</i>	(OPTIONAL) Enter the keyword ip-sa-mask followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF
ip-da-mask <i>value</i>	(OPTIONAL) Enter the keyword ip-da-mask followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF

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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Added nh-ecmp option
Version 7.7.1.1	Added nh-ecmp option
Version 6.5.1.0	Added support for the line card option on TeraScale only
Version 6.3.1.0	Added the support for ECMP and LAG on TeraScale only

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, FTOS maintains bi-directionality with masks set to XX 00 for line card 1 and 00 XX for line card 2 (**ip-sa-mask** and **ip-da-mask**). The mask value must be the same for both line cards when using multiple line cards as ingress (where XX is any value from 00 to FF for both line cards). For example, assume traffic is flowing between line card 1 and line card 2:

hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00

hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, then use the **hash-algorithm** command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

On TeraScale if the keyword **ECMP** or **LAG** is not entered, FTOS assumes it to be common for both. If the keyword **ECMP** or **LAG** is entered separately, both should fall in the range of 0 to 23 or 24 to 47 since compression enable/disable is common for both.

TeraScale and ExaScale support the range 0-47. The default for ExaScale is 24.



0-11	Compression Enabled
	rotate [0 - 11]
12 - 23	Compression Enabled
	shift [0 - 11]
24 - 35	Compression Disabled
	rotate [0 - 11]
36 - 47	Compression Disabled
	shift [0 - 11]

Related Commands

[load-balance \(E-Series\)](#)

Change the traffic balancing method.

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

crc-upper	Uses the upper 32 bits of the key for the hash computation Default: crc-lower
dest-ip	Uses the destination IP for ECMP hashing Default: enabled
lsb	Returns the LSB of the key as the hash Default: crc-lower

Defaults **crc-lower, dest-ip enabled**

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 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 \(C-Series and S-Series\)](#) Change the traffic balancing method.


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

seed value	Enter the keyword followed by the seed value. Range: 0 - 4095
linecard slot	Enter the keyword followed by the line card slot number.
port-set number	Enter the keyword followed by the line card port-pipe number.

Defaults	None
Command Modes	CONFIGURATION
Command History	Version 8.3.1.0 Introduced on E-Series.
Usage Information	<p>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.</p> <p>FTOS provides a CLI-based solution for modifying the hash seed to ensure that on each configured system, the ECMP selection is same. When configured, the same seed is set for ECMP, LAG, and NH, and is used for incoming traffic only.</p> <p> 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.</p>

ip ecmp-deterministic

- E** 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 FTOS sorts the CAM entries.

ipv6 ecmp-deterministic

- E** 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 Version 8.3.1.0 Introduced on E-Series.

Usage Information After enabling IPv6 Deterministic ECMP, traffic loss occurs for a few milliseconds while FTOS 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

E

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

events Enter the keyword **events** to enable debugging of FEFD state changes.

packets Enter the keyword **packets** to enable debugging of FEFD to view information on packets sent and received.

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 Privilege

fefd

E Enable Far-End Failure Detection on an interface.

Syntax **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

E Change the FEFD mode on an interface.

Syntax **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

E Enable FEFD globally on the system.

Syntax **fefd-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.

Default: Normal mode

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 **fefd-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

E Disable FEFD on an interface only. This command overrides the [fefd-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

E Set an interval between control packets.

Syntax **fefd interval seconds**

To return to the default value, enter **no fefd interval**.

Parameters *seconds* Enter a number as the time between FEFD control packets.
Range: 3 to 300 seconds
Default: 15 seconds

Defaults 15 seconds

Command Modes INTERFACE

fefd-global interval

E Configure an interval between FEFD control packets.

Syntax **fefd-global interval** *seconds*

To return to the default value, enter no **fefd-global interval**.

Parameters *seconds* Enter a number as the time between FEFD control packets.
Range: 3 to 300 seconds
Default: 15 seconds

Defaults 15 seconds

Command Modes CONFIGURATION

fefd reset

E 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

E View FEFD status globally or on a specific interface.

Syntax **show fefd** [*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.

Command Modes EXEC
EXEC Privilege

Example

```
FTOS#sh fefd
FEFD is globally 'ON', interval is 10 seconds, mode is 'Aggressive'.
```

```




INTERFACE      MODE           INTERVAL      STATE
                (second)
Gi 5/0         Aggressive    10            Admin Shutdown
Gi 5/1         Aggressive    10            Admin Shutdown
Gi 5/2         Aggressive    10            Admin Shutdown
Gi 5/3         Aggressive    10            Admin Shutdown
Gi 5/4         Aggressive    10            Admin Shutdown
Gi 5/5         Aggressive    10            Admin Shutdown
Gi 5/6         Aggressive    10            Admin Shutdown
Gi 5/7         Aggressive    10            Admin Shutdown
Gi 5/8         Aggressive    10            Admin Shutdown
Gi 5/9         Aggressive    10            Admin Shutdown
Gi 5/10        NA            NA            Locally disabled
Gi 5/11        Aggressive    10            Err-disabled
FTOS#
```

Table 19-37. Description of show fefd display

Field	Description
Interface	Displays the interfaces type and number.
Mode	Displays the mode (aggressive or normal) or NA if the interface contains fefd disable in its configuration.
Interval	Displays the interval between FEFD packets.
State	Displays the state of the interface and can be one of the following: <ul style="list-style-type: none"> • bi-directional (interface is up and connected and seeing neighbor's echoes) • err-disabled (only found when the FEFD mode is aggressive and when the interface has not seen its neighbor's echoes for 3 times the message interval. To reset an interface in this state, use the fefd reset command.) • unknown (only found when FEFD mode is normal) • locally disabled (interface contains the fefd disable command in its configuration) • Admin Shutdown (interface is disabled with the shutdown command)

Force10 Resilient Ring Protocol (FRRP)

Overview

Force10 Resilient Ring Protocol (FRRP) is supported on platforms   

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 frp`
- `debug frp`
- `description`
- `disable`
- `interface`
- `member-vlan`
- `mode`
- `protocol frp`
- `show frp`
- `timer`

Important Points to Remember

- FRRP is media- and speed-independent.
- FRRP is a Dell Force10 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 *ring-id* (Optional) Enter the ring identification number.
Range: 1 to 255

Defaults No default values or behavior

Command Modes EXEC

Command History
Version 8.2.1.0 Introduced for the C-Series
Version 7.5.1.0 Introduced

Example FTOS#clear frrp

```
Clear frrp statistics counter on all ring [confirm] yes
```

```
FTOS#clear frrp 4
```

```
Clear frrp statistics counter for ring 4 [confirm] yes
```

```
FTOS#
```

Usage Information Executing this command, without the optional *ring-id*, will clear statistics counters on all the available rings. FTOS requires a command line confirmation before the command is executed. This commands 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

event Enter the keyword **event** to display debug information related to ring protocol transitions.

packet Enter the keyword **packet** to display brief debug information related to control packets.

detail Enter the keyword **detail** to display detailed debug information related to the entire ring protocol packets.

ring-id (Optional) Enter the ring identification number.
Range: 1 to 255

count Enter the keyword **count** followed by the number of debug outputs.
number Range: 1 to 65534

Defaults Disabled

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 8.2.1.0	Introduced for the C-Series
Version 7.4.1.0	Introduced

Usage Information Since the Resilient Ring Protocol can potentially transmit 20 packets per interface, debug information must be restricted.

description

C **E** Enter an identifying description of the ring.

Syntax **description** *Word*

To remove the ring description, use the **no description** [*Word*] command.

Parameters

<i>Word</i>	Enter a description of the ring. Maximum: 255 characters
-------------	---

Defaults No default values or behavior

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 8.2.1.0	Introduced for the C-Series
Version 7.4.1.0	Introduced

disable

C **E** Disable the Resilient Ring Protocol.

Syntax **disable**

To enable the Resilient Ring Protocol, use the **no disable** command.

Defaults Disabled

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 8.2.1.0	Introduced for the C-Series
Version 7.4.1.0	Introduced

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 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 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 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-frpp)

Command History

Version 8.2.1.0	Introduced for the C-Series
Version 7.4.1.0	Introduced

Usage Information

This command causes the Ring Manager to take ownership of these two ports after the configuration is validated by the IFM. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is, the interface does not belong to any ring.

Related Commands

[show frpp](#) Display the Resilient Ring Protocol configuration information

member-vlan

C **E** Specify the member VLAN identification numbers.

Syntax **member-vlan** { *vlan-range* }

To return to the default, use the **no member-vlan** [*vlan-range*] command.

Parameters

<i>vlan-range</i>	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 8.2.1.0	Introduced for the C-Series
Version 7.4.1.0	Introduced

mode

C **E** Set the Master or Transit mode of the ring.

Syntax **mode** { **master** | **transit** }

To reset the mode, use the **no mode** { **master** | **transit** } command.

Parameters

master	Enter the keyword master to set the Ring node to Master mode.
transit	Enter the keyword transit to set the Ring node to Transit mode.

Defaults Mode None

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 8.2.1.0	Introduced for the C-Series
Version 7.4.1.0	Introduced

protocol frrp

C **E** 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

<i>ring-id</i>	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

C E 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

Example 1 (summary) FTOS#show frrp summary

Ring-ID	State	Mode	Ctrl_Vlan	Member_Vlans
2	UP	Master	2	11-20, 25,27-30
31	UP	Transit	31	40-41
50	Down	Transit	50	32

FTOS#

Example 2 (ring-id) 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
(ring-id
summary)**

```
FTOS#show frrp 2 summary
Ring-ID      State      Mode      Ctrl_Vlan   Member_Vlans
-----
2            Up         Master    2           11-20, 25, 27-30
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.

Parameters

hello-interval *milliseconds* Enter the keyword **hello-interval** followed by the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be enter in increments of 50 milliseconds, for example 50, 100, 150 and so on. If an invalid value is enter, 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**

Version 8.2.1.0 Introduced for the C-Series

Version 7.4.1.0 Introduced

**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.

Force10 Service Agent

Overview

The Force10 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, refer to the **Service Agent (FTSA)** chapter in the *FTOS Configuration Guide*.

All commands in this chapter are supported on C-Series and the E-Series using TeraScale 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
- 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 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.

Related Commands

- [call-home](#) Start FTSA and Enter the FTSA mode.
- [domain-name](#) Specify the domain name to be used for the Administrator's email address.
- [server](#) Configure a recipient.
- [smtp server-address](#) Identify the local SMTP (Simple Mail Transfer Protocol) server from which FTSA email messages will be forwarded.

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

Version 7.6.1.0 Introduced on C-Series
Version 6.3.1.0 Introduced for E-Series

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), FTOS 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 FTOS removes the current FTSA configuration from the running configuration.

Related Commands

call-home	Start FTSA and Enter the FTSA mode.
smtp server-address	Identify the local SMTP server from which FTSA email messages will be forwarded.
admin-email	Enter the Administrator's email address.

case-number

C **E** Specify a case number for the associated policy.

Syntax [no] `case-number word`

Parameters

<i>word</i>	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.
-------------	---

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 <code>config-callhome-policy-name</code> 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.

seq cli-action



Configure an action to execute an FTOS command for one-time operation, triggered as part of the selected action list.

Syntax `seq number cli-action command`

Parameters

<code>seq number</code>	Use the keyword seq followed by a number that FTOS uses to execute the list of actions in numerical order.
<code>command</code>	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 <code>conf-call-home-actionlist-name</code> 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

<code>seq number</code>	Use the keyword seq followed by a number that FTOS uses to execute the list of actions in numerical order.
<code>cli-debug debug-command</code>	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)
<code>time seconds</code>	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**[action-list](#)

Specify an action list for the associated policy and enter the conf-call-home-actionlist-name mode.

seq cli-show

C **E**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**

`seq number` Use the keyword **seq** followed by a number that FTOS uses to execute the list of actions in numerical order.

`cli-show` Enter the keyword **cli-show**, followed by a **show** command.
`show-command` Range: 1-100(max 100 chars including quotes)

`repeat number` Enter the keyword **repeat**, followed by the number of times that the output of the designated **show** command should be collected.
 Range: 1–10 (number of times to collect output)

`delay seconds` Enter the keyword **delay**, followed by the interval, in number of seconds, to wait in collecting instances of the output of the designated **show** command.
 Range: 1–120 (number of seconds to wait between collections)

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

UsageIf the command has spaces, such as **show processes cpu time**, put the words following **show** in double quotes.**Related
Commands**[action-list](#)

Specify an action list for the associated policy and enter the conf-call-home-actionlist-name mode.

contact-address

C **E**

Enter your customer address (up to 100 characters) to be included in type 5 FTSA messages.

Syntax`contact-address 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-email

C **E** Enter a customer email address (up to 60 characters) to be included in type 5 FTSA messages.

Syntax contact-email *address*

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-name

C **E** Enter a customer contact name (up to 25 characters) to be included in type 5 FTSA messages.

Syntax contact-name *name*

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-notes

C **E** 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

C **E** 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

C **E** 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

C **E** Monitor FTSA email messages through the CLI.

Syntax debug 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	Version 7.6.1.0	Introduced on C-Series
	Version 6.3.1.0	Introduced for E-Series

Related Commands [show debugging](#) Display the status of FTSA (call-home) debugging.

default-action

C **E** Select the information collection action that matches the equivalent test group.

Syntax default-action {hardware | software | exception}

Parameters

hardware	Enter the keyword hardware to collect hardware information. Refer to the FTOS Configuration Guide for the list of actions executed by this keyword.
software	Enter the keyword software to collect software information. Refer to the FTOS Configuration Guide for the list of actions executed by this keyword.
exception	Enter the keyword exception to collect exception information. Refer to the FTOS Configuration Guide for the list of actions executed by this keyword.

Defaults No default behavior or values

Command Mode CALL-HOME ACTION-LIST

Command History	Version 7.7.1.0	Introduced on C-Series and E-Series
------------------------	-----------------	-------------------------------------

Usage Information Starting with FTOS 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

C **E** Invoke one of three preset system-monitoring test groups.

Syntax default-test {hardware | software | exception}

Parameters

hardware	Enter the keyword hardware to monitor hardware conditions. Refer to the FTOS Configuration Guide for the list of conditions monitored by this keyword.
software	Enter the keyword software to monitor software conditions. Refer to the FTOS Configuration Guide for the list of conditions monitored by this keyword.
exception	Enter the keyword exception to monitor the exceptions events. Refer to the FTOS Configuration Guide for the list of conditions monitored by this keyword.

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 <code>policy-test-list</code> command puts you in the <code>config-callhome-testlist</code> mode, where you use this command to invoke one of three possible test groups. FTOS monitors the system for any event in the selected test group. If such an event occurs, FTOS invokes the action you define using the <code>default-action</code> 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 <code>config-callhome-testlist-name</code> mode.

description

C **E** Enter a description for the Call Home mode.

Syntax `description { description }`

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

Parameters *description* Enter a description to identify the Call Home mode(80 characters maximum).

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

C **E** 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 *domain name* Enter the keyword `domain-name` followed by the complete domain name of the Administrator's email address, for example, `domain_name.com`.

Defaults The domain name specified in the `admin-email` command



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 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	Version 7.6.1.0	Introduced on C-Series
	Version 6.3.1.0	Introduced for E-Series

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.

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.

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	Identify the SMTP server.
server	Configure each recipient.

encrypt



Specify email encryption for this server.

Syntax encrypt

To remove email encryption for this server, use the **no encrypt** command.

Defaults no 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

Usage Information 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.

Related Commands

call-home	Start FTSA and Enter the FTSA mode.
keyadd	Add a public key to the server.
server	Configure each recipient.

frequency

C **E**

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

C **E**

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 Force10 server associated with the default Dell Force10 Support recipient has a public key that is shipped as part of FTOS, so you do not need to enter the key's filename for that server. However, if the Dell Force10 public key is changed, a notification will be made to download the new key from the Dell Force10 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

<code>delay 60–1440</code>	(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.
<code>severity 0–7</code>	(OPTIONAL) Enter the keyword severity followed by the error severity level entered in the system log that should be collected into the FTSA message.
<code>filter word</code>	(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.

Related Commands

call-home	Start FTSA and Enter the FTSA mode.
log-only	Select the information collection action that matches the selected test group.
logging buffered	Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.
show logging	Display the logging settings and system messages logged to the internal buffer of the switch.

log-only



Execute this command if you want FTSA data to be collected in a local log rather than to be sent to configured FTSA recipients.

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 mail 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

- [call-home](#) Start FTSA and Enter the FTSA mode.
- [default-action](#) Select the information collection action that matches the selected test group.

match

C **E**

This command enables you to execute the configured action list based on one of three test list criteria.

Syntax match {any | all | simultaneous}

Parameters

all Entering this keyword will require that all conditions in the test list be matched in order to execute the associated action list.

any 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.

simultaneous Entering this keyword indicates that the test conditions must be matched in the same sampling period in order to execute the associated action list.

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

- [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.

message-format

C **E**

Set the format of an action-list (type-5) email message.

Syntax message-format {xml | text}

Parameters

xml Enter the keyword **xml** to have the type-5 mail generated in XML format.

text Enter the keyword **text** to have the type-5 mail generated in text format.

Defaults 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>
<F10_info>
<policy_name>xxxxxxx</policy_name>
<case_number>xxxxxx</case_number>
<pr_number>xxxxxx</pr_number>
</F10_info>

  <action_list_name> name </action_list_name>
  <test_list_match>
<match> keyword : value </match>
<match> cpu-5-min : 98% </match>
<match> etc... </match>
  </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	Version 7.8.1.0	Concurrent policies changed from three to five
	Version 7.7.1.0	Introduced on C-Series and E-Series
Usage Information	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 <code>policy-test-list</code> command. Choose the associated action to perform with the <code>policy-action-list</code> command.	
Related Commands	call-home	Start FTSA and Enter the FTSA mode.
	case-number	Specify a case number for the associated policy
	default-test	Invoke one of three system-monitoring test groups.
	policy-action-list	Name a policy action list and enter the config-callhome-actionlist-name mode.
	policy-test-list	Name a policy test list and enter the config-callhome-testlist-name mode.
	pr-number	Create an entry for a PR number in policy mode. The PR number is the issue identifier (bug ID) maintained by Dell Force10, and is associated with the test list.
	test-list	Enter the name of a configured policy test list to be associated with the selected policy.

policy-action-list

C **E** 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 `word` Enter the name (up to 20 characters) of the new policy test list.

Defaults No default behavior or values

Command Modes conf-callhome

Command History Version 7.7.1.0 Introduced on C-Series and E-Series

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

C **E** Name a policy test list and enter the config-callhome-testlist-name mode.

Syntax `policy-test-list word`

Parameters `word` Enter the name (up to 20 characters) of the new policy test list.

Defaults No default behavior or values

Command Mode conf-callhome

Command History Version 7.7.1.0 Introduced on C-Series and E-Series

Usage Information 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

C **E**

Enter a PR (problem report) number associated with the selected policy. The number is the issue identifier (bug ID) maintained by Dell Force10.

Syntax `pr-number number`

Parameters `number` Enter a 5-digit PR number, as supplied by Dell Force10.

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

C **E**

Enter the email address of the recipient associated with the selected server name.

Syntax `recipient email address`

To remove the recipient, use the `no recipient email address` command.

Parameters `email address` Enter the recipient's full email address. For example, `name@domain_name.com`.

Defaults `ftsa@force10networks.com` (associated with the Dell Force10 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

<i>percentage</i>	Enter a CPU utilization percentage. Range: 0–100
<i>cpu</i>	Select a CPU: CP, LP, RP1, or RP2
<i>rpm-any</i>	Monitor all RPM CPUs for the <code>run-cpu</code> condition (CP, RP1, and RP2)

Default None

Command Mode CALL-HOME POLICY

Command History

Version 8.2.1.0	Added variable <i>cpu</i> , and keyword <i>rpm-any</i> . Keyword <i>more-than</i> changed to <i>greater-than</i> . Keyword <i>unconditional</i> removed.
Version 7.8.1.0	Introduced on C-Series and E-Series

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 [policy](#) Create a policy with a name and enter config-callhome-policy-name mode.

sample-rate



Set the sampling interval for how often to execute the configured test condition.

Syntax `sample-rate number`

Parameters

<i>number</i>	Set the sampling interval for how often to execute the configured test condition. Range: 1–1440 (minutes)
---------------	--

Default 1 (one minute)

Command Mode	conf-callhome-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.
	policy-test-list	Name a policy test list and enter the config-callhome-actionlist-name mode.
	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 message-text (deprecated)	Search for a stated value in the output of the designated SHOW command or message type.
	test-limit	Set the number of times that the test list should be executed.

server

C **E** Use this command to create a server name to be associated with a particular recipient.

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 Force10

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 Force10 server name is configured for FTSA messages to be sent by default to Dell Force10 Support at `ftsa@force10networks.com`. If you want to change that address, enter the command `server Force10`. You will be placed at that server-specific prompt (`conf-callhome-Force10`), where you would then use the `recipient` command to enter a new address.

In addition to modifying the Dell Force10 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	call-home	Start FTSA and Enter the FTSA mode.
	enable	Enable FTSA (call home) email for the selected recipient.
	recipient	Enter the recipient's email address.
	enable	Enable FTSA (call home) email for the selected recipient.

show configuration

C **E** Display the FTSA (call-home) configuration.

Syntax show configuration

Defaults No default behavior or values

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

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 FTOSDefaultPublicKey
  no encrypt
  enable
FTOS(conf-callhome)#
```

show debugging

C **E** Display the status of FTSA (call-home) debugging.

Syntax show debugging

Defaults No default behavior or values

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

Example

```
FTOS(conf-callhome)#show debugging

CALLHOME:
  Callhome service debugging is on

FTOS(conf-callhome)#
```

Related Commands	debug call-home	Monitor FTSA email messages through the CLI.
-------------------------	---------------------------------	--

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

```
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

[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
Default: 25

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)

C **E** Configure an action to collect and compare multiple samples of a statistic.

Syntax `test-condition statistic operator sample { cpu | rpm-any } number`

Parameters	<code>test-condition <i>statistic</i></code>	Enter the keyword test-condition , followed by one of the following statistic request types: <ul style="list-style-type: none"> <code>cpu-1-min</code>: Average CPU utilization for 1 minute <code>cpu-5-min</code>: Average CPU utilization for 5 minutes <code>interface-bit-rate {input output} slot#</code>: Instantaneous bit rate on a given line card <code>interface-crc <i>interface</i></code>: Number of CRC errors on a given interface <code>interface-rate {input output} <i>interface</i></code>: Packet rate on a given interface <code>interface-throttles <i>interface</i></code>: Number of throttles on an interface <code>memory-free</code>: Free system memory <code>memory-free-percent</code>: Free system memory free in percentage <code>memory-used</code>: System memory used <code>memory-used-percent</code>: System memory used in percentage <code>wred-drops <i>interface</i></code>: Number of WRED drops on an interface (E-Series only)
	<code><i>operator</i></code>	Enter one of the following Boolean comparison operators: decrease , equal-to , greater-than , increase , less-than , not-equal-to , no-change .
	<code>sample <i>number</i></code>	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. Range: 2–100 Default: 2
	<code><i>cpu</i> <i>rpm-any</i></code>	Enter the processor that will be tested: <code>cp</code> , <code>lp</code> , <code>rp1</code> , <code>rp2</code> , 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

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.

Examples

```
FTOS(conf-call-home-testlist-test)#test-condition cpu-1-min increase number?
<0-100> Enter the boolean comparison value
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 ?
<0-100> Enter the boolean comparison value
FTOS(conf-callhome-testlist-test)#test-condition cpu-5-min decrease 10
```

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-callhome-testlist-test)#test-condition interface-bit-rate ?
input Input interface
output Output interface
FTOS(conf-callhome-testlist-test)#test-condition interface-bit-rate input ?
<0-3> Slot number
FTOS(conf-callhome-testlist-test)#test-condition interface-bit-rate input 1
decrease ?
<0-10000> Enter the boolean comparison value in mbits/sec
FTOS(conf-callhome-testlist-test)#test-condition interface-bit-rate input 1
decrease 10 ?
sample The time interval to check the condition
<cr>
FTOS(conf-callhome-testlist-test)#test-condition interface-bit-rate input 1
decrease 10 sample ?
<2-100> Enter the sample value (default = 2)
FTOS(conf-callhome-testlist-test)#test-condition interface-bit-rate input 1
decrease 10 sample 2
```

Here are other examples of test-condition configuration statements.

```
FTOS(conf-call-home-testlist-test)#test-condition interface-crc 1 decrease
number 90 sample 5
FTOS(conf-call-home-testlist-test)#test-condition memory-free-percent
no-change sample 4
```

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)

- C** **E** 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 <i>statistic</i>	Enter the keyword test-condition , followed by one of the following statistic request types: <ul style="list-style-type: none"> • 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 <i>interface</i>: Number of CRC errors on a given interface • interface-rate <i>interface</i>: Packet rate on a given interface • interface-throttles <i>interface</i>: 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 <i>interface</i>: Number of WRED drops on an interface (E-Series only)
	<i>operator</i>	Enter one of the following Boolean comparison operators: decrease , equal-to , greater-than , increase , less-than , not-equal-to , no-change .
	number <i>value</i>	Enter the keyword number , followed by an integer to be the comparison value to the designated statistic, in the range pertinent to the statistic.
	<i>cpu</i> 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 FTOS 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. FTOS displays the acceptable range, as shown below

Examples

```
FTOS(conf-callhome-testlist-test)#test-condition cpu-5-min greater-than ?
number                               The boolean comparison value
FTOS(conf-callhome-testlist-test)#test-condition cpu-5-min greater-than num-
ber ?
<0-100>                               Enter the boolean comparison value
FTOS(conf-callhome-testlist-test)#test-condition cpu-5-min greater-than num-
ber 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 \(comparing samples\)](#) Collect multiple samples of a statistic and compare them using the specified comparator and hurdle value.
- [test-condition message-text \(deprecated\)](#) Search for a stated value in the output of the designated **show** command or message type.

test-condition message-text (deprecated)

C **E** 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 FTOS.

Syntax test-condition message-text command *string* equal-to string *string*

Parameters

- test-condition message-text command *string*** Enter the keywords test-condition message-text command, and then for *string*, enter a **show** command in quotes.
Range: 1–64 characters
- equal-to string *string*** Enter the keywords equal-to string, and then for *string*, enter the text to search for in the show command designated above.
Range: 1–64 characters

Defaults none

Command Modes conf-callhome-testlist-test

**Command
History**

- Version 8.2.1.0 Deprecated.
- Version 7.8.1.0 Introduced on C-Series and E-Series

**Usage
Information**

In the following example:

- 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

```

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</ifAd-
minStatus>

```

**Related
Commands**



[dampen](#) Set a delay before sampling for a test condition again after it has been matched.

[test-condition \(comparing samples\)](#) Configure an action to collect and compare multiple samples of a statistic.

[test-condition \(comparison to a value\)](#) Collect a statistic and compare it to a stated value.

[test-limit](#) Set the number of times that the test list that should be executed.

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**

[dampen](#) Set a delay before sampling for a test condition again after it has been matched.

[test-condition \(comparing samples\)](#) Configure an action to collect and compare multiple samples of a statistic.

[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.

[sample-rate](#) Set the sampling interval for how often to execute the configured test condition.

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 config-callhome-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. FTOS monitors the system for any event in the selected test group. If such an event occurs, FTOS invokes the action you defined using the **default-action** command and then associate in this policy with the **action-list** command.

Table 21-38. FTSA Test Sets

Hardware test set	Software test set	Exception test set
SFM status transition from active to other state	SWP Timeout	CPU usage more than 85%
Line card transition from active to other state	IPC Timeout	System crash
Port-pipe error or transition to down	IRC timeout	Task crash
RPM status transition from active to other state	CPU usage more than 85%	Dump, reload due to error, RPM failover due to error
PEM transition from up to other state	Memory usage more than 85%	
AC power supply transition from up to other state		
Fan tray down or individual fan down		
Overtemp of any item listed in SHOW environment		
Over/under-voltage of any item listed in show environment		

Related Commands

- [action-list](#) Specify a policy action list for the associated policy and enter the conf-call-home-actionlist-name mode.
- [case-number](#) Specify a case number for the associated policy.
- [dampen](#) Set a delay before sampling for a test condition again after it has been matched.
- [policy](#) Create a policy name and enter config-callhome-policy-name mode.
- [policy-test-list](#) Name a policy test list and enter the config-callhome-testlist-name mode.

GARP VLAN Registration (GVRP)

Overview

GARP VLAN Registration (GVRP) is supported on platforms [C](#), [E](#), and [S](#)

Commands

The GVRP commands are:

- [clear gvrp statistics](#)
- [bpdu-destination-mac-address](#)
- [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 (unspecified) with a specific VLAN ID and a specific port.
- On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
- GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
- GVRP updates are not sent to any blocked Spanning Tree Protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- GVRP operates only on ports that are in the STP forwarding state. If GVRP is enabled, a port that changes to the STP forwarding state automatically begins to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.
- VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
- GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge needs to classify and analyze packets by VLAN protocols, you must manually configure protocol-based VLANs, and simply rely on GVRP for VLAN updates. But if the local bridge needs to know only how to reach a given VLAN, then GVRP provides all necessary information.
- The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

clear gvrp statistics

C **E** **S** 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 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 EXEC

Command History Version 7.6.1.0 Introduced on C, E, and S-Series

Related Commands [show gvrp statistics](#) Display the GVRP statistics

debug gvrp

C **E** **S**

Enable debugging on GVRP.

Syntax **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.

pdu Enter the keyword **pdu** followed one of the following 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 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 Disabled

Command Modes EXEC Privilege

Command History Version 7.6.1.0 Introduced on C, E, and S-Series

disable

C **E** **S**

Globally disable GVRP.

Syntax **disable**

To re-enable GVRP, use the **no disable** command.

Defaults Enabled

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

garp timers

C E S

Set the intervals (in milliseconds) for sending GARP messages.

Syntax

garp timers {**join** | **leave** | **leave-all**}

To return to the previous setting, use the **no garp timers** {**join** | **leave** | **leave-all**} command.

Parameters

- join** Enter the keyword **join** followed by the number of milliseconds to configure the join time.
Range: 100-2147483647 milliseconds
Default: 200 milliseconds
Note: Designate the milliseconds in multiples of 100
- leave** Enter the keyword **leave** followed by the number of milliseconds to configure the leave time.
Range: 100-2147483647 milliseconds
Default: 600 milliseconds
Note: Designate the milliseconds in multiples of 100
- leave-all** Enter the keyword **leave-all** followed by the number of milliseconds to configure the leave-all time.
Range: 100-2147483647 milliseconds
Default: 1000 milliseconds
Note: Designate the milliseconds in multiples of 100

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

C **E** **S**

Enable GVRP on physical interfaces and LAGs.

Syntax `gvrp enable`

To disable GVRP on the interface, use the **no gvrp enable** command.

Defaults Disabled

Command Modes CONFIGURATION-INTERFACE

Command History Version 7.6.1.0 Introduced on C, E, and S-Series

Related Commands [disable](#) Globally disable GVRP.

gvrp registration

C **E** **S**

Configure the GVRP register type.

Syntax `gvrp registration {fixed | normal | forbidden}`

To return to the default, use the **gvrp register normal** command.

Parameters

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

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

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

Defaults Default registration is **normal**

Command Modes CONFIGURATION-INTERFACE

Command History Version 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

C **E** **S** Access GVRP protocol — (config-gvrp)#.

Syntax **protocol gvrp**

Defaults Disabled

Command Modes CONFIGURATION

Command History Version 7.6.1.0 Introduced on C, E, and S-Series

Related Commands [disable](#) Globally disable GVRP.

show config

C **E** **S** 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

C **E** **S** 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

```
FTOS#show garp timers
GARP Timers      Value (milliseconds)
-----
Join Timer       200
Leave Timer       600
LeaveAll Timer    10000
FTOS#
```

Related Commands [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 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

EXEC
EXEC Privilege

Command History

Version 7.6.1.0 Introduced on C, E, and S-Series

Example

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

Port	GVRP Status	Edge-Port
Gi 3/0	Disabled	No
Gi 3/1	Disabled	No
Gi 3/2	Enabled	No
Gi 3/3	Disabled	No
Gi 3/4	Disabled	No
Gi 3/5	Disabled	No
Gi 3/6	Disabled	No
Gi 3/7	Disabled	No
Gi 3/8	Disabled	No

```
R3#show gvrp brief
```

Usage Information

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

GVRP Participants running on <port_list>

to

GVRP Participants running on no ports

Related Commands

[show gvrp statistics](#) Display the GVRP statistics

show gvrp statistics

C **E** **S** 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 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.

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 7.6.1.0 Introduced on C, E, and S-Series

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 Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
Failed Registrations: 0
FTOS#
```

Usage Information

Invalid messages/attributes skipped can occur in the following cases:

- The incoming GVRP PDU has an incorrect length.
- “End of PDU” was reached before the complete attribute could be parsed.
- The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01).
- The attribute that was being parsed had an invalid attribute length.
- The attribute that was being parsed had an invalid GARP event.

- The attribute that was being parsed had an invalid VLAN ID. The valid range is 1 - 4095.

A failed registration can occur for the following reasons:

- Join requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state).
- An entry for a new GVRP VLAN could not be created in the GVRP database.

**Related
Commands**

[show gvrp](#)

Display the GVRP configuration

High Availability (HA)

Overview

High Availability (HA) in FTOS 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**

FTOS 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 (refer to the [redundancy protocol](#) command).

High Availability is supported on E-Series ExaScale **E**_x with FTOS 8.1.1.0. and later.

Commands

The HA commands available in FTOS 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

E 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 Version 8.2.1.0 Introduced

Usage Information The patch filename includes the FTOS 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 FTOS 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

E 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

<code>process</code>	Configure a process to be restartable.
<code>count number</code>	Enter the number of times a process can restart within the configured period. Range: 1-3 Default: 3
<code>period minutes</code>	Enter the amount of time within which the process can restart <i>count</i> 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 Version 8.4.1.0 Introduced on E-Series.

Related Commands [show processes restartable](#) Display the processes and tasks configured for restartability.

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

Command History

Version 8.3.1.0 Added the **all** option

Version 8.1.1.0 Introduced on E-Series ExaScale
 Version 7.6.1.0 Introduced on E-Series

Usage Information

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.

redundancy force-failover



Force the secondary RPM to become primary RPM or or force the backup unit in an S-Series stacking configuration to become the management unit. This command can also be used to upgrade the software on one RPM from the other when the other has been loaded with the upgraded software.

Syntax **redundancy force-failover {rpm | stack-unit}**

Parameters

rpm Enter the keyword **rpm** to force the secondary RPM to become the primary RPM.
stack-unit Enter the keyword **stack-unit** to force the backup unit in the stack to become the management unit (S-Series only).
Note: Using this command will reboot the stack-unit.

Defaults Not configured.

Command Modes EXEC Privilege

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

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. 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.

Note: On the S-Series, using this command will reboot the stack-unit.

Example

```
FTOS#redundancy force-failover rpm
Peer RPM's SW version is different but HA compatible.
Failover can be done by warm or hitless upgrade.
All linecards will be reset during warm upgrade.
```

```
Specify hitless upgrade or warm upgrade [confirm hitless/warm]:hitless
Proceed with warm upgrade [confirm yes/no]:
```

redundancy primary

C **E** Set an RPM as the primary RPM.

Syntax **redundancy primary [rpm0 | rpm1]**

To delete a configuration, enter **no redundancy primary**.

Parameters

rpm0 Enter the keyword **rpm0** to set the RPM in slot R0 as the primary RPM.

rpm1 Enter the keyword **rpm1** to set the RPM in slot R1 as the primary RPM.

Defaults The RPM in slot R0 is the Primary RPM.

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

redundancy protocol

C **E** Enable hitless protocols.

Syntax **redundancy protocol {lacp | xstp}**

To disable a hitless protocol, enter **no redundancy protocol {lacp | xstp}**.

Parameters

lacp Enter the keyword **lacp** to make LACP hitless.

xstp Enter the keyword **xstp** to invoke hitless STP (all STP modes—MSTP, PVST+, RSTP, STP).

Note: On the C-Series, hitless STP is available only for MSTP, PVST+, and RSPT.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 8.2.1.0 Introduced on C-Series

Version 8.1.1.0 Introduced on E-Series ExaScale

Version 7.6.1.0 Introduced on E-Series

Related Commands

[show lacp](#) Display the lacp configuration

[show redundancy](#) Display the current redundancy configuration.

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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.6.1.0	Introduced on E-Series

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

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

Command History

Version 7.5.1.0	Introduced on C-Series Only
-----------------	-----------------------------

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

```
FTOS#show sfm all

Switch Fabric State:  up

-- Switch Fabric Modules --
Slot  Status
-----
  0    active
  1    active

FTOS#configure
FTOS(conf)#redundancy sfm standby
Taking secondary SFM offline...
!
FTOS(conf)#do show sfm all
```



```

Switch Fabric State: up

-- Switch Fabric Modules --
Slot  Status
-----
  0    active
  1    standby

FTOS(conf)#no redundancy sfm
Taking secondary SFM online...
!
FTOS(conf)#do show sfm all

Switch Fabric State: up

-- Switch Fabric Modules --
Slot  Status
-----
  0    active
  1    active

```

**Related
Commands**

- [show sfm](#) Display the SFM status
- [show switch links](#) Display the switch fabric backplane or internal status.

redundancy synchronize

C **E** **S** Manually synchronize data once between the Primary RPM and the Secondary RPM.

Syntax `redundancy synchronize [full | persistent-data | system-data]`

Parameters

- full** Enter the keyword **full** to synchronize all data.
- persistent-data** Enter the keywords **persistent-data** to synchronize the startup configuration between RPMs.
- system-data** Enter the keywords **system-data** to synchronize persistent-data and the running configuration file, event log, SFM and line card states.

Defaults Not configured.

Command Modes EXEC Privilege

**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

show patch

E Display the system patches loaded with the In-Service Modular Hot Fix Command.

Syntax `show patch`

Command Modes EXEC

Command History Version 8.2.1.0 Introduced on E-Series

Related Commands [patch flash://RUNTIME_PATCH_DIR](#) Insert an In-Service Modular Hot-Fix patch.

show processes restartable

E Display the processes and tasks configured for restartability.

Syntax `show processes restartable [history]`

Parameters `history` Display the last time the restartable processes crashed.

Command Modes EXEC Privilege

Command History Version 8.4.1.0 Introduced on E-Series

Example FTOS#`sho processes restartable`

```
-----
Process name      State      How many times restarted      Timestamp last restarted
-----
radius            enabled    0                               [-]
tacplus           enabled    0                               [-]
-----
```

FTOS#`show processes restartable history`

```
-----
Process name      Timestamp last crashed
-----
radius            [5/23/2001 10:11:47]
-----
```

Related Commands [process restartable](#)

show redundancy

C **E** **S** Display the current redundancy configuration.

Syntax **show redundancy**

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
Version 7.6.1.0	Introduced on E-Series

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: --
-----
Line Card Config:    succeeded Jul 13 2007 21:28:53
Start-up Config:     succeeded Jul 13 2007 21:28:53
SFM Config State:    succeeded Jul 13 2007 21:28:53
Runtime Event Log:   succeeded Jul 13 2007 21:28:53
Running Config:      succeeded Jul 13 2007 21:28:53
FTOS#
```

Table 23-39. show redundancy Command Example Fields

Field	Description
RPM Status	<p>Displays the following information:</p> <ul style="list-style-type: none"> Slot number of the RPM Whether the RPM is Primary or Standby The state of the RPM: Active, Standby, Booting, or Offline Whether the link to the second RPM is up or down.
PEER RPM Status	Displays the state of the second RPM, if present
RPM Redundancy Configuration	<p>Displays the following information:</p> <ul style="list-style-type: none"> 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	<p>Displays the following information:</p> <ul style="list-style-type: none"> 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	<p>Displays the data sync information and the timestamp for the data sync:</p> <ul style="list-style-type: none"> 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. <p>This field only appears when you enter the command from the Primary RPM.</p>

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

- FTOS 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

C **E** **S** 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 an 100/1000 Base-T 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.

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 legacy command

Usage Information

IGMP commands accept *only* non-VLAN interfaces—specifying VLAN will not yield a results.

debug ip igmp

C **E** **S** 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:
- 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 255 for TeraScale, 1 to 512 for ExaScale
 - For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. This keyword is only available on the E-Series and C-Series.
 - For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults	Disabled
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 legacy command
Usage Information	IGMP commands accept <i>only</i> non-VLAN interfaces—specifying a VLAN will not yield results. This command displays packets for IGMP and IGMP Snooping.

ip igmp access-group

C **E** **S** 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 Version 7.8.1.0 Introduced on C-Series and S-Series
Version 7.6.1.0 Introduced on E-Series

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

C **E** **S** Use this feature to limit the number of IGMP groups that can be joined in a second.

Syntax ip igmp group-join-limit *number*

Parameters *number* Enter the number of IGMP groups permitted to join in a second.
Range: 1 to 10000

Defaults No default values or behavior

Command Modes CONFIGURATION (conf-if-*interface-slot/port*)

Command History Version 7.8.1.0 Introduced on C-Series and S-Series
Version 7.6.1.0 Introduced on E-Series

ip igmp immediate-leave

C **E** **S** 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 group-list *prefix-list-name* Enter the keyword **group-list** followed by a string up to 16 characters long of the *prefix-list-name*.

Defaults Not configured

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

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

C **E** **S** 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

C **E** **S**

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

<i>seconds</i>	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

C **E** **S**

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

<i>std-access-list</i>	Specify the standard IP access list that contains the mapping rules for multicast groups.
<i>source-address</i>	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 joins; 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.

Note: A group in **include** mode must have at least one source address defined.

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

Version 7.5.1.0 Expanded to support the **exclude** and **include** options
E-Series legacy command

Usage Information

A group in the **include** mode should have at least one source address defined. In **exclude** mode if no source address is specified, FTOS implicitly assumes all sources are included. If neither **include** or **exclude** is specified, FTOS 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

[show ip igmp groups](#) Display IGMP group information

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

C **E** **S** View the IGMP groups.

Syntax show ip igmp groups [*group-address* [detail] | detail | *interface* [*group-address* [detail]]]

Parameters	<i>group-address</i>	(OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
	<i>interface</i>	(OPTIONAL) Enter the interface type and slot/port information: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 E-Series Range: 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.
	<i>detail</i>	(OPTIONAL) Enter the keyword detail to display the IGMPv3 source information.

Command Modes EXEC
EXEC Privilege

Command History	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

```
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#
```

Table 24-40. show ip igmp groups Command Example Fields

Field	Description
Group Address	Lists the multicast address for the IGMP group.
Interface	Lists the interface type, slot and port number.
Uptime	Displays the amount of time the group has been operational.
Expires	Displays the amount of time until the entry expires.
Last Reporter	Displays the IP address of the last host to be a member of the IGMP group.

show ip igmp interface

C **E** **S** 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 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 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.

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
E-Series legacy command

Usage Information

IGMP commands accept *only* non-VLAN interfaces—specifying VLAN will not yield a results.

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
FTOS#
```

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 7.8.1.0 Introduced on C-Series and S-Series
Version 7.7.1.0 Introduced on E-Series

Related Commands [ip igmp ssm-map](#) Use a statically configured list to translate (*,G) memberships to (S,G) memberships.

IGMP Snooping Commands

FTOS supports IGMP Snooping version 2 and 3 on all Dell Force10 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

- FTOS supports version 1, version 2, and version 3 hosts.
- FTOS IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac-address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 FIB.
- FTOS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- FTOS 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

C **E** **S** 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

C **E** **S** 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

Version 8.2.1.0	Introduced on the C-Series and S-Series.
Version 7.7.1.1	Introduced on E-Series.

ip igmp snooping last-member-query-interval

C **E** **S** 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

<i>milliseconds</i>	Enter the interval in milliseconds. Default: 1000 milliseconds Range: 100 to 65535
---------------------	--

Defaults 1000 milliseconds

Command Modes 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

ip igmp snooping mrouter

C **E** **S** Statically configure a VLAN member port as a multicast router interface.

Syntax ip igmp snooping mrouter interface *interface*

To delete a specific multicast router interface, use the no igmp snooping mrouter interface *interface* command.

Parameters

interface <i>interface</i>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none">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 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.For a Port Channel interface, enter the keyword port-channel followed by a number: C-Series and S-Series Range: 1-128 E-Series Range: 1 to 255 for TeraScale and 1 to 512 for ExaScale.
----------------------------	---

Defaults Not configured

Command Modes	INTERFACE VLAN—(conf-if-vl- <i>n</i>)	
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	FTOS provides the capability of statically configuring interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the <code>ip igmp snooping mrouter interface</code> command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.	

ip igmp snooping querier

C **E** **S** Enable IGMP querier processing for the VLAN interface.

Syntax ip igmp snooping querier

To disable IGMP querier processing for the VLAN interface, enter `no ip igmp snooping querier` command.

Defaults Not configured

Command Modes INTERFACE VLAN—(conf-if-vl-*n*)

Command History

Version 7.6.1.0	Introduced on S-Series
Version 7.5.1.0	Introduced on C-Series
E-Series legacy command	

Usage Information This command enables the IGMP switch to send General Queries periodically. This is useful when there is no multicast router present in the VLAN because the multicast traffic does not need to be routed. An IP address must be assigned to the VLAN interface for the switch to act as a querier for this VLAN.

show ip igmp snooping mrouter

C **E** **S** Display multicast router interfaces.

Syntax show ip igmp snooping mrouter [vlan *number*]

Parameters

vlan <i>number</i>	Enter the keyword vlan followed by the vlan number. Range: 1-4094
--------------------	--

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
E-Series legacy command

Example

```
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 Force10 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 with FTOS 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](#)
- [keepalive](#)
- [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] vrid | vrf instance}] | learning-limit]`

Parameters

interface (OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface:

- For a 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 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.
[vrf instance] 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 8.4.1.0	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
FTOS#clear counters
Clear counters on all interfaces [confirm]

Related Commands

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.

clear dampening

C **E** **S** 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 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.

Defaults Without a specific interface specified, the command clears all interface dampening counters

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 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.

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

long | **medium** | **short** Enter the keyword that matches the cable length to be used at the selected port:

short = For 1-meter and 3-meter cable lengths

medium = For 5-meter cable length

long = For 10-meter and 15-meter cable lengths

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 example 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 1 (Unsuccessful)

```
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 example below shows a successful CX4 cable length configuration.

**Example 2
(Successful)**

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

For details on using XFP ports with CX4 cables, refer to your S-Series hardware guide.

**Related
Commands**

[show config](#) Display the configuration of the selected interface.

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

<i>half-life</i>	Enter the number of seconds after which the penalty is decreased. The penalty is decreased by half after the half-life period expires. Range: 1 to 30 seconds Default: 5 seconds
<i>reuse-threshold</i>	Enter a number as the reuse threshold, the penalty value below which the interface state is changed to “up”. Range: 1 to 20000 Default: 750
<i>suppress-threshold</i>	Enter a number as the suppress threshold, the penalty value above which the interface state is changed to “error disabled”. Range: 1 to 20000 Default: 2500
<i>max-suppress-time</i>	Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. Range: 1 to 86400 Default: 20 seconds

Defaults Disabled

Command Modes INTERFACE (conf-if-)

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 7.4.1.0	Introduced on E-Series
Example	<pre>FTOS(config-if-gi-3/2)#dampening 20 800 4500 120 FTOS(config-if-gi-3/2)#</pre>	
Usage Information	<p>With each flap, FTOS 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:</p> <ul style="list-style-type: none"> • <i>suppress-threshold</i> should be greater than <i>reuse-threshold</i> • <i>max-suppress-time</i> should be at least 4 times <i>half-life</i> <p> Note: Dampening cannot be applied on an interface that is monitoring traffic for other interfaces.</p>	
Related Commands	clear dampening	Clear the dampening counters on all the interfaces or just the specified interface.
	show interfaces dampening	Display interface dampening information.

description



Assign a descriptive text string to the interface.

Syntax

description *desc_text*

To delete a description, enter **no description**.

Parameters

desc_text Enter a text string up to 240 characters long.

Defaults

No description is defined.

Command Modes

INTERFACE

Command History

Version 8.1.1.0	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	Modified for E-Series: Revised from 78 to 240 characters.

Usage Information

- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks (“*desc_text*”).
- Entering a text string after the [description](#) command overwrites any previous text string configured as the description.

- The [shutdown](#) and [description](#) commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the [show interfaces description](#) command to display descriptions configured for each interface.

**Related
Commands**

[show interfaces description](#)

Display description field of interfaces.

disable-on-sfm-failure

E 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

Command History
Version 7.7.1.0 Introduced on E300 systems only

Usage Information 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)

C **E** Set the mode of the Management interface.

Syntax **duplex {half | full}**

To return to the default setting, enter **no duplex**.

Parameters
half Enter the keyword **half** to set the Management interface to transmit only in one direction.
full Enter the keyword **full** to set the Management interface to transmit in both directions.




Defaults Not configured

Command Modes INTERFACE

Command History
Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.5.1.0 Introduced on C-Series
Version 6.4.1.0 Documentation modified—added Management to distinguish from [duplex \(10/100 Interfaces\)](#)

Usage Information	This command applies only to the Management interface on the RPMs.	
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.
	speed (Management interface)	Set the speed on the Management interface.

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**.

Parameters

half Enter the keyword **half** to set the physical interface to transmit only in one direction.

full Enter the keyword **full** to set the physical interface to transmit in both directions.

Defaults Not configured

Command Modes INTERFACE

Command History

Version 8.1.1.0	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

Usage Information This command applies to any physical interface with speed set to 10/100.



Note: Starting with FTOS 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

speed (for 10/100/1000 interfaces)	Set the speed on the Base-T Ethernet interface.
negotiation auto	Enable or disable auto-negotiation on an interface.

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>}`

The **threshold** keyword is supported on C-Series and S-Series only.

Parameters

rx on	Enter the keywords rx on to process the received flow control frames on this port. This is the default value for the receive side.
rx off	Enter the keywords rx off to ignore the received flow control frames on this port.
tx on	Enter the keywords tx on to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.
tx off	Enter the keywords tx off so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.
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

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 6.5.1.9 and 7.4.1.0	Introduced on E-Series
Version 7.8.1.0	Introduced on C-Series and S-Series with thresholds

Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full duplex flow control, stations implementing the pause operation instruct the MAC to enable reception of frames with a destination address equal to this multicast address.

The pause:

- Starts when *either* the packet pointer or the buffer threshold is met (whichever is met first). When the discard threshold is met, packets are dropped.
- Ends when *both* the packet pointer and the buffer threshold fall below 50% of the threshold settings.

The *discard threshold* defines when the interface starts dropping the packet on the interface. This may be necessary when a connected device does not honor the flow control frame sent by the 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 Force10 TAC for information and assistance.
- Asymmetric flow control (**rx on tx off** or **rx off tx on**) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

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

- FTOS only supports **rx on tx on** and **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

```
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 FTOS negotiates the flow control values between two Dell Force10 chassis connected back-to-back using 1G copper ports.

Table 25-41. Negotiated Flow Control Values

Configured				Negotiated			
LocRxConf	LocTxConf	RemoteRxConf	RemoteTxConf	LocNegRx	LocNegTx	RemNegRx	RemNegTx
off	off	off	off	off	off	off	off
		off	on	off	off	off	off
		on	off	off	off	off	off
		on	on	off	off	off	off
off	on	off	off	off	off	off	off
		off	on	off	off	off	off
		on	off	off	on	on	off
		on	on	off	off	off	off
on	off	off	off	off	off	off	off
		off	on	on	off	off	on
		on	off	on	on	on	on
		on	on	on	on	on	on
on	on	off	off	off	off	off	off
		off	on	off	off	off	off
		on	off	on	on	on	on
		on	on	on	on	on	on

Related Commands

[show running-config](#)
[show interfaces](#)

Display the flow configuration parameters (non-default values only).
 Display the negotiated flow control parameters.

interface



Configure a physical interface on the switch.

Syntax `interface interface`

Parameters

interface

Enter one of the following keywords and slot/port or number information:

- For 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 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.

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	<pre>FTOS(conf)#interface gig 0/0 FTOS(conf-if-gi-0/0)#exit#</pre>	
Usage Information	<p>You cannot delete a physical interface.</p> <p>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.</p>	
Related Commands	interface loopback	Configure a Loopback interface.
	interface null	Configure a Null interface.
	interface port-channel	Configure a port channel.
	interface sonet	Configure a SONET interface.
	interface vlan	Configure a VLAN.
	show interfaces	Display interface configuration.

interface loopback

C **E** **S** 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

```
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

C **E** 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

```
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	management route	Configure a static route that points to the Management interface or a forwarding router.
	duplex (Management)	Clear FIB entries on a specified line card.
	speed (Management interface)	Clear FIB entries on a specified line card.

interface null

C **E** **S** Configure a Null interface on the switch.

Syntax **interface null** *number*

Parameters *number* Enter zero (0) as the Null interface number.

Defaults	Not configured; <i>number</i> = 0	
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	<pre>FTOS(conf)#interface null 0 FTOS(conf-if-nu-0)#</pre>	
Usage Information	You cannot delete the Null interface. The only configuration command possible in a Null interface is ip unreachable s.	
Related Commands	interface	Configure a physical interface.
	interface loopback	Configure a Loopback interface.
	interface port-channel	Configure a port channel.
	interface vlan	Configure a VLAN.
	ip unreachable s	Enable generation of ICMP unreachable messages.

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 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 This command has no default behavior or values.

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 6.1.1.0	Introduced for E-Series

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 1 (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 2 (Multiple Ports Prompt)

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

Example 3 (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 example is an example of a single range bulk configuration.

Example 4 (Single Range Bulk Configuration)

```
FTOS(config)# interface range gigabitethernet 5/1 - 23
FTOS(config-if-range)# no shutdown
FTOS(config-if-range)#
```

The following example 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 5
(Multiple Range Bulk Configuration - Gigabit & Ten Gigabit Ethernet)

```
FTOS(config-if)# interface range gigabitethernet 5/1 - 23, tengigabitether-
net 1/1 - 2
FTOS(config-if-range)# no shutdown
FTOS(config-if-range)#
```

The following example shows how to use commas to add SONET, VLAN, and port-channel interfaces to the range.

Example 6
(Multiple Range Bulk Configuration - SONET, VLAN, port channel)

```
FTOS(config-if)# interface range gigabitethernet 5/1 - 23, tengigabitether-
net 1/1 - 2, Vlan 2 - 100 , Port 1 - 25
FTOS(config-if-range)# no shutdown
FTOS(config-if-range)#
```

Related Commands

interface port-channel	Configure a port channel group.
interface vlan	Configure a VLAN interface.
show config (from INTERFACE RANGE mode)	Show the bulk configuration interfaces.
show range	Show the bulk configuration ranges.
interface range macro (define)	Define a macro for an interface-range.

interface range macro (define)

C **E** **S** 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

<i>name</i>	Enter up to 16 characters for the macro name.
<i>interface , interface ,...</i>	<p>Enter the interface keyword (refer to parameter 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.</p> <p>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.</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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 VLAN, enter the keyword vlan followed by a number from 1 to 4094.

Defaults This command has no default behavior or value

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
	Version 6.2.1.1	Introduced
Example	<pre>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)#</pre>	
Usage Information	The above example is an example of how to define an interface macro named <i>test</i> . Execute the show running-config command to display the macro definition.	
Related Commands	interface range	Configure a range of command (bulk configuration)
	interface range macro name	Run an interface range macro.

interface range macro *name*

C **E** **S** Run the interface-range macro to automatically configure the pre-defined range of interfaces.

Syntax **interface range macro *name***

Parameters *name* Enter the name of an existing macro.

Defaults This command has no default behavior or value

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 6.2.1.1	Introduced

Usage Information The following example runs the macro named *test* that was defined earlier.

Example

```
FTOS(config)#interface range macro test
FTOS(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#
FTOS
```

Related Commands	interface range	Configure a range of command (bulk configuration)
	interface range macro (define)	Define a macro for an interface range (bulk configuration)

interface vlan

C **E** **S**

Configure a VLAN. You can configure up to 4094 VLANs.

Syntax `interface vlan vlan-id`

To delete a VLAN, use the **no interface vlan *vlan-id*** command.

Parameters

vlan-id Enter a number as the VLAN Identifier.
Range: 1 to 4094.

Defaults

Not configured, except for the Default VLAN, which is configured as VLAN 1.

Command Modes

CONFIGURATION

Command History

Version 8.2.1.0	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

```
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. Refer to [Chapter 10, 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.

keepalive

C **E** **S**

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	<i>seconds</i>	(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.	

link debounce-timer

E 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 affect from the next debounce onward.

monitor

C **E** **S** 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 **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 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

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

The delta column displays changes since the last screen refresh.

Example 1 (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

```

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

m - Change mode

c - Clear screen

l - Page up

a - Page down

T - Increase refresh interval

t - Decrease refresh interval

q - Quit

Example 2
(all interfaces)

```

systest-3 Monitor time: 00:01:31 Refresh Intvl.: 2s Time: 03:54:14

Interface Link In Packets [delta] Out Packets [delta]
Gi 0/0 Down 0 0 0 0
Gi 0/1 Down 0 0 0 0
Gi 0/2 Up 61512 52 66160 42
Gi 0/3 Up 63086 20 9405888 24
Gi 0/4 Up 14697471418 2661481 13392989657 2661385
Gi 0/5 Up 3759 3 161959604 832816
Gi 0/6 Up 4070 3 8680346 5
Gi 0/7 Up 61934 34 138734357 72
Gi 0/8 Up 61427 1 59960 1
Gi 0/9 Up 62039 53 104239232 3
Gi 0/10 Up 17740044091 372 7373849244 79
Gi 0/11 Up 18182889225 44 7184747584 138
Gi 0/12 Up 18182682056 0 3682 1
Gi 0/13 Up 18182681434 43 6592378911 144
Gi 0/14 Up 61349 55 86281941 15
Gi 0/15 Up 59808 58 62060 27
Gi 0/16 Up 59889 1 61616 1
Gi 0/17 Up 0 0 14950126 81293
Gi 0/18 Up 0 0 0 0
Gi 0/19 Down 0 0 0 0
Gi 0/20 Up 62734 54 62766 18
Gi 0/21 Up 60198 9 200899 9
Gi 0/22 Up 17304741100 3157554 10102508511 1114221
Gi 0/23 Up 17304769659 3139507 7133354895 523329

m - Change mode c - Clear screen
b - Display bytes r - Display pkts/bytes per sec
l - Page up a - Page down
T - Increase refresh interval t - Decrease refresh interval
q - Quit

```

Table 25-42. monitor Command Menu Options

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

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 25-43. Difference between Link MTU and IP MTU

Layer 2 Overhead	Link MTU and IP MTU Delta
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

negotiation auto

C **E** **S** Enable auto-negotiation on an interface.

Syntax **negotiation auto**

To disable auto-negotiation, enter **no negotiation auto**.

Defaults Enabled.

Command Modes INTERFACE

Command History

Version 8.1.1.0	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 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 10Mbps or 100Mbps.

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.

Example 1 (Negotiation)

```

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.

Example 2 (Display Auto-negotiation)

```
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:
...
```

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 25-44. Auto-negotiation and Link Speed Combinations

Port 0	Port 1	Link Status between Port 1 and Port 2
auto-negotiation enabled* speed 1000 or auto	auto-negotiation enabled* speed 1000 or auto	Up at 1000 Mb/s
auto-negotiation enabled speed 100	auto-negotiation enabled speed 100	Up at 100 Mb/s
auto-negotiation disabled speed 100	auto-negotiation disabled speed 100	Up at 100 Mb/s
auto-negotiation disabled speed 100	auto-negotiation enabled speed 100	Down
auto-negotiation enabled* speed 1000 or auto	auto-negotiation disabled speed 100	Down

* 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

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

Example 1 (Configuration)

```
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 example 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 example is an example showing 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 2 (Display 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 example 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 3 (Unconfigure 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-gi-7/0)#no portmode hybrid
FTOS(conf-if-vl-20)#
```

Related Commands

show interfaces switchport	Display the configuration of switchport (Layer 2) interfaces on the switch.
switchport	Place the interface in a Layer 2 mode.
vlan-stack trunk	Specify an interface as a trunk port to the Stackable VLAN network.

rate-interval

C **E** **S**

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

C **E** **S**

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

show config (from INTERFACE RANGE mode)

C **E** **S** Display the bulk configured interfaces ([interface range](#)).

Syntax **show config**

Command Modes CONFIGURATION INTERFACE (conf-if-range)

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 on E-Series

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

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 Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383.
- For the management interface on an 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 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 255 for TeraScale and 1 to 512 for ExaScale.
- 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.
- For a VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.2.1.2	Include SFP and SFP+ optics power detail in E-Series and C-Series output.
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 7.8.1.0	Output expanded to include SFP+ media in C-Series
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
Version 6.3.1.0	Added Pluggable Media Type field in E-Series TeraScale output

Usage

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.

Example 1

```
FTOS#show interfaces tengigabitethernet 2/0
TenGigabitEthernet 2/0 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:3a
Interface index is 100990998
Internet address is 213.121.22.45/28
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 02:31:45
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  Input 0 IP Packets, 0 Vlans 0 MPLS
```



```

    0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
    0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
    0 symbol errors, 0 runts, 0 giants, 0 throttles
    0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
Output Statistics:
    1 packets, 64 bytes, 0 underruns
    0 Multicasts, 2 Broadcasts, 0 Unicasts
    0 IP Packets, 0 Vlans, 0 MPLS
    0 throttles, 0 discarded
Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
    Output 00.00 Mbits/sec,        0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:00:27

```

Table 25-45. Lines in show interfaces Command Example

Line	Description
TenGigabitEthernet 2/0...	Displays the interface's type, slot/port, and administrative and line protocol status.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
MTU 1554...	Displays link and IP MTU information. If the chassis is in Jumbo mode, this number can range from 576 to 9252.
LineSpeed	Displays the interface's line speed.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the show interfaces counters were cleared.
Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	<p>Displays all the input statistics including:</p> <ul style="list-style-type: none"> Number of packets and bytes into the interface Number of packets with IP headers, VLAN tagged headers and MPLS headers <p>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.</p> <ul style="list-style-type: none"> Packet size and the number of those packets inbound to the interface Number of runts, giants, and throttles packets: <ul style="list-style-type: none"> runts = number of packets that are less than 64B giants = packets that are greater than the MTU size throttles = packets containing PAUSE frames Number of CRC, IP Checksum, overrun, and discarded packets: <ul style="list-style-type: none"> 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

Table 25-45. Lines in show interfaces Command Example (Continued)

Line	Description
Output Statistics:	<p>Displays output statistics sent out of the interface including:</p> <ul style="list-style-type: none"> 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
Rate information...	<p>Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds).</p> <p>Traffic rate is displayed in bits, packets per second, and percent of line rate.</p>
Time since...	Elapsed time since the last interface status change (hh:mm:ss format).

**Example 2
(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:
  857732 packets, 54894848 bytes, 0 underruns
  857732 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 25-46. Fields in show interfaces Command Example (TeraScale)

Line	Description
TenGigabitEthernet 0/0...	Interface type, slot/port and administrative and line protocol status.
Hardware is...	Interface hardware information, assigned MAC address, and current address.
Pluggable media present...	<p>Present pluggable media wavelength, type, and rate. The error scenarios are:</p> <ul style="list-style-type: none"> • Wavelength, Non-qualified — Dell Force10 ID is not present, but wavelength information is available from XFP or SFP serial data • Wavelength, F10 unknown—Dell Force10 ID is present, but not able to determine the optics type • Unknown, Non-qualified— if wavelength is reading error, and Dell Force10 ID is not present <p>Dell Force10 allows unsupported SFP and XFP transceivers to be used, but FTOS 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.</p>
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
MTU 1554...	Displays link and IP MTU information.
LineSpeed	Displays the interface’s line speed, duplex mode, and Slave
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the show interfaces counters were cleared.
Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	<p>Displays all the input statistics including:</p> <ul style="list-style-type: none"> • Number of packets and bytes into the interface • Number of packets with VLAN tagged headers • Packet size and the number of those packets inbound to the interface • Number of Multicast and Broadcast packets: <ul style="list-style-type: none"> Multicasts = number of MAC multicast packets Broadcasts = number of MAC broadcast packets • Number of runts, giants, and throttles packets: <ul style="list-style-type: none"> runts = number of packets that are less than 64B giants = packets that are greater than the MTU size throttles = packets containing PAUSE frames • Number of CRC, overrun, and discarded packets: <ul style="list-style-type: none"> CRC = packets with CRC/FCS errors overrun = number of packets discarded due to FIFO overrun conditions discarded = the sum of runts, giants, CRC, and overrun packets discarded without any processing

Table 25-46. Fields in show interfaces Command Example (TeraScale)

Line	Description
Output Statistics:	Displays output statistics sent out the interface including: <ul style="list-style-type: none"> Number of packets, bytes and underruns out of the interface Packet size and the number of those packets outbound to the interface Number of Multicast, Broadcast and Unicast packets: <ul style="list-style-type: none"> Multicasts = number of MAC multicast packets Broadcasts = number of MAC broadcast packets Unicasts = number of MAC unicast packets Number of VLANs, throttles, discards, and collisions: <ul style="list-style-type: none"> Vlans = number of VLAN tagged packets throttles = packets containing PAUSE frames discarded = number of packets discarded without any processing collisions = number of packet collisions wred=count both packets discarded in the MAC and in the hardware-based queues
Rate information...	Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds) Traffic rate is displayed in bits, packets per second, and percent of line rate.
Time since...	Elapsed time since the last interface status change (hh:mm:ss format).

**Example 3
(1G SFP
Interface)**

```

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 SFP 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 Vlans
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  0 packets, 0 bytes, 0 underruns
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 Vlans, 0 throttles, 0 discarded, 0 collisions, 0 wredrops
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#
```

**Example 4
(10G SFP+ ,
C-Series)**

```
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#
```

**Example 5
(Management
Ethernet)**

```
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
```

**Usage
Information**

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**

show interfaces configured	Display any interface with a non-default configuration.
show interfaces linecard	Display information on all interfaces on a specific line card.
show interfaces phy	Display auto-negotiation and link partner information
show interfaces rate	Display information of either rate limiting or rate policing on the interface.
show interfaces switchport	Display Layer 2 information about the interfaces.
show inventory (C-Series and E-Series)	Display the chassis type, components (including media), FTOS version including hardware identification numbers and configured protocols.
show inventory (S-Series)	Display the S-Series switch type, components (including media), FTOS version including hardware identification numbers and configured protocols.
show ip interface	Display Layer 3 information about the interfaces.

show linecard	Display the line card(s) status.
show range	Display all interfaces configured using the interface range command.

show interfaces configured

C **E** **S** 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 Forcel0Eth, 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

C **E** **S** 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 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.
- 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 8.1.1.0 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

```
FTOS#show interfaces dampening
Interface      Supp   Flaps   Penalty   Half-Life   Reuse   Suppress   Max-Sup
                State
Gi 3/2         Up     0       0         20          800     4500       120
Gi 3/10        Up     0       0         5           750     2500       20
FTOS#
```

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

E 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

Version 8.2.1.0

Introduced on E-Series ExaScale

Version 7.7.1.0

Introduced on E-Series

Related Commands

[show interfaces](#)

Display information on a specific physical interface or virtual interface.

show interfaces description

C **E** **S** 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 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 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 information.
- For VLAN interfaces, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.2.1.0	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 6.2.1.1	Introduced on E-Series

Example

```

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 25-47. show interfaces description Command Example Fields

Field	Description
Interface	Displays type of interface and associated slot and port number.
OK?	Indicates if the hardware is functioning properly.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.
Description	Displays the description (if any) manually configured for the interface.

Related Commands

[show interfaces](#) Display information on a specific physical interface or virtual interface.

show interfaces linecard

C **E** Display information on all interfaces on a specific line card.

Syntax `show interfaces linecard slot-number`

Parameters

<i>slot-number</i>	Enter a number for the line card slot. C-Series Range: 0-7 for C300; 0-3 for 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 example 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 Force10 is inserted, it might work, but its details might not be readable by FTOS and not displayed here.

Example

```
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 33883138
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

CES Display auto-negotiation and link partner information.

Syntax show interfaces gigabitethernet *slot/port* phy

Parameters gigabitethernet Enter the keyword **gigabitethernet** followed by the slot/port information.

Command Modes EXEC
EXEC Privilege

Command History
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

```
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 25-48. Lines in show interfaces gigabitethernet Command Example

Line	Description
Mode Control	Indicates if auto negotiation is enabled. If so, indicates the selected speed and duplex.
Mode Status	Displays auto negotiation fault information. When the interface completes auto negotiation successfully, the autoNegComplete field and the linkstatus field read "True."
AutoNegotiation Advertise	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.
AutoNegotiation Remote Partner's Ability	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
AutoNegotiation Expansion	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.
1000Base-T Control	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.
Phy Specific Control	Values are: 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[show interfaces](#)

Display information on a specific physical interface or virtual interface.

show interfaces stack-unit

S 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).

Command Modes EXEC
EXEC Privilege

Command History Version 7.6.1.0 Introduced for S-Series only

Example

```
FTOS#show interfaces stack-unit 0
GigabitEthernet 0/1 is down, line protocol is down
Hardware is Forcel0Eth, address is 00:01:e8:4c:f2:82
  Current address is 00:01:e8:4c:f2:82
Pluggable media not present
Interface index is 34129154
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto, Mode auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3w0d17h
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  5144 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  0 packets, 0 bytes, 0 underruns
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
  Output 00.00 Mbits/sec,        0 packets/sec, 0.00% of line-rate
Time since last interface status change: 3w0d17h

GigabitEthernet 0/2 is down, line protocol is down
Hardware is Forcel0Eth, address is 00:01:e8:4c:f2:83
  Current address is 00:01:e8:4c:f2:83
!-----output truncated -----!
```

Related Commands

show hardware stack-unit	Display data plane and management plane input/output statistics.
show interfaces	Display information on a specific physical interface or virtual interface.

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`

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.

linecard slot-number

(OPTIONAL) Enter the keyword **linecard** followed by the slot number.

C-Series Range: 0 to 7 for C300; 0–3 for C150

E-Series Range: 0 to 13 on the E1200, 0 to 6 on the E600, 0 to 5 on the E300

Defaults No default behavior or values

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 7.5.1.0	Introduced on E-Series

Example

```
FTOS#show interfaces status
Port      Description  Status Speed      Duplex  Vlan
Gi 0/0                    Up      1000 Mbit  Auto    --
Gi 0/1                    Down    Auto      Auto     1
Gi 0/2                    Down    Auto      Auto     1
Gi 0/3                    Down    Auto      Auto     --
Gi 0/4  Force10Port  Up      1000 Mbit  Auto    30-130
Gi 0/5                    Down    Auto      Auto     --
Gi 0/6                    Down    Auto      Auto     --
Gi 0/7                    Up      1000 Mbit  Auto    1502,1504,1506-1508,1602
Gi 0/8                    Down    Auto      Auto     --
Gi 0/9                    Down    Auto      Auto     --
Gi 0/10                   Down    Auto      Auto     --
Gi 0/11                   Down    Auto      Auto     --
Gi 0/12                   Down    Auto      Auto     --
Gi 0/13                   Down    Auto      Auto     --
Gi 0/14                   Down    Auto      Auto     --
Gi 0/15                   Down    Auto      Auto     --
FTOS#
```

Related Commands

[show interfaces](#)

Display information on a specific physical interface or virtual interface.

show interfaces switchport



Display only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces' IEEE 802.1Q tag status and VLAN membership.

Syntax `show interfaces switchport [interface [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 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.
- Enter the keyword **backup** to view the backup interface for this interface.

linecard

slot-number

(OPTIONAL) Enter the keyword **linecard** followed by the slot number. This option is available only on E-Series and C-Series.

C-Series Range: 0-7 for C300; 0-3 for C150

E-Series Range: 0 to 13 on the E1200, 0 to 6 on the E600, 0 to 5 on the E300

stack-unit

unit-id

(OPTIONAL) Enter the keyword **stack-unit** followed by the stack member number. This option is available only on S-Series.

Range: 0 to 1

Command Modes

EXEC

EXEC Privilege

Command History

Version 8.2.1.0 Support for 4093 VLANs on E-Series ExaScale

Version 8.1.1.0 Introduced on E-Series ExaScale

Version 7.6.1.0 Support added for hybrid port/native VLAN, introduced on S-Series

Version 7.5.1.0 Introduced on C-Series

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--
```

Table 25-49. Items in show interfaces switchport Command Example

Items	Description
Name	Displays the interface's type, slot and port number.
802.1QTagged	Displays whether if the VLAN tagged ("True"), untagged ("False"), or hybrid ("Hybrid", which supports both untagged and tagged VLANs by port 13/0.
Vlan membership	Lists the VLANs to which the interface is a member. Starting with FTOS 7.6.1, this field can display native VLAN membership by port 13/0.

Related Commands

interface	Configure a physical interface on the switch.
show ip interface	Displays Layer 3 information about the interfaces.
show interfaces	Display information on a specific physical interface or virtual interface.
show interfaces transceiver	Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show interfaces transceiver



Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

Syntax

show interfaces [gigabitethernet | tengigabitethernet] *slot/port* transceiver

Parameters

gigabitethernet	For a 10/100/1000 interface, enter the keyword gigabitethernet followed by the slot/port information.
tengigabitethernet	For a 10G interface, enter the keyword tengigabitethernet followed by the slot/port information.

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Output augmented with diagnostic data for pluggable media
Version 7.7.1.0	Removed three fields in output: Vendor Name, Vendor OUI, Vendor PN
Version 7.6.1.0	Introduced on C-Series and S-Series
Version 6.5.4.0	Introduced on E-Series

Usage

Refer to the example below for an example screenshot, and refer to the following table or a description of the output fields.

For related commands, refer to the Related Commands section, below, and refer to the Debugging and Diagnostics chapter for your platform at the end of this book.

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 Transceiver Code = 0x00 0x00 0x00 0x01 0x20 0x40 0x0c 0x05
SFP 0 Encoding = 0x01
SFP 0 BR Nominal = 0x15
SFP 0 Length(9um) Km = 0x00
SFP 0 Length(9um) 100m = 0x00
SFP 0 Length(50um) 10m = 0x1e
SFP 0 Length(62.5um) 10m = 0x0f
SFP 0 Length(Copper) 10m = 0x00
SFP 0 Vendor Rev = A
SFP 0 Laser Wavelength = 850 nm
SFP 0 CheckCodeBase = 0x66
SFP 0 Serial Extended ID fields
SFP 0 Options= 0x00 0x12
SFP 0 BR max= 0
SFP 0 BR min= 0
SFP 0 Vendor SN= P5N1ACE
SFP 0 Datecode = 040528
SFP 0 CheckCodeExt = 0x5b
```

```
SFP 1 Diagnostic Information
=====
SFP 1 Rx Power measurement type = Average
=====
SFP 1 Temp High Alarm threshold = 95.000C
SFP 1 Voltage High Alarm threshold = 3.900V
SFP 1 Bias High Alarm threshold = 17.000mA
SFP 1 TX Power High Alarm threshold = 0.631mW
SFP 1 RX Power High Alarm threshold = 1.259mW
SFP 1 Temp Low Alarm threshold = -25.000C
SFP 1 Voltage Low Alarm threshold = 2.700V
SFP 1 Bias Low Alarm threshold = 1.000mA
SFP 1 TX Power Low Alarm threshold = 0.067mW
SFP 1 RX Power Low Alarm threshold = 0.010mW
=====
SFP 1 Temp High Warning threshold = 90.000C
SFP 1 Voltage High Warning threshold = 3.700V
SFP 1 Bias High Warning threshold = 14.000mA
SFP 1 TX Power High Warning threshold = 0.631mW
SFP 1 RX Power High Warning threshold = 0.794mW
SFP 1 Temp Low Warning threshold = -20.000C
SFP 1 Voltage Low Warning threshold = 2.900V
SFP 1 Bias Low Warning threshold = 2.000mA
SFP 1 TX Power Low Warning threshold = 0.079mW
SFP 1 RX Power Low Warning threshold = 0.016mW
=====
SFP 1 Temperature = 39.930C
SFP 1 Voltage = 3.293V
SFP 1 Tx Bias Current = 6.894mA
SFP 1 Tx Power = 0.328mW
SFP 1 Rx Power = 0.000mW
=====
SFP 1 Data Ready state Bar = False
```

```

SFP 1 Rx LOS state = True
SFP 1 Tx Fault state = False
SFP 1 Rate Select state = False
SFP 1 RS state = False
SFP 1 Tx Disable state = False
=====
SFP 1 Temperature High Alarm Flag = False
SFP 1 Voltage High Alarm Flag = False
SFP 1 Tx Bias High Alarm Flag = False
SFP 1 Tx Power High Alarm Flag = False
SFP 1 Rx Power High Alarm Flag = False
SFP 1 Temperature Low Alarm Flag = False
SFP 1 Voltage Low Alarm Flag = False
SFP 1 Tx Bias Low Alarm Flag = False
SFP 1 Tx Power Low Alarm Flag = False
SFP 1 Rx Power Low Alarm Flag = True
=====
!-----output truncated -----!

```

Table 25-50. Diagnostic Data in show interfaces transceiver

Line	Description
Rx Power measurement type	Output depends on the vendor, typically either “Average” or “OMA” (Receiver optical modulation amplitude).
Temp High Alarm threshold	Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.
Voltage High Alarm threshold	Displays the interface index number used by SNMP to identify the interface.
Bias High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.

Table 25-50. Diagnostic Data in show interfaces transceiver (Continued)

Line	Description
Temperature	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.
Voltage	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.
Tx Bias Current	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.
Tx Power	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.
Rx Power	Present Rx power of the SFP. This value is either average Rx power or OMA.This depends upon on the Rx Power measurement type displayed above. If this crosses Rx power alarm/warning thresholds, then the Rx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, then the Rx power low alarm/warning flag is set to true.
Data Ready state Bar	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.
Rx LOS state	This is the digital state of the Rx_LOS output pin.This is set to true if the operating status is down.
Tx Fault state	This is the digital state of the Tx Fault output pin.
Rate Select state	This is the digital state of the SFP rate_select input pin.
RS state	This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.
Tx Disable state	If the admin status of the port is down then this flag will be set to true.
Temperature High Alarm Flag	This can be either true/False and it depends on the Current Temperature value displayed above.
Voltage High Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias High Alarm Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power High Alarm Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power High Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature Low Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias Low Alarm Flag	This can be either true or false, depending on the Tx bias current value displayed above.

Table 25-50. Diagnostic Data in show interfaces transceiver (Continued)

Line	Description
Tx Power Low Alarm Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature High Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage High Warning Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias High Warning Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power High Warning Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature Low Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Warning Flag	This can be either true or false, depending on the Current voltage value displayed above.
Tx Bias Low Warning Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power Low Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Warning Flag	This can be either true or false, depending on the Current Rx power value displayed above.

Related Commands

interface	Configure a physical interface on the switch.
show ip interface	Displays Layer 3 information about the interfaces.
show interfaces	Display information on a specific physical interface or virtual interface.
show inventory (C-Series and E-Series)	Display the chassis type, components (including media), FTOS version including hardware identification numbers and configured protocols.
show inventory (S-Series)	Display the S-Series switch type, components (including media), FTOS version including hardware identification numbers and configured protocols.

show range



Display all interfaces configured using the [interface range](#) command.

Syntax

show range

Command Mode

INTERFACE RANGE (config-if-range)

Command History

Version 8.2.1.0	Support for 4093 VLANs on E-Series ExaScale
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

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)#
```

Related Commands	interface	Configure a physical interface on the switch.
	show ip interface	Displays Layer 3 information about the interfaces.
	show interfaces	Display information on a specific physical interface or virtual interface.

shutdown



Disable an interface.

Syntax **shutdown**

To activate an interface, enter **no shutdown**.

Defaults The interface is disabled.

Command Modes INTERFACE

Command History

Version 8.1.1.0	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 legacy command	

Usage Information

The [shutdown](#) command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the [show ip interface brief](#) command. Disabled interfaces are listed as down.

Disabling a VLAN or a port channel causes different behavior. When a VLAN is disabled, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the [shutdown](#) command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, you must enter [no shutdown](#) on the port channel interface and at least one interface within that port channel.

The [shutdown](#) and [description](#) commands are the only commands that you can configure on an interface that is a member of a port channel.

Related Commands

interface port-channel	Create a port channel interface.
interface vlan	Create a VLAN.
show ip interface	Displays the interface routing status. Add the keyword brief to display a table of interfaces and their status.

speed (for 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 upSyntax

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 i 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. Refer to [negotiation auto](#) for more information)
Note: When this setting is enabled, only 100oBase-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. Refer to [negotiation auto](#) for more information)

Defaults

auto

Command Modes

INTERFACE

Command History

Version 8.3.1.0	Supported on LC-EH-GE-50P or the LC-EJ-GE-50P cards
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 legacy command	

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 FTOS 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)

C **E** 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

10 Enter the keyword **10** to set the interface's speed to 10 Mb/s.
100 Enter the keyword **100** to set the interface's speed to 100 Mb/s.
auto Enter the keyword **auto** to set the interface to auto-negotiate its speed.

Defaults `auto`

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

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

C **E** **S** Place an interface in Layer 2 mode.

Syntax `switchport [backup interface { gigabit slot/port | tengigabit slot/port | 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 slot/port | tengigabit slot/port | port-channel number }**.

Parameters

backup interface 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.

gigabit Enter this keyword if the backup port is a 1G port.

tengigabit Enter this keyword if the backup port is a 10G port.

port-channel Enter this keyword if the backup port is a static or dynamic port channel.

slot/port Specify the line card and port number of the backup port.

Defaults	Disabled (The interface is in Layer 3 mode.)	
Command Modes	INTERFACE	
Command History	Version 8.4.1.0	Added support for port-channel interfaces (port-channel number option).
	Version 8.1.1.0	Introduced on E-Series ExaScale
	Version 7.7.1.0	Added backup interface option.
	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	<p>If an IP address or VRRP group is assigned to the interface, you cannot use the switchport command on the interface. To use the switchport command on an interface, only the no ip address and no shutdown statements must be listed in the show config output.</p> <p>When you enter the switchport command, the interface is automatically added to the default VLAN.</p> <p>To use the switchport backup interface command on a port, you must first enter the switchport command. For details, refer to the Configuring Redundant Links section in the Layer 2 chapter of the <i>FTOS Configuration Guide</i>.</p>	
Related Commands	interface port-channel	Create a port channel interface.
	show interfaces switchport	Display information about switchport interfaces.

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

Command History

Version 8.1.1.2	Introduced on E-Series ExaScale
pre-Version 6.2.1.0	Introduced for E-Series

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 example 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.

Example

```
interface TenGigabitEthernet 13/0
  no ip address
  no shutdown
FTOS(conf-if-te-13/0)#
```



```

FTOS(conf-if-te-13/0)#wanport
% Error: Port should be in shutdown mode, config ignored Te 13/0.
FTOS(conf-if-te-13/0)#
FTOS(conf-if-te-13/0)#shutdown
FTOS(conf-if-te-13/0)#
FTOS(conf-if-te-13/0)#wanport
FTOS(conf-if-te-13/0)#

```

**Related
Commands**

ais-shut	Send LAIS on shutdown
alarm-report	Enable reporting of a selected alarm
clock source	Configure a clock source
down-when-looped	Send a message when a loopback condition is detected
flag	Set flags to ensure interoperability
framing	Set framing type
keepalive	Enable keepalive
loopback	Troubleshoot a SONET loopback

Port Channel Commands

A Link Aggregation Group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In FTOS, a LAG is referred to as a Port Channel.

Table 25-51. Port Channel Limits

Platform	Maximum Port Channel IDs	Maximum Members per Port Channel
E-Series ExaScale	255	64
E-Series TeraScale	255	16
C-Series	128	8
S-Series	128	8

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](#)
- [show interfaces port-channel](#)
- [show port-channel-flow](#)



Note: The FTOS implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information on FTOS Link Aggregation Control Protocol (LACP) for dynamic LAGs, refer to [Chapter 31, Link Aggregation Control Protocol \(LACP\)](#).

For more information on configuring and using Port Channels, refer to the *FTOS Configuration Guide*.

channel-member



Add an interface to the Port Channel, while in the INTERFACE PORTCHANNEL mode.

Syntax

channel-member *interface*

To delete an interface from a Port Channel, use the **no channel-member** *interface* command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a 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.

Defaults

Not configured.

Command Modes

INTERFACE PORTCHANNEL

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

Use the [interface port-channel](#) command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration. 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.

Related Commands

- [description](#) Assign a descriptive text string to the interface.
- [interface port-channel](#) Create a Port Channel interface.
- [shutdown](#) Disable/Enable the port channel.

group



Group two LAGs in a supergroup (“fate-sharing group” or “failover group”).

Syntax

group *group_number* **port-channel** *number* **port-channel** *number*

To remove an existing LAG supergroup, use the **no group** *group_number* command.

Parameters

- group_number* Enter an integer from 1 to 32 that will uniquely identify this LAG fate-sharing group.
- port-channel** *number* Enter the keyword **port-channel** followed by an existing LAG *number*. Enter this keyword/variable combination twice, identifying the two LAGs to be paired.

Defaults

No default values or behavior

Command Modes

PORT-CHANNEL FAILOVER-GROUP (conf-po-failover-grp)

Command History

- Version 8.1.1.0 Introduced on E-Series ExaScale
- Version 7.6.1.0 Introduced for C-Series, E-Series, and S-Series

Example

```
FTOS(conf)#port-channel failover-group
FTOS(conf-po-failover-grp)#group 1 port-channel 1 port-channel 2
FTOS(conf-po-failover-grp)#
```

Related Commands

- [port-channel failover-group](#) Access the PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.
- [show interfaces port-channel](#) Display information on configured Port Channel groups.

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 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.

Related Commands

channel-member	Add a physical interface to the LAG.
interface	Configure a physical interface.
interface loopback	Configure a Loopback interface.
interface null	Configure a null interface.
interface vlan	Configure a VLAN.
shutdown	Disable/Enable the port channel.

minimum-links

C **E** **S**

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

C **E** **S**

Access the PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

Syntax `port-channel failover-group`

To remove all LAG failover groups, use the **no port-channel failover-group** command.

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.6.1.0	Introduced for C-Series, E-Series, and S-Series

Usage Information 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, refer to the Port Channel chapter in the *FTOS Configuration Guide*.

Related Commands

group	Group two LAGs in a supergroup (“fate-sharing group”).
show interfaces port-channel	Display information on configured Port Channel groups.

show config

C **E** **S**

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

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

show interfaces port-channel

C **E** **S**

Display information on configured Port Channel groups.

Syntax **show interfaces port-channel** [*channel-number*] [**brief**]

Parameters

<i>channel-number</i>	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 TeraScale and 1 to 512 for ExaScale.
brief	(OPTIONAL) Enter the keyword brief to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.6.1.0	Introduced for S-Series; Modified to display LAG failover group status
Version 7.5.1.0	Introduced for C-Series

E-Series legacy command

Example 1

```
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 25-52. show interfaces port-channel Command Example Fields

Field	Description
Port-Channel 1...	Displays the LAG's status. In the example, the status of the LAG's LAG fate-sharing group ("Failover-group") is listed.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Port-channel is part...	Indicates whether the LAG is part of a LAG fate-sharing group ("Failover-group").
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
MTU 1554...	Displays link and IP MTU.
LineSpeed	Displays the interface's line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.
Members in this...	Displays the interfaces belonging to this port channel.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the show interfaces counters were cleared.
Queueing strategy..	States the packet queuing strategy. FIFO means first in first out.
packets input...	Displays the number of packets and bytes into the interface.
Input 0 IP packets...	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.
0 64-byte...	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
Received 0...	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
Rate information...	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
Time since...	Displays the time since the last change in the configuration of this interface.

**Example 2
(brief)**

```

FTOS#sh int por 1 br
LAG Mode  Status      Uptime  Ports
1  L2    up          00:00:08  Gi 3/0    (Up) *
                   Gi 3/1    (Down)
                   Gi 3/2    (Up)
FTOS#

```

Table 25-53. show interfaces port-channel brief Command Example Fields

Field	Description
LAG	Lists the port channel number.
Mode	Lists the mode: <ul style="list-style-type: none"> L3 - for Layer 3 L2 - for Layer 2
Status	Displays the status of the port channel. <ul style="list-style-type: none"> down - if the port channel is disabled (shutdown) up - if the port channel is enabled (no shutdown)
Uptime	Displays the age of the port channel in hours:minutes:seconds.
Ports	Lists the interfaces assigned to this port channel.
(untitled)	Displays the status of the physical interfaces (up or down). In Layer 2 port channels, an * (asterisk) indicates which interface is the primary port of the port channel. The primary port sends out interface PDU. In Layer 3 port channels, the primary port is not indicated.

**Related
Commands**

[show lacp](#) Display the LACP matrix.

show port-channel-flow

C **E** **S** 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 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: <ul style="list-style-type: none"> 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.
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.
source-port number	Enter the keyword source-port followed by the source port number. Range: 1-65536 Default: None
destination-port number	Enter the keyword destination-port followed by the destination port number. Range: 1-65536 Default: None
source-mac address	Enter the keyword source-mac followed by the MAC source address in the nn:nn:nn:nn:nn:nn format.
destination-mac address	Enter the keyword destination-mac followed by the MAC destination address in the nn:nn:nn:nn:nn:nn format.

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.

```
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]} {source-port *number* destination-port *number*}

- 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

[load-balance \(E-Series\)](#)

Balance traffic over E-Series port channel members.

Time Domain Reflectometer (TDR)

TDR is supported on E-Series ExaScale  with FTOS 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—refer to 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

C **E** **S** Test the condition of copper cables on 100/1000 Base-T modules.

Syntax `tdr-cable-test interface`

Parameters *interface* Enter the keyword **GigabitEthernet** followed by the slot/port information for the 100/1000 Ethernet interface.

Defaults No default behavior or setting

Command Modes EXEC

Command History

Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.7.1.0	Introduced on S-Series
Version 7.6.1.0	Introduced on C-Series
Version 6.1.1.0	Introduced on E-Series

Usage Information 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.

show tdr

C **E** **S** Display the TDR test results.

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

Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.7.1.0	Support added for S-Series
Version 7.6.1.0	Support added for C-Series
Version 6.1.1.0	Introduced

Example

```

FTOS#show tdr gigabitethernet 10/47
Time since last test: 00:00:02
  Pair A, Length: OK Status: Terminated
  Pair B, Length: 92 (+/- 1) meters, Status: Short
  Pair C, Length: 93 (+/- 1) meters, Status: Open
  Pair D, Length: 0 (+/- 1) meters, Status: Impedance Mismatch

```

Table 25-54. TDR Test Status

Status	Definition
<i>OK Status: Terminated</i>	TDR test is complete, no fault is detected on the cable, and the test is terminated
Length: 92 (+/- 1) meters, Status: Shorted	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.
Length: 93 (+/- 1) meters, Status: Open	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.
Status: Impedance Mismatch	There is an impedance mismatch in the cables.

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: **E**
- 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

E Enable UDP debug and display the debug information on a console.

Syntax **debug ip udp-helper**

To disable debug information, use the **no debug ip udp-helper** command.

Defaults Debug disabled

Command Modes EXEC

EXEC Privilege

Example 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**

ip udp-broadcast-address	Configure a UDP IP address for broadcast
ip udp-helper udp-port	Enable the UDP broadcast feature on an interface.
show ip udp-helper	Display the configured UDP helper(s) on all interfaces.

ip udp-broadcast-address

E Configure an IP UDP address for broadcast.

Syntax **ip udp-broadcast-address** *address*

To delete the configuration, use the **no ip udp-broadcast-address** *address* command.

Parameters *address* Enter an IP broadcast address in dotted decimal format (A.B.C.D).

Defaults Not Configured

Command Modes INTERFACE (config-if)

Usage Information When a UDP broadcast packet is flooded out of an interface, and the outgoing interface is configured using this command, the outgoing packet's IP destination address is replaced with the configured broadcast address.

**Related
Commands**

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.

ip udp-helper udp-port

E 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.
Note: If this option is not used, all UDP Ports are considered by default.

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

E Display the configured UDP helper(s) on all interfaces.

Syntax **show ip udp-helper**

Defaults No default configuration or values

Command Modes EXEC

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 Force10 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
- ip name-server
- ip proxy-arp
- ip redirects
- ip route

- ip source-route
- ip unreachable
- ip vlan-flooding
- load-balance (C-Series and S-Series)
- load-balance (E-Series)
- management route
- show arp
- show arp retries
- show hosts
- show ip cam linecard
- show ip cam stack-unit
- show ip fib linecard
- show ip fib stack-unit
- show ip flow
- show ip interface
- show ip management-route
- show ipv6 management-route
- show ip protocols
- show ip route
- show ip route list
- show ip route summary
- show ip traffic
- show protocol-termination-table
- show tcp statistics

arp



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

- | | |
|--------------------|---|
| <i>vrf name</i> | E-Series Only: Enter the VRF process identifier to tie the static route to the VRF process. |
| <i>ip-address</i> | Enter an IP address in dotted decimal format. |
| <i>mac-address</i> | Enter a MAC address in nnnn.nnnn.nnnn format. |
| <i>interface</i> | Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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. |

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 6.2.1.1	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

C **E** **S** Enable ARP learning via Gratuitous ARP.

Syntax **arp learn-enable**

Defaults Disabled

Command Modes CONFIGURATION

Command History
Version 8.3.1.0 Introduced

Usage Information In FTOS 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:

- 1 At time t=0 FTOS sends an ARP request for IP *A.B.C.D*
- 2 At time t=1 FTOS receives an ARP request for IP *A.B.C.D*
- 3 At time t=2 FTOS 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, FTOS installs an ARP entry on all 3 CPUs.

arp retries

C **E** **S** Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

Syntax **arp retries** *number*

Parameters
number Enter the number of retries.
Range: 5 to 20.
Default: 5

Defaults	5
Command Modes	CONFIGURATION
Command History	Version 8.3.1.0 Introduced
Usage Information	Retries are 20 seconds apart.
Related Commands	show arp retries Display the configured number of ARP retries.

arp timeout

C **E** **S**

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

seconds Enter the number of minutes.
Range: 0 to 35790.
Default: 240 minutes.

Defaults 240 minutes (4 hours)

Command Modes INTERFACE

Command History

Version 8.1.1.0 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

Related Commands [show interfaces](#) Displays the ARP timeout value for all available interfaces.

clear arp-cache

C **E** **S**

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 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.
- 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	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 7.9.1.0	Introduced VRF on the E-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

clear host

C **E** **S** Remove one or all dynamically learnt host table entries.

Syntax **clear host name**

Parameters

name Enter the name of the host to delete.
Enter * to delete all host table entries.

Command Modes EXEC Privilege

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

clear ip fib linecard



Clear all Forwarding Information Base (fib) entries in the specified line card (use this command with caution, refer to [Usage Information](#) below)

Syntax `clear ip fib linecard slot-number | vrf vrf instance`

Parameters

slot-number Enter the number of the line card slot.
C-Series and **S-Series** Range: 0-7
E-Series Range: 0 to 13 on E12001200i, 0 to 6 on E600/E600i; 0 to 5 on E300

vrf instance (Optional) **E-Series Only**: Clear only the FIB entries on the specified card associated with the VRF instance.

Command Mode

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 7.9.1.0	Introduced VRF on the E-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

Usage Information

Use this command to clear Layer 3 CAM inconsistencies.



Caution: Executing this command will cause traffic disruption.

Related Commands

[show ip fib linecard](#) Show FIB entries.

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 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

Related Commands

[ip route](#) Assign an IP route to the switch.
[show ip route](#) View the routing table.
[show ip route summary](#) View a summary of the routing table.

clear tcp statistics

C **E** **S** 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

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

debug arp

C **E** **S** 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 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.

count value (OPTIONAL) Enter the keyword **count** followed by the count value.
Range: 1 to 65534

Command Modes EXEC Privilege

Command History

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

C **E** **S**

Enable debug information for DHCP relay transactions and display the information on the console.

Syntax

debug ip dhcp

To disable debug, use the **no debug ip dhcp** command.

Defaults

Debug disabled

Command Modes EXEC Privilege

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.6.1.0 Added support for S-Series
Version 7.5.1.0 Introduced on C-Series
Version 6.4.1.0 Introduced on E-Series

Example

```
FTOS#debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request,
hops = 0, XID = 0xbf05140f, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request,
hops = 0, XID = 0xbf05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops
= 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP Request,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply, hops
= 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
FTOS#
```

**Related
Commands**

[ip helper-address](#)

Specify the destination broadcast or host address for DHCP server request.

[ip helper-address hop-count disable](#)

Disable hop-count increment for DHCP relay agent.

debug ip icmp

C **E** **S**

View information on the Internal Control Message Protocol (ICMP).

Syntax

debug ip icmp [*interface*] [*count value*]

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

Parameters

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 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 VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

count value

(OPTIONAL) Enter the keyword **count** followed by the count value.

Range: 1 to 65534

Default: Infinity

Command Modes

EXEC Privilege

**Command
History**

Version 8.2.1.0	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

Example

```
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 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 Mode

EXEC Privilege

Command History

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	Added the access-group option
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

Example

```
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739, win=8191 ACK PUSH
IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd
    TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226, sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739, win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd
    UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 0
    ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
```



```

IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (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 26-55. debug ip packet Command Example Fields

Field	Description
s=	Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.
d=	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.
len	Displays the packet's length.
sending rcvd fragment sending broad/multicast proto unroutable	The last part of each line lists the status of the packet.
TCP src=	Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.
UDP src=	Displays the source and destination ports for the UDP packets.
ICMP type=	Displays the ICMP type and code.
IP Fragment	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.

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 (refer to the following example). 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 (refer to the following example).

Example

```
FTOS#debug ip packet access-group test
%Error: port operator GT not supported in access-list debug
%Error: port operator LT not supported in access-list debug
%Error: port operator RANGE not supported in access-list debug
%Error: port operator NEQ not supported in access-list debug

FTOS#00:10:45: %RPM0-P:CP %IPMGR-3-DEBUG_IP_PACKET_ACL_AMBIGUOUS_EXP: Ambig-
uous rules not supported in access-list debug, access-list debugging is
turned off
FTOS#
```

ip address

C **E** **S**

Assign a primary and secondary IP address to the interface.

Syntax `ip address ip-address mask [secondary]`

To delete an IP address from an interface, use the **no ip address** [*ip-address*] command.

Parameters

ip-address Enter an IP address in dotted decimal format.

mask Enter the mask of the IP address in slash prefix format (for example, /24).

secondary (OPTIONAL) Enter the keyword **secondary** to designate the IP address as the secondary address.

Defaults Not configured.

Command Modes INTERFACE

Command History

Version 8.1.1.0 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

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

C **E** **S**

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

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

ip domain-list



Configure names to complete unqualified host names.

Syntax `ip domain-list name`

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

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

Defaults Disabled.

Command Modes CONFIGURATION

Command History

Version 8.1.1.0	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 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

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 To fully enable DNS, also specify one or more domain name servers with the [ip name-server](#) command.

FTOS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

To view current bindings, use the [show hosts](#) command.

Related Commands

ip name-server	Specify a DNS server.
show hosts	View current bindings.

ip domain-name

C **E** **S** Configure one domain name for the switch.

Syntax **ip domain-name** *name*

To remove the domain name, enter **no ip domain-name**.

Parameters

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

Defaults Not configured.

Command Modes CONFIGURATION

Command History

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 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

ip domain-list	Configure additional names.
--------------------------------	-----------------------------

ip fib download-igp-only

- E** Configure the E-Series to download only IGP routes (for example, OSPF) on to line cards. When the command is configured or removed, it clears the routing table (similar to [clear ip route](#) command) and only IGP routes populate the table.

Syntax **ip fib download-igp-only [small-fib]**

To return to default setting, use the **no ip fib download-igp-only [small-fib]** command.

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

- C** **E** **S** Specify the address of a DHCP server so that DHCP broadcast messages can be forwarded when the DHCP server is not on the same subnet as the client.

Syntax **ip helper-address ip-address | default-vrf**

To remove a DHCP server address, enter **no ip helper-address**.

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
Version 7.5.1.0	Added support for C-Series
pre-Version 6.2.1.1	Introduced on E-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.

FTOS uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and FTOS forwards to the client with source port=67, destination port=68.

ip helper-address hop-count disable

C **E** **S** 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

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
Version 6.3.1.0	Introduced for E-Series

Usage Information

This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through FTOS. If the incoming boot request already has a non-zero hops field, the message will be relayed with the same value for hops. However, the message will be discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.

Related Commands

ip helper-address	Specify the destination broadcast or host address for DHCP server requests.
show running-config	Display the current configuration and changes from default values.

ip host

C **E** **S** Assign a name and IP address to be used by the host-to-IP address mapping table.

Syntax **ip host *name ip-address***

To remove an IP host, use the **no ip host *name [ip-address]*** command.

Parameters

<i>name</i>	Enter a text string to associate with one IP address.
<i>ip-address</i>	Enter an IP address, in dotted decimal format, to be mapped to the name.

Defaults Not 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

ip max-frag-count

C **E** **S**

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

E

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

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 6.1.1.0	Introduced for E-Series

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.

Table 26-56. Difference between Link MTU and IP MTU

Layer 2 Overhead	Difference between Link MTU and IP MTU
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

Related Commands

[mtu](#)

Set the link MTU for an Ethernet interface.

ip name-server

C **E** **S**

Enter up to 6 IPv4 addresses of name servers. The order you enter the addresses determines the order of their use.

Syntax `ip name-server ipv4-address [ipv4-address2...ipv4-address6]`

To remove a name server, use the **no ip name-server *ip-address*** command.

Parameters

ipv4-address Enter the IPv4 address, in dotted decimal format, of the name server to be used.

ipv4-address2... (OPTIONAL) Enter up five more IPv4 addresses, in dotted decimal format, of name servers to be used.

ipv4-address6 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

FTOS 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](#) Configure an IPv6 name server.

ip proxy-arp

C **E** **S**

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

Related Commands

[show ip interface](#) Displays the interface routing status and configuration.

ip redirects

E

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

Version 8.1.1.0	Introduced on E-Series ExaScale
pre-Version 6.1.1.0	Introduced for E-Series

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

C **E** **S**

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

<i>vrf name</i>	(OPTIONAL) E-Series Only: Enter the keyword vrf followed by the VRF Instances name to tie the static route to the VRF instance.
<i>destination</i>	Enter the IP address in dotted decimal format of the destination device.
<i>mask</i>	Enter the mask in slash prefix formation (/x) of the destination device's IP address.
<i>ip-address</i>	Enter the IP address in dotted decimal format of the forwarding router.
<i>interface</i>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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 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.
<i>distance</i>	(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 <i>tag-value</i>	(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

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 7.9.1.0	Introduced VRF on the E-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 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

C **E** **S** Enable FTOS to forward IP packets with source route information in the header.

Syntax **ip source-route**

To drop packets with source route information, enter **no ip route-source**.

Defaults Enabled.

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

ip unreachable

C **E** **S** Enable the generation of Internet Control Message Protocol (ICMP) unreachable messages.

Syntax **ip unreachable**

To disable the generation of ICMP messages, enter **no ip unreachable**.

Defaults Disabled

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 6.1.1.0	Introduced on E-Series

ip vlan-flooding

E Enable unicast data traffic flooding on VLAN member ports.

Syntax **ip vlan-flooding**
To disable, use the **no ip vlan-flooding** command.

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 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)

C S By default for C-Series and S-Series, FTOS 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

Version 7.6.1.0	Added support for S-Series
Version 7.5.1.0	Introduced on C-Series

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](#) Change the algorithm used to distribute traffic flows across a Port Channel.

load-balance (E-Series)

E By default, for E-Series chassis, FTOS 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 **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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 6.1.1.0	Introduced for E-Series

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 26-57. Configurations of the load-balance Command

Configuration	Switched IP Traffic	Routed IP Traffic (IPv4 Only)	Switched Non-IP Traffic
Default (IP 5-tuple)	IP 5-tuple	IP 5-tuple	MAC based
ip-selection 3-tuple	IP 3-tuple	IP 3-tuple	MAC based
mac	MAC based	IP 5-tuple	MAC based
ip-selection 3-tuple and mac	MAC based	IP 3-tuple	MAC based
ip-selection packet-based	Packet based: IPv4 No distribution: IPv6	Packet based: IPv4	MAC based
ip-selection packet-based and mac	MAC based	Packet based: IPv4	MAC based

Related Commands [ip address](#) Change the algorithm used to distribute traffic on an E-Series chassis.

management route

C **E** 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

<i>{ ipv4-address ipv6-address } / mask</i>	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.
<i>forwarding-router-address</i>	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
Version 7.5.1.0	Support added for C-Series
pre-Version 6.1.1.0	Introduced for E-Series

Usage Information When a static route (or a protocol route) overlaps with Management static route, the static route (or a protocol route) is preferred over the Management Static route. Also, Management static routes and the Management Connected prefix are not reflected in the hardware routing tables. Separate routing tables are maintained for IPv4 and IPv6 management routes. This command manages both tables.

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.
speed (Management interface)	Set the speed for the Management interface.

show arp

C **E** **S** Display the ARP table.

Syntax **show arp** [*vrf vrf name*][**interface** *interface* | **ip** *ip-address* [*mask*] | **macaddress** *mac-address* [*mac-address mask*]] [**cpu** { **cp** | **rp1** | **rp2** }] [**static** | **dynamic**] [**summary**]

Parameters

<i>vrf name</i>	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: <ul style="list-style-type: none">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 <i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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: <p>C-Series and S-Series Range: 1-128 E-Series Range: 1 to 255 for TeraScale and 1 to 512 for ExaScale.</p> 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.
ip <i>ip-address mask</i>	(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 <i>mac-address mask</i>	(OPTIONAL) Enter the keyword macaddress followed by a MAC address in nn:nn:nn:nn:nn:nn format. Enter the optional MAC address mask in nn:nn:nn:nn:nn format also.
static	(OPTIONAL) Enter the keyword static to view entries entered manually.
dynamic	(OPTIONAL) Enter the keyword dynamic to view dynamic entries.
summary	(OPTIONAL) Enter the keyword summary to view a summary of ARP entries.

Command Modes EXEC Privilege

Command History

Version 8.2.1.0	Support 4094 VLANs on E-Series ExaScale (prior limit was 2094)
Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.9.1.0	Introduced VRF on the E-Series
Version 7.8.1.0	Augmented to display local ARP entries learned from private VLANs (PVLANS)
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

The following example shows two VLANs that are associated with a private VLAN (PVLAN) (refer to [Chapter 47, Private VLAN \(PVLAN\)](#)), a feature added for C-Series and S-Series in FTOS 7.8.1.0.

Example 1 (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	192.2.1.251	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
```

Example 2
(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
```

Example 3
(cpu cp)

```
FTOS#sho arp cpu cp
Protocol Address Age(min) Hardware Address Interface VLAN CPU
-----
Internet 10.1.2.206 0 00:a0:80:00:15:b8 Ma 0/0 - CP
Internet 182.16.1.20 0 00:30:19:24:2d:70 Gi 8/0 - CP
Internet 100.10.10.10 0 00:30:19:4f:d3:80 Gi 8/12 - CP
Internet 10.1.2.209 12 00:a0:80:00:12:6c Ma 0/0 - CP
FTOS#
```

Table 26-58. show arp Command Example Fields

Row Heading	Description
Protocol	Displays the protocol type.
Address	Displays the IP address of the ARP entry.
Age(min)	Displays the age in minutes of the ARP entry.
Hardware Address	Displays the MAC address associated with the ARP entry.
Interface	Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.
VLAN	Displays the VLAN ID, if any, associated with the ARP entry.
CPU	Lists which CPU the entries are stored on.

Example 4
(summary)

```
FTOS# show arp summary
Total Entries Static Entries Dynamic Entries CPU
-----
83 0 83 CP
FTOS
```

Table 26-59. show arp summary Command Example Fields

Row Heading	Description
Total Entries	Lists the total number of ARP entries in the ARP table.
Static Entries	Lists the total number of configured or static ARP entries.
Dynamic Entries	Lists the total number of learned or dynamic ARP entries.
CPU	Lists which CPU the entries are stored on.

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

C **E** **S** Display the configured number of ARP retries.

Syntax **show arp retries**

Command Modes EXEC

EXEC Privilege

Command History Version 8.3.1.0 Introduced

Related Commands [arp retries](#) Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

show hosts

C **E** **S** View the host table and DNS configuration.

Syntax **show hosts**

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

```
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 26-60. show hosts Command Example Fields

Field	Description
Default domain...	Displays the domain name (if configured).
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.

Table 26-60. show hosts Command Example Fields (Continued)

Field	Description
Name servers are...	Lists the name servers, if configured.
Host	Displays the host name assigned to the IP address.
Flags	Classifies the entry as one of the following: <ul style="list-style-type: none"> • perm - the entry was manually configured and will not time out • temp - the entry was learned and will time out after 72 hours of inactivity. Also included in the flag is an indication of the validity of the route: <ul style="list-style-type: none"> • ok - the entry is valid. • ex - the entry expired. • ?? - the entry is suspect.
TTL	Displays the amount of time until the entry ages out of the cache. For dynamically learnt entries only.
Type	Displays IP as the type of entry.
Address	Displays the IP address(es) assigned to the host.

Related Commands

traceroute	View DNS resolution
ip host	Configure a host.

show ip cam linecard

C E 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

<i>number</i>	Enter the number of the line card. Range: 0 to 13 on a E1200/1200i, 0 to 6 on a E600600i, and 0 to 5 on a E300.
<i>pipe-number</i>	Enter the number of the line card's port-pipe. Range: 0 to 1
<i>ip-address mask [longer-prefix]</i>	(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 <i>index-number</i>	(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.
<i>vrf instance</i>	(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
 Version 7.5.1.0 Introduced on C-Series
 pre-Version 6.1.1.0 Introduced for E-Series

Example FTOS#show ip cam linecard 13 port-set 0

```

  Index   Destination   EC CG V C   Next-Hop   VId   Mac-Addr   Port
  -----
  3276    6.6.6.2     0 0 1 1     0.0.0.0   0 00:00:00:00:00:00 17c1 CP
  3277    5.5.5.2     0 0 1 1     0.0.0.0   0 00:00:00:00:00:00 17c1 CP
  3278    4.4.4.2     0 0 1 1     0.0.0.0   0 00:00:00:00:00:00 17c1 CP
  3279    3.3.3.2     0 0 1 1     0.0.0.0   0 00:00:00:00:00:00 17c1 CP
  3280    2.2.2.2     0 0 1 1     0.0.0.0   0 00:00:00:00:00:00 17c1 CP
  11144   6.6.6.0     0 0 1 1     0.0.0.0   6 00:00:00:00:00:00 17c5 RP2
  11145   5.5.5.0     0 0 1 1     0.0.0.0   5 00:00:00:00:00:00 17c5 RP2
  11146   4.4.4.0     0 0 1 1     0.0.0.0   4 00:00:00:00:00:00 17c5 RP2
  11147   3.3.3.0     0 0 1 1     0.0.0.0   3 00:00:00:00:00:00 17c5 RP2
  11148   2.2.2.0     0 0 1 1     0.0.0.0   2 00:00:00:00:00:00 17c5 RP2
  65535   0.0.0.0     0 0 1 1     0.0.0.0   0 00:00:00:00:00:00 17c5 RP2
  FTOS#
  
```

Table 26-61. show ip cam Command Example Fields

Field	Description
Index	Displays the CAM index number of the entry.
Destination	Displays the destination route of the index.
EC	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.
CG	Displays 0.
V	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.
C	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP or RP2, depending on Egress port.
Next-Hop	Displays the next hop IP address of the entry.
VId	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
Mac Addr	Displays the next-hop router's MAC address.
Port	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

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

```

Prefix Len Current Use Initial Sz
-----
32          7      37994
31          0       1312
30          0       3932
29          0       1312
28          0       1312
27          0       1312
26          0       1312
25          0       1312
24          6      40610
23          0       3932
22          0       2622
21          0       2622
20          0       2622
19          0       2622
18          0       1312
17          0       1312
16          0       3932
15          0       1312
14          0       1312
13          0       1312
12          0       1312
11          0       1312
10          0       1312
9           0       1312
8           0       1312
7           0       1312
6           0       1312
5           0       1312
4           0       1312
3           0       1312
2           0       1312
1           0       1312
0           0         8

```

FTOS#

Table 26-62. show ip cam summary Command Example Fields

Field	Description
Prefix Length	Displays the prefix-length or mask for the IP address configured on the linecard 0 port pipe 0.
Current Use	Displays the number of routes currently configured for the corresponding prefix or mask on the linecard 0 port pipe 0.
Initial Size	Displays the CAM size allocated by FTOS for the corresponding mask. The CAM size is adjusted by FTOS if the number of routes for the mask exceeds the initial allocation.

show ip cam stack-unit

S 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

0-7 Enter the stack-unit ID, from 0 to 7.

pipe-number Enter the number of the Port-Pipe number.
S50n, S50V range: 0 to 1; S25N, S25P, S25V range: 0 to 0

ip-address mask [longer-prefix] (OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only.
Enter the keyword **longer-prefixes** to view routes with a common prefix.

summary (OPTIONAL) Enter the keyword **summary** to view a table listing route prefixes and the total number routes which can be entered in to CAM.

Command Modes

EXEC
EXEC Privilege

Command History

Version 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 cam stack-unit 0 port-set 0 10.10.10.10/32 longer-prefixes

```

Destination      EC CG V C  VId      Mac-Addr      Port
-----
10.10.10.10      0  0 1 1    0 00:00:00:00:00:00  3f01  CP
FTOS#

```

Table 26-63. show ip cam Command Example Fields

Field	Description
Destination	Displays the destination route of the index.
EC	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.
CG	Displays 0.
V	Displays a 1 if the entry is valid and a 0 otherwise.
C	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the control processor, depending on Egress port.
V Id	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
Mac Addr	Displays the next-hop router's MAC address.
Port	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

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]`

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

FTOS>show ip fib linecard 12

Destination	Gateway	First-Hop	Mac-Addr	Port	VIId	Index	EC
3.0.0.0/8	via 100.10.10.10, So 2/8	100.10.10.10	00:01:e8:00:03:ff	So 2/8	0	60260	0
3.0.0.0/8	via 101.10.10.10, So 2/9						
100.10.10.0/24	Direct, So 2/8	0.0.0.0	00:01:e8:00:03:ff	So 2/8	0	11144	0
100.10.10.1/32	via 127.0.0.1	127.0.0.1	00:00:00:00:00:00	CP	0	3276	0
100.10.10.10/32	via 100.10.10.10, So 2/8	100.10.10.10	00:01:e8:00:03:ff	So 2/8	0	0	0
101.10.10.0/24	Direct, So 2/9	0.0.0.0	00:00:00:00:00:00	RP2	0	11145	0
101.10.10.1/32	via 127.0.0.1	127.0.0.1	00:00:00:00:00:00	CP	0	3277	0
101.10.10.10/32	via 101.10.10.10, So 2/9	101.10.10.10	00:01:e8:01:62:32	So 2/9	0	1	0

FTOS>

Table 26-64. show ip fib linecard Command Example Fields

Field	Description
Destination	Lists the destination IP address.
Gateway	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.
First-Hop	Displays the first hop IP address.
Mac-Addr	Displays the MAC address.
Port	Displays the egress-port information.

Table 26-64. show ip fib linecard Command Example Fields

Field	Description
VId	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
Index	Displays the internal interface number.
EC	Displays the number of ECMP paths.

Related Commands

[clear ip fib linecard](#) Clear FIB entries on a specified line card.

show ip fib stack-unit

S 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 26-65. show ip fib linecard Command Example Fields

Field	Description
Destination	Lists the destination IP address.
Gateway	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.
First-Hop	Displays the first hop IP address.

Table 26-65. show ip fib linecard Command Example Fields

Field	Description
Mac-Addr	Displays the MAC address.
Port	Displays the egress-port information.
VId	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
EC	Displays the number of ECMP paths.

Related Commands

[clear ip fib linecard](#) Clear FIB entries on a specified line card.

show ip flow

C **E** **S**

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.
(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 8.1.1.0 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 packets 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

```
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 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.

brief

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

linecard (OPTIONAL) Enter the keyword **linecard** followed by the number of the line card slot.
slot-number C-Series Range: 0-7
 E-Series Range: 0 to 13 on a E1200/1200i, 0 to 6 on a E600/E600i, and 0 to 5 on a E300
Note: This keyword is not available on the S-Series.

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

Command Modes EXEC
 EXEC Privilege

Command History

Version 8.1.1.2	Supported on E-Series ExaScale E600i
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 1

```
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 unreachable are not sent

FTOS#
```

Table 26-66. show ip interface Command Example Items

Lines	Description
TenGigabitEthernet 0/0...	Displays the interface's type, slot/port and physical and line protocol status.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
IP MTU is...	Displays IP MTU value.
Inbound access...	Displays the name of the any configured incoming access list. If none is configured, the phrase "not set" is displayed.
Proxy ARP...	States whether proxy ARP is enabled on the interface.
Split horizon...	States whether split horizon for RIP is enabled on the interface.
Poison Reverse...	States whether poison for RIP is enabled on the interface
ICMP redirects...	States if ICMP redirects are sent.
ICMP unreachable...	States if ICMP unreachable messages are sent.

Example 2 (brief)

```
FTOS#show ip int brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet 1/0      unassigned      NO  Manual administratively down down
GigabitEthernet 1/1      unassigned      NO  Manual administratively down down
GigabitEthernet 1/2      unassigned      YES Manual up          up
```

```
GigabitEthernet 1/3    unassigned    YES Manual up          up
GigabitEthernet 1/4    unassigned    YES Manual up          up
GigabitEthernet 1/5    10.10.10.1   YES Manual up          up
GigabitEthernet 1/6    unassigned    NO  Manual administratively down down
```

Table 26-67. show ip interface brief Column Headings

Field	Description
Interface	Displays type of interface and the associated slot and port number.
IP-Address	Displays the IP address for the interface, if configured.
Ok?	Indicates if the hardware is functioning properly.
Method	Displays Manual if the configuration is read from the saved configuration.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.

show ip management-route

C **E** View the IP addresses assigned to the Management interface.

Syntax `show ip management-route [all | connected | summary | static]`

Parameters

all (OPTIONAL) Enter the keyword **all** to view all IP addresses assigned to all Management interfaces on the switch.

connected (OPTIONAL) Enter the keyword **connected** to view only routes directly connected to the Management interface.

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

Example

```
FTOS#show ip management-route

Destination          Gateway              State
-----
10.1.2.0/24          ManagementEthernet 0/0    Connected
172.16.1.0/24        10.1.2.4            Active

FTOS#
```

show ipv6 management-route

C **E** 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

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 protocols

C **E** **S** View information on all routing protocols enabled and active on the switch.

Syntax `show ip protocols`

Command Modes EXEC
EXEC Privilege

Command History

Version 8.1.1.0	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
pre-Version 6.1.1.0	Introduced for E-Series

Example

```
FTOS#show ip protocols
Routing Protocol is "bgp 1"
  Cluster Id is set to 20.20.20.3
  Router Id is set to 20.20.20.3
  Fast-external-fallover enabled
  Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
    BGP table version is 0, main routing table version 0
    Distance: external 20 internal 200 local 200
  Neighbor(s):
```

```

Address : 20.20.20.2
Filter-list in : foo
Route-map in : foo
Weight : 0
Address : 5::6
Weight : 0
FTOS#

```

show ip route



View information, including how they were learned, about the IP routes on the switch.

Syntax `show ip route [vrf vrf name] hostname | ip-address [mask] [longer-prefixes] | list prefix-list | protocol [process-id | routing-tag] | all | connected | static | summary]`

Parameter

<i>vrf name</i>	E-Series Only: Clear only the route entries tied to the VRF process.
<i>ip-address</i>	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
<i>mask</i>	(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. Refer to show ip route list .
<i>protocol</i>	(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 <i>as-number</i> . (E-Series only) If you enter isis , you can include the ISIS <i>routing-tag</i> . (E-Series only) If you enter ospf , you can include the OSPF <i>process-id</i> .
<i>process-id</i>	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
<i>routing-tag</i>	(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 . Refer to show ip route summary .

Command Modes

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 7.6.1.0	Introduced on S-Series
Version 7.5.1.0	Introduced on C-Series
pre-Version 6.1.1.0	Introduced for E-Series

**Example 1
(all)**

```
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
```

	Destination	Gateway	Dist/Metric	Last Change
	-----	-----	-----	-----
R	3.0.0.0/8	via 100.10.10.10, So 2/8 via 101.10.10.10, So 2/9	120/1	00:07:12
C	100.10.10.0/24	Direct, So 2/8	0/0	00:08:54
> R	100.10.10.0/24	Direct, So 2/8	120/0	00:08:54
C	101.10.10.0/24	Direct, So 2/9	0/0	00:09:15
> R	101.10.10.0/24	Direct, So 2/9	120/0	00:09:15

FTOS#

**Example 2
(summary &
static)**

```
FTOS#show ip route summary
Route Source      Active Routes  Non-active Routes
connected         2              0
static            1              0
Total             3              0
```

Total 3 active route(s) using 612 bytes

```
R1_E600i>show ip route static ?
```

```
| Pipe through a command
<cr>
```

```
R1_E600i>show ip route static
```

	Destination	Gateway	Dist/Metric	Last Change
	-----	-----	-----	-----
*S	0.0.0.0/0	via 10.10.91.9, Gi 1/2	1/0	3d2h

FTOS>

Table 26-68. show ip route all Command Example Fields

Field	Description
(undefined)	Identifies the type of route: <ul style="list-style-type: none"> • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IP address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

show ip route list

C **E** **S** 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

Related Commands

[ip prefix-list](#) Enter the CONFIGURATION-IP PREFIX-LIST mode and configure a prefix list.

[show ip prefix-list summary](#) Display a summary of the configured prefix lists.

Example FTOS#show ip route list test

Codes: C - connected, S - static, R - RIP,
 B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated,
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
 E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
 L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default,
 > - non-active route, + - summary route

Gateway of last resort is not set

	Destination	Gateway	Dist/Metric	Last Change
	-----	-----	-----	-----
R	2.1.0.0/24	via 2.1.4.1, Gi 4/43	120/2	3d0h
R	2.1.1.0/24	via 2.1.4.1, Gi 4/43	120/2	3d1h
R	2.1.2.0/24	via 2.1.4.1, Gi 4/43	120/1	3d0h
R	2.1.3.0/24	via 2.1.4.1, Gi 4/43	120/1	3d1h
C	2.1.4.0/24	Direct, Gi 4/43	0/0	3d1h

show ip route summary

C **E** **S** 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 FTOS>show ip route summary

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

Table 26-69. show ip route summary Column Headings

Column Heading	Description
Route Source	Identifies how the route is configured in FTOS.
Active Routes	Identifies the best route if a route is learned from two protocol sources.
Non-active Routes	Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route will become the best route.
ospf 100	If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
Total 1388 active...	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.

Related Commands

`show ip route` Display information about the routes found in switch.

show ip traffic

C **E** **S** View IP, ICMP, UDP, TCP and ARP traffic statistics.

Syntax `show ip traffic [all | cp | rp1 | rp2]`

Note: These options are supported only on the E-Series.

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

Example

```
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
Frag: 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 26-70. show ip traffic output definitions

Keyword	Definition
unknown protocol...	No receiver for these packets. Counts those packets whose protocol type field is not recognized by FTOS.
not a gateway...	Packets can not be routed; host/network is unreachable.
security failures...	Counts the number of received unicast/multicast packets that could not be forwarded due to: <ul style="list-style-type: none"> route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group destination IP address belongs to reserved prefixes; host/network unreachable
bad options...	Unrecognized IP option on a received packet.
Fraggs:	IP fragments received.
... reassembled	Number of IP fragments that were reassembled.
... timeouts	Number of times a timer expired on a reassembled queue.
... too big	Number of invalid IP fragments received.
... couldn't fragment	Number of packets that could not be fragmented and forwarded.
...encapsulation failed	Counts those packets which could not be forwarded due to ARP resolution failure. FTOS sends an arp request prior to forwarding an IP packet. If a reply is not received, FTOS repeats the request three times. These packets are counted in encapsulation failed.
Rcvd:	
...short packets	The number of bytes in the packet are too small.
...bad length	The length of the packet was not correct.
...no port broadcasts	The incoming broadcast/multicast packet did not have any listener.
...socket full	The applications buffer was full and the incoming packet had to be dropped.

Usage Information

The F10 Monitoring MIB provides access to the statistics described below.

Table 26-71. F10 Monitoring MIB

Command Display	Object	OIDs
IP statistics:		
Bcast:		
Received	f10BcastPktRecv	1.3.6.1.4.1.6027.3.3.5.1.1
Sent	f10BcastPktSent	1.3.6.1.4.1.6027.3.3.5.1.2
Mcast:		
Received	f10McastPktRecv	1.3.6.1.4.1.6027.3.3.5.1.3
Sent	f10McastPktSent	1.3.6.1.4.1.6027.3.3.5.1.4
ARP statistics:		
Rcvd:		
Request	f10ArpReqRecv	1.3.6.1.4.1.6027.3.3.5.2.1
Replies	f10ArpReplyRecv	1.3.6.1.4.1.6027.3.3.5.2.3
Sent:		
Request	f10ArpReqSent	1.3.6.1.4.1.6027.3.3.5.2.2
Replies	f10ArpReplySent	1.3.6.1.4.1.6027.3.3.5.2.4
Proxy	f10ArpProxySent	1.3.6.1.4.1.6027.3.3.5.2.5

show protocol-termination-table

E 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

Command History

Version 8.1.1.2 Introduced support for E-Series ExaScale E600i
 Version 8.1.1.0 Introduced on E-Series ExaScale
 Version 6.4.1.0 Introduced

Example

```

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      UDP       any       67       Q7      6   No        -         CP
4      TCP       any       22       Q7      6   No        -         CP
5      TCP       22       any      Q7      6   No        -         CP
6      TCP       639      any      Q7      6   No        -         RP2
7      TCP       any      639     Q7      6   No        -         RP2
8      TCP       646      any      Q7      6   No        -         RP1
9      TCP       any      646     Q7      6   No        -         RP1
10     UDP       646      any      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       69       any     Q7      6   No        -         CP
25     TCP       any     161     Q7      6   No        -         CP
26     TCP       161      any     Q7      6   No        -         CP
27     TCP       162      any     Q7      6   No        -         CP
28     TCP       any     162     Q7      6   No        -         CP
29     UDP       any     161     Q7      6   No        -         CP
30     UDP       161      any     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     IGMP     any      any     Q7      6   No        -         RP2
35     OSPF     any      any     Q7      6   No        -         RP1
36     RSVP     any      any     Q7      6   No        -         RP1
FTOS#

```

Usage Information

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

Related Commands

[show ip cam stack-unit](#) Display the CAM table

show tcp statistics

C **E** **S** 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.

rp1 Enter the keyword **rp1** to view only TCP statistics from Route Processor 1.

rp2 Enter the keyword **rp2** to view only TCP statistics from Route Processor 2.

Command Modes EXEC Privilege

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale

Version 6.4.1.0 Introduced

Example FTOS#show tcp stat cp

```
Control Processor TCP:
Rcvd: 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 26-72. show tcp statistics cp Command Example Fields

Field	Description
Rcvd:	Displays the number and types of TCP packets received by the switch. <ul style="list-style-type: none"> Total = total packets received no port = number of packets received with no designated port.
0 checksum error...	Displays the number of packets received with the following: <ul style="list-style-type: none"> checksum errors bad offset to data too short

Table 26-72. show tcp statistics cp Command Example Fields (Continued)

Field	Description
329 packets...	Displays the number of packets and bytes received in sequence.
17 dup...	Displays the number of duplicate packets and bytes received.
0 partially...	Displays the number of partially duplicated packets and bytes received.
7 out-of-order...	Displays the number of packets and bytes received out of order.
0 packets with data after window	Displays the number of packets and bytes received that exceed the switch's window size.
0 packets after close	Displays the number of packet received after the TCP connection was closed.
0 window probe packets...	Displays the number of window probe and update packets received.
41 dup ack...	Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.
10184 ack...	Displays the number of acknowledgement packets and bytes received.
Sent:	Displays the total number of TCP packets sent and the number of urgent packets sent.
25 control packets...	Displays the number of control packets sent and the number retransmitted.
11603 data packets...	Displays the number of data packets sent.
24 data packets retransmitted	Displays the number of data packets resent.
355 ack...	Displays the number of acknowledgement packets sent and the number of packet delayed.
0 window probe...	Displays the number of window probe and update packets sent.
7 Connections initiated...	Displays the number of TCP connections initiated, accepted, and established.
14 Connections closed...	Displays the number of TCP connections closed, dropped.
20 Total rxmt...	Displays the number of times the switch tried to resend data and the number of connections dropped during the TCP retransmit timeout period.
0 Keepalive	Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.

IPv6 Access Control Lists (IPv6 ACLs)

Overview

IPv6 ACLs and IPv6 Route Map commands are supported on platforms: C E S

- [IPv6 ACL Commands](#)
- [IPv6 Route Map Commands](#)



Note: For IPv4 ACL commands, refer to [Chapter 10, 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

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.

Command Modes

CONFIGURATION

Command History

Version 8.4.2.0 Introduced on the E-Series TeraScale

Version 8.2.1.0 Introduced on the S-Series

Version 7.8.1.0 Introduced on the C-Series

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).

clear counters ipv6 access-group

C **E** **S** 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

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

deny

C **E** **S** 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

<i>ip-protocol-number</i>	Enter an IPv6 protocol number. Range: 0 to 255
icmp	Enter the keyword icmp to deny Internet Control Message Protocol version 6.
ipv6	Enter the keyword ipv6 to deny any Internet Protocol version 6.
tcp	Enter the keyword tcp to deny the Transmission Control protocol.
udp	Enter the keyword udp to deny the User Datagram Protocol.

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

deny icmp



Configure a filter to drop all or specific ICMP messages.

Syntax

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

<i>source address</i>	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.
<i>mask</i>	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
<i>destination address</i>	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.
<i>message-type</i>	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: 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 have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword monitor to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured

Command Modes ACCESS-LIST

Command History

Version 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.

The following table lists the keywords displayed in the CLI help and their corresponding ICMP Message Type Name.

Table 27-73. ICMP Message Type Keywords

Keyword	ICMP Message Type Name
dest-unreachable	Destination unreachable
echo	Echo request (ping)
echo-reply	Echo reply
inverse-nd-na	Inverse neighbor discovery advertisement
inverse-nd-ns	Inverse neighbor discovery solicitation
log	Log matches against this entry
mobile-advertisement	Mobile prefix advertisement
mobile-solicitation	Mobile prefix solicitation
mrouter-advertisement	Multicast router advertisement
mrouter-solicitation	Multicast router solicitation
mrouter-termination	Multicast router termination
nd-na	Neighbor advertisement
nd-ns	Neighbor solicitation
packet-too-big	Packet is too big
parameter-problem	Parameter problems
redirect	Neighbor redirect
router-advertisement	Neighbor discovery router advertisement
router-renumbering	All routers renumbering
router-solicitation	Neighbor discovery router solicitation
time-exceeded	All time exceeded

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

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

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 <i>ipv6-address</i>	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: <ul style="list-style-type: none"> • 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 <i>port</i> command parameter).
port <i>port</i>	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: <ul style="list-style-type: none"> • 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.
bit	Enter a flag or combination of bits: <ul style="list-style-type: none"> 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. 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	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.

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	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111110000000	7936	7999	64
8	0001111101000000	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

- [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** 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 <i>ipv6-address</i>	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: <ul style="list-style-type: none"> • eq = equal to • neq = not equal to • gt = greater than • lt = less than • range = inclusive range of ports
port <i>port</i>	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535
destination <i>address</i>	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.
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

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.

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:

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256


```

7      0001111100000000 111111111000000 7936 7999 64
8      0001111101000000 1111111111111111 8000 8000 1

```

Total Ports: 4001

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

```

Rule#      Data          Mask          From To      #Covered
1          0000000000000000 111111000000000 0      1023 1024

```

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

C **E** **S** 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).
- 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

Defaults Disabled

Command Modes INTERFACE

Command History

- Version 8.4.2.1 Introduced on the S-Series
- Version 7.8.1.0 Introduced 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 on the E-Series TeraScale

Usage Information

You can assign an IPv6 access group to a physical, LAG, or VLAN interface context.

Example

```
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

C **E** 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

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 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 on the E-Series TeraScale

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.

Related Commands [show config](#) View the current configuration.

permit

C **E** 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

<i>ip-protocol-number</i>	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

C **E** **S**

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

<i>source address</i>	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.
<i>mask</i>	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
<i>destination address</i>	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.
<i>message-type</i>	(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 have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword monitor to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured

Command Modes ACCESS-LIST

Command History

Version 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.

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.

Parameters

<i>source address</i>	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 The :: notation specifies successive hexadecimal fields of zero.
<i>mask</i>	Enter a network mask in /prefix format (/x).
any	Enter the keyword any to specify that all routes are subject to the filter.
host ipv6-address	Enter the keyword host followed by the IPv6 address of the host in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zero
<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"> • 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 <i>port</i> parameter.)
<i>port port</i>	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.

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

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.

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	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	7680	7935	256
7	0001111100000000	1111111110000000	7936	7999	64
8	0001111101000000	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.

Parameters

<i>source address</i>	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 The :: notation specifies successive hexadecimal fields of zero.
<i>mask</i>	Enter a network mask in /prefix format (/x).
any	Enter the keyword any to specify that all routes are subject to the filter.
<i>host ipv6-address</i>	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
<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"> • 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 <i>port</i> parameter.)
<i>port port</i>	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535
<i>destination address</i>	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.
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:

Rule#	Data	Mask	From	To	#Covered
1	0000111110100000	1111111111100000	4000	4031	32
2	0000111111000000	1111111111100000	4032	4095	64
3	0001000000000000	1111100000000000	4096	6143	2048
4	0001100000000000	1111110000000000	6144	7167	1024
5	0001110000000000	1111111000000000	7168	7679	512
6	0001111000000000	1111111100000000	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 IP packets.

[permit tcp](#) Assign a permit filter for TCP packets.

remark

C **E** **S**

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

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

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

C **E** **S**

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.

<i>access-list-name</i>	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.
<i>StartingSeqNum</i>	Enter the starting sequence number to resequence. Range: 0 - 4294967290
<i>Step-to-Increment</i>	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

resequence prefix-list ipv6

C **E** **S** Re-assign sequence numbers to entries of an existing prefix list.

Syntax `resequence prefix-list ipv6 { prefix-list-name StartingSeqNum Step-to-increment }`

Parameters

<i>prefix-list-name</i>	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.
<i>StartingSeqNum</i>	Enter the starting sequence number to resequence. Range: 0 – 65535
<i>Step-to-Increment</i>	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

seq

C **E** **S**

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

<i>sequence-number</i>	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.
<i>ipv6-protocol-number</i>	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.
<i>source address</i>	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.
<i>mask</i>	Enter a network mask in /prefix format (/X).
any	Enter the keyword any to specify that all routes are subject to the filter.
host <i>ipv6-address</i>	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
<i>operator</i>	(OPTIONAL) Enter one of the following logical operands: <ul style="list-style-type: none"> • 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 <i>port</i> 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

Version 8.4.2.1	Introduced on the E-Series TeraScale and 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	Added monitor option

Related Commands

deny	Configure a filter to drop packets.
permit	Configure a filter to forward packets.

show cam-acl

C **E** **S** 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**Example 1
(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          :          5
Ipv4Acl        :          6
Ipv6Acl        :          0
Ipv4Qos        :          1
L2Qos          :          1

FTOS#show cam-acl

```

**Example 2
(manually-set
profile)**

```

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**

Version 8.4.2.1 Introduced on the S-Series

Version 8.4.2.0	Introduced on the E-Series TeraScale
Version 8.2.1.0	Introduced on the E-Series ExaScale
Version 7.8.1.0	Introduced on the C-Series

Example

```

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

C **E** **S** 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

<i>access-list-name</i>	Enter the name of the ACL to be displayed, up to 140 characters.
<i>cam_count</i>	List the count of the CAM rules for this ACL.
<i>interface interface</i>	Enter the keyword interface followed by the interface type and slot/port or number information: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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.

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
	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 on the E-Series TeraScale

Example

```

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 27-74. show ip accounting access-lists Command Example Field

Field	Description
“Ingress IPv6...”	Displays the name of the IPv6 ACL, in this example “AcList1”.
“seq 10...”	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.

show running-config acl

C **E** **S** Display the ACL running configuration.

Syntax `show running-config acl`

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 support on the E-Series TeraScale

Example

```
FTOS#show running-config acl
!
ip access-list extended ext-acl1
!
ip access-list standard std-acl1
!
ipv6 access-list Ac11
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

C **E** **S** Verify that enough ACL 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 line cards, or enter the line card *number* to get information for a specific card.
Range: 0-6 for E-Series, 0-7 for C-Series

Defaults None

Command Modes 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 C-Series and E-Series TeraScale

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.

```
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#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#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

Table 27-75. Output Explanations: test cam-usage

Term	Explanation
Linecard	Lists the line card or line cards that are checked. Entering all shows the status for line cards in the chassis
Portpipe	Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering all shows the status for line cards and port-pipes in the chassis.

Table 27-75. Output Explanations: test cam-usage

Term	Explanation
CAM Partition	Shows the CAM profile of the CAM
Available CAM	Identifies the amount of CAM space remaining for that profile
Estimated CAM per Port	Estimates the amount of CAM space the listed policy will require.
Status	Indicates whether or not the policy will be allowed in the CAM

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

C **E** **S**

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	Redistribute routes that match the next-hop IP address.
match ipv6 route-source	Redistribute routes that match routes advertised by other routers.

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 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.

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 next-hop	Redistribute routes that match the next-hop IP address.

route-map

C **E** **S**

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

map-name Enter a text string to name the route map, 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

Example

```
FTOS ( conf ) #route-map Rmap1
FTOS ( config-route-map ) #match ?
...
ip                IP specific information
ipv6              IPv6 specific information
...
```

Related Commands

[show config](#) View the current configuration.

set ipv6 next-hop

C **E** **S**

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

ipv6-address Enter the IPv6 address in the **X:X:X::X** format.
Note: The **::** notation specifies successive hexadecimal fields of zeros

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
Version 7.4.1.0	Introduced support on the E-Series TeraScale

Usage Information

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

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

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

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

Example

```
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. [Table 25-2, "FTOS and IPv6 Feature Support," in IPv6 Addressing](#) in the Configuration Guide for information on the FTOS version and platform that supports IPv6 in each software feature.

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

C E S Clear (refresh) all FIB entries on a linecard.

Syntax `clear ipv6 fib linecard slot`

Parameters *slot* Enter the slot number to clear the FIB for a linecard.

Command Mode EXEC Privilege

Command History

Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on C-Series and S-Series
Version 7.4.1.0	Introduced on E-Series TeraScale

clear ipv6 route

C **E** **S**

Clear (refresh) all or a specific route from the IPv6 routing table.

Syntax `clear ipv6 route { * | ipv6-address prefix-length }`

Parameters

***** Enter the * to clear (refresh) all routes from the IPv6 routing table.

ipv6-address 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

prefix-length

Command Mode EXEC Privilege

Command History

Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.8.1.0 Introduced on C-Series and S-Series
Version 7.4.1.0 Introduced on E-Series TeraScale

ipv6 address

C **E** **S**

Configure an IPv6 address to an interface.

Syntax `ipv6 address { ipv6-address prefix-length }`

To remove the IPv6 address, use the **no ipv6 address { *ipv6-address prefix-length* }** command.

Parameters

ipv6-address 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

prefix-length

Defaults No default values or behavior

Command Modes INTERFACE

Command History

Version 8.4.1.0 Support added on the management Ethernet port.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.8.1.0 Introduced on C-Series and S-Series
Version 7.4.1.0 Introduced on E-Series TeraScale

Example

```
FTOS(conf)#interface gigabitethernet 10/0
FTOS(conf-if-gi-10/0)#ipv6 address ?
X:X:X:X::X IPv6 address
FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 ?
<0-128> Prefix length in bits
FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96 ?
<cr>
FTOS(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96
FTOS(conf-if-gi-10/0)#show config
!
```

```

interface GigabitEthernet 10/0
  no ip address
  ipv6 address 2002:1:2::3 /96
  no shutdown
FTOS(conf-if-gi-10/0)#

```

Usage Information FTOS 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.

ipv6 name-server

C **E** **S** 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

<i>ipv6-address</i>	Enter the IPv6 address (X:X:X:X::X) of the name server to be used.
<i>ipv6-address2...</i>	Enter up five more IP addresses, in dotted decimal format, of name servers to be used.
<i>ipv6-address6</i>	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

C **E** **S** Assign a name and IPv6 address to be used by the host-to-IP address mapping table.

Syntax **ipv6 host** *name ip-address*

Parameters

<i>name</i>	Enter a text string to associate with one IP address.
<i>ipv6-address</i>	Enter an IPv6 address (X:X:X:X::X) to be mapped to the name.

Defaults Not 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

ipv6 nd prefix-advertisement

C **E** **S**

Specify which IPv6 prefixes are include 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

<i>ipv6-prefix</i>	Enter an IPv6 prefix.
<i>prefix-length</i>	Enter the prefix followed by the prefix length. <i>Length</i> Range: 0-128
default	Enter this keyword to set default parameters for all prefixes.
no-advertise	Enter this keyword to prevent the specified prefix from being advertised.
no-autoconfig	Enter this keyword to disable Stateless Address Autoconfiguration.
no-rtr-address	Enter this keyword to exclude the full router address from router advertisements (the R bit is not set).
off-link	Enter this keyword to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.
<i>valid-lifetime</i> infinite	Enter the amount of time that the prefix is advertised, or enter infinite for an unlimited amount of time. Default: 2592000 Range: 0 to 4294967295
<i>preferred-lifetime</i> infinite	Enter the amount of time that the prefix is preferred, or enter infinite for an unlimited amount of time. Default: 604800 Range: 0 to 4294967295; the maximum value means that the preferred lifetime does not expire.

Command Mode INTERFACE

Command History Version 8.3.2.0 Introduced on the E-Series TeraScale, C-Series, and S-Series.

ipv6 route

C **E** **S**

Establish a static IPv6 route.

Syntax `ipv6 route ipv6-address prefix-length { ipv6-address | interface | interface ipv6-address } [distance] [tag value] [permanent]`

To remove the IPv6 route, use the **no ipv6 route *ipv6-address prefix-length* { *ipv6-address* | *interface* | *interface ipv6-address* } [*distance*] [*tag value*] [**permanent**]** command.

Parameters

<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format.
<i>prefix-length</i>	Range: /0 to /128 Note: The :: notation specifies successive hexadecimal fields of zeros
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none">• 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.
<i>ipv6-address</i>	(OPTIONAL) Enter the forwarding router IPv6 address in the x:x:x:x::x format. Note: The :: notation specifies successive hexadecimal fields of zeros
<i>distance</i>	(OPTIONAL) Enter a number as the distance metric assigned to the route. Range: 1 to 255
<i>tag value</i>	(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

Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on C-Series and S-Series
Version 7.4.1.0	Introduced on E-Series TeraScale

Example

```
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
FTOS#

```

Usage Information

When the interface goes down, FTOS withdraws the route. The route is re-installed, by FTOS, when the interface comes back up. When a recursive resolution is “broken,” FTOS withdraws the route. The route is re-installed, by FTOS, when the recursive resolution is satisfied.

Related Commands

[show ipv6 route](#) View the IPv6 configured routes.

ipv6 unicast-routing

C **E** **S** Enable IPv6 Unicast routing.

Syntax **ipv6 unicast-routing**

To disable unicast routing, use the **no ipv6 unicast-routing** command.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 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

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, FTOS 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

C **E** **S** 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 keyword **port-set** followed by the port-pipe number.
Range: 0 to 1

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

Example 1 (fib)

FTOS#`show ipv6 cam linecard 13 fib`

```
Neighbor                               Mac-Addr           Port           VId
-----
[  31] 2002:44:1:1:1::11                00:00:01:1a:1e:d5 Gi 13/2        0

Prefix                                Next-Hop           Mac-Addr           Port           VId EC
-----
[ 3147] 100::/64                        [  0] 2002:44:1:1:1::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#

```

Example 2

```

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:fe17:5cae          00:01:e8:17:5c:ae 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] :                               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

C **E** **S** 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 keyword **port-set** followed by the port-pipe number.
Range: 0 to 1

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/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

C **E** View all Forwarding Information Base entries.

Syntax `show ipv6 fib linecard slot-number {summary | ipv6-address}`

Parameters

<i>slot-number</i>	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.
<i>ipv6-address</i>	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

Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on C-Series and S-Series
Version 7.4.1.0	Introduced on E-Series TeraScale

show ipv6 fib stack-unit

C **E** **S** View all Forwarding Information Base entries.

Syntax `show ipv6 fib stack-unit unit-number [summary] ipv6-address`

Parameters

<i>slot-number</i>	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.
<i>ipv6-address</i>	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

Version 8.4.2.1	Introduced on S-Series
Version 7.8.1.0	Introduced on C-Series
Version 7.4.1.0	Introduced on E-Series TeraScale

show ipv6 interface

C **E** **S** Display the status of interfaces configured for IPv6.

Syntax `show ipv6 interface interface [brief] [configured] [gigabitethernet slot | slot/port] [linecard slot-number] [loopback interface-number] [managementethernet slot/port] [port-channel number] [tengigabitethernet slot | slot/port] [vlan vlan-id]`

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> • For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the <i>slot/port</i> 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 <i>slot/port</i> 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 <i>slot-number</i>	(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 <i>slot/port</i>	(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 tengigabitethernet interface.
vlan	(OPTIONAL) View information for IPv6 VLANs.

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. Support for the managementethernet <i>slot/port</i> parameter was added.
Version 7.8.1.0	Introduced on C-Series
Version 7.4.1.0	Introduced on E-Series TeraScale

Usage Information The Management port is enabled by default (**no shutdown**). If necessary, use the [ipv6 address](#) command to assign an IPv6 address to the Management port.

Example 1 (interface)

```
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
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds

```

**Example 2
(interface
management
ethernet)**

```

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

```

**Example 3
(brief)**

```

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
  fd0a:bbbb:cccc:1004::50/64
...
Vlan 3                      [up/up]
  fe80::201:e8ff:fe3a:19b7
  7::1/64

```

show ipv6 route

C **E** **S** 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	<p>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.</p> <p>The :: notation specifies successive hexadecimal fields of zeros.</p> <p>prefix-length</p> <p>hostname (OPTIONAL) View information for this IPv6 routes with Host Name</p> <p>all (OPTIONAL) View information for all IPv6 routes</p> <p>bgp (OPTIONAL) View information for all IPv6 BGP routes</p> <p>connected (OPTIONAL) View only the directly connected IPv6 routes.</p> <p>isis (OPTIONAL) View information for all IPv6 IS-IS routes</p> <p>list (OPTIONAL) View the IPv6 prefix list</p> <p>ospf (OPTIONAL) View information for all IPv6 OSPF routes</p> <p>rip (OPTIONAL) View information for all IPv6 RIP routes</p> <p>static (OPTIONAL) View only routes configured by the <code>ipv6 route</code> command.</p> <p>summary (OPTIONAL) View a brief list of the configured IPv6 routes.</p>
------------------	--

Defaults No default values or behavior

Command Modes EXEC
EXEC Privilege

Command History	<p>Version 8.2.1.0 Introduced on E-Series ExaScale</p> <p>Version 7.8.1.0 Introduced on C-Series and S-Series</p> <p>Version 7.4.1.0 Introduced on E-Series TeraScale</p>
------------------------	---

Example 1 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 2
(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 28-76. show ipv6 route Command Example Fields

Field	Description
(undefined)	Identifies the type of route: <ul style="list-style-type: none"> • L = Local • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IPv6 address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

trust ipv6-diffserv

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 28-77. IPv6 -Diffserv Mapping

IPv6 Service Class Field	Queue ID
111XXXXX	7
110XXXXX	6
101XXXXX	5
100XXXXX	4
011XXXXX	3
010XXXXX	2
001XXXXX	1
000XXXXX	0

IPv6 Border Gateway Protocol (IPv6 BGP)

Overview

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on platforms: C E S

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`
- `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 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 extcommunity-list
- 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
- show ip bgp next-hop
- show ip bgp paths
- show ip bgp paths as-path
- show ip bgp paths community
- show ip bgp paths extcommunity
- show ip bgp regexp
- timers bgp

address-family

C **E** **T** **S** Enable the IPv4 multicast or the IPv6 address family.

Syntax `address-family [ipv4 multicast| ipv6unicast]`

Parameters

ipv4 multicast	Enter BGPv4 multicast mode.
ipv6 unicast	Enter BGPv6 mode.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version 8.4.2.1	Introduced on C-Series and S-Series.
Version 6.5.1.0	Introduced on E-Series TeraScale

Usage Information Enter ipv6 unicast to enter the BGP for IPv6 mode (CONF-ROUTER_BGPv6_AF).

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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X format followed by the prefix length in the /x format.
<i>prefix-length</i>	Range: /0 to /128 The :: notation specifies successive hexadecimal fields of zeros
advertise-map <i>map-name</i>	(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 <i>map-name</i>	(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 <i>map-name</i>	(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

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

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

C **E** **S**

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

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

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

C **E** **S**

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

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

If you enable this command, use the [capture bgp-pdu max-buffer-size](#) * command to recompute the best path.

bgp bestpath med confed

C **E** **S**

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

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

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

C **E** **S**

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

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

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

C **E** **S**

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	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	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	<i>ip-address</i>	Enter an IP address as the route reflector cluster ID.
	<i>number</i>	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults Not configured.

Command Modes ROUTER BGP

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 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 ipv6 unicast cluster-list	View paths with a cluster ID.

bgp confederation identifier

C **E** **S** 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

<i>as-number</i>	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 S-Series.
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

C **E** **S** 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

<i>as-number</i>	Enter the AS number. Range: 1 to 65535
<i>...as-number</i>	(OPTIONAL) Enter up to 16 confederation numbers. Range: 1 to 65535.

Defaults Not configured.

Command Modes ROUTER BGP

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

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

[bgp confederation identifier](#) Configure a confederation ID.

bgp dampening

C **E** **S**

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

<i>half-life</i>	(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
<i>reuse</i>	(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
<i>suppress</i>	(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
<i>max-suppress-time</i>	(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 <i>map-name</i>	(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 S-Series.
Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	Introduced on E-Series TeraScale

Usage Information	If you enter bgp dampening , the default values for <i>half-life</i> , <i>reuse</i> , <i>suppress</i> , and <i>max-suppress-time</i> 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 command.	
Related Commands	show ip bgp ipv6 unicast dampened-paths	View the BGP paths

bgp default local-preference

C **E** **S** 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

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

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 The [bgp default local-preference](#) command setting is applied by all routers within the AS.

bgp enforce-first-as

C **E** **S** 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 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	show ip bgp ipv6 unicast neighbors	Display IPv6 routing information exchanged by BGP neighbors.
	show ip protocols	View Information on routing protocols.
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

bgp fast-external-fallover

C **E** **S** 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

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 The [bgp fast-external-fallover](#) command appears in the [show config](#) command output.

bgp four-octet-as-support

C **E** **S** 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 *FTOS Configuration Guide*.

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

bgp graceful-restart

C **E** **S**

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 <i>ip-address</i> <i>peer-group-name</i>	Enter the keyword neighbor followed by one of the options listed below: <ul style="list-style-type: none"> <i>ip-address</i> of the neighbor in IP address format of the neighbor <i>peer-group-name</i> of the neighbor peer group.
restart-time <i>seconds</i>	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 <i>seconds</i>	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

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 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

C **E** **S**

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	
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	The <code>bgp log-neighbor-changes</code> command appears in the <code>show config</code> command output.	
Related Commands	<code>show config</code>	View the current configuration

bgp non-deterministic-med

C **E** **S** 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

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 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

C **E** **S** 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	<p>This command is a <i>knob</i> to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the <i>first</i> 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.</p> <p>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.</p>	
Related Commands	capture bgp-pdu max-buffer-size	Set the size of the BGP packet capture buffer
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

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

[show ip protocols](#) View information on all routing protocols enabled and active on the E-Series.

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

bgp router-id

C **E** **S**

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

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 Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

C **E** **T** **S**

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 BGPV6 ADDRESS FAMILY (conf-router_bgpv6_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.

Related Commands [clear ip bgp ipv6 unicast soft in](#) Activate inbound policies for IPv6 routes without resetting the BGP TCP session.

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 on E-Series TeraScale

capture bgp-pdu neighbor (ipv6)

C **E** **S** Enable capture of an IPv6 BGP neighbor packet.

Syntax `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

<code>ipv6-address</code>	Enter the IPv6 address of the target BGP neighbor.
<code>direction { both rx tx }</code>	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

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

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

C **E** **S** 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

<code>100-102400000</code>	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 S-Series.
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)

C **E** **S**

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 S-Series.
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

C **E** **S**

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 S-Series.
	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

C **E** **S**

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 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.

Command Modes EXEC Privilege

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

clear ip bgp peer-group

C **E** **S** 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

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

clear ip bgp ipv6 dampening

C **E** **S** 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 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

Command Modes EXEC Privilege

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 After you enter this command, the software deletes history routes and returns suppressed routes to active state.

clear ip bgp ipv6 flap-statistics

C **E** **S** 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 | regex 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 <i>as-path-name</i>	(OPTIONAL) Enter the keyword filter-list followed by the name of a configured AS-PATH list.
regexp <i>regular-expression</i>	(OPTIONAL) Enter the keyword regexp followed by regular expressions. Use one or a combination of the following: <ul style="list-style-type: none"> · (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 S-Series.
Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	Introduced on E-Series TeraScale

Usage Information

If you enter [clear ip bgp ipv6 flap-statistics](#) without any parameters, all statistics are cleared.

Related Commands

[show ip bgp ipv6 unicast flap-statistics](#) View BGP flap statistics.

clear ip bgp ipv6 unicast soft



Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

Syntax

clear ip bgp { * | *as-number* | *ipv4-neighbor-addr* | *ipv6-neighbor-addr* | *peer-group name* } **ipv6 unicast soft** [**in** | **out**]

Parameters

*	Clear and reapply policies for all BGP sessions.
<i>as-number</i>	Clear and reapply policies for all neighbors belonging to the AS. Range: 0-65535 (2-Byte) <i>or</i> 1-4294967295 (4-Byte) <i>or</i> 0.1-65535.65535 (Dotted format)
<i>ipv4-neighbor-addr</i> <i>ipv6-neighbor-addr</i>	Clear and reapply policies for a neighbor.
<i>peer-group name</i>	Clear and reapply policies for all BGP routers in the specified peer group.
ipv6 unicast	Clear and reapply policies for all IPv6 unicast routes.
in	Reapply only inbound policies. Note: If you enter soft , without an in or out option, both inbound and outbound policies are reset.
out	Reapply only outbound policies. Note: If you enter soft , without an in or out option, both inbound and outbound policies are reset.

Command Modes EXEC Privilege

Command History

Version 8.4.1.0	Added support for IPv4 multicast and IPv6 unicast 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 on the E-Series TeraScale

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

<i>ipv6-address</i>	(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 <i>peer-group-name</i>	Enter the keyword peer-group followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword in to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword out to view only information on outbound BGP routes.

Command Modes EXEC Privilege

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

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.

debug ip bgp events

C **E** **S**

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** command.

Parameters

ipv6-address (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.

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

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

Enter the **no debug ip bgp** command to remove all configured debug commands for BGP.

debug ip bgp ipv6 dampening

C **E** **S**

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 inbound dampened routes.

out (OPTIONAL) Enter the keyword **out** to view only outbound dampened routes.

Command Modes EXEC Privilege

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

Enter **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.

debug ip bgp ipv6 unicast soft-reconfiguration



Enable soft-reconfiguration debugging for IPv6 unicast routes.

Syntax `debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration`

To disable debugging, use the **no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration** command.

Parameters

<i>ipv4-address</i> <i>ipv6-address</i>	Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
<i>peer-group-name</i>	Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
ipv6 unicast	Debug soft reconfiguration for IPv6 unicast routes.

Defaults Disabled

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 S-Series
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 `debug ip bgp [ipv6-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

<i>ipv6-address</i>	(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 <i>peer-group-name</i>	(OPTIONAL) Enter the keyword peer-group followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword in to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword out to view only outbound keepalive messages.

Command Modes	EXEC Privilege	
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	Enter the <code>no debug ip bgp</code> command to remove all configured debug commands for BGP.	

debug ip bgp notifications

C **E** **S** 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	<i>ipv6-address</i>	(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.
	peer-group <i>peer-group-name</i>	(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 S-Series.
	Version 8.2.1.0	Introduced on E-Series ExaScale
	Version 7.4.1.0	Introduced on E-Series TeraScale
Usage Information	Enter the <code>no debug ip bgp</code> command to remove all configured debug commands for BGP.	

debug ip bgp updates

C **E** **S** 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.

Parameters	<i>ipv6-address</i>	(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.
	peer-group <i>peer-group-name</i>	(OPTIONAL) Enter the keyword peer-group followed by the name of the peer group.
	ipv6 unicast [<i>ipv6-address</i>]	(OPTIONAL) Enter the keyword ipv6 unicast , and, optionally, an ipv6 address.
	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.

Command Modes EXEC Privilege

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 Enter the [no debug ip bgp](#) command to remove all configured debug commands for BGP.

default-metric



Allows 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 *number* Enter a number as the metric to be assigned to routes from other protocols.
Range: 1 to 4294967295.

Defaults 0

Command Modes ROUTER BGP

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 The [default-metric](#) command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands [bgp always-compare-med](#) Enable comparison of all BGP MED attributes.
[redistribute](#) Redistribute routes from other routing protocols into BGP.

description

C **E** **S**

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 S-Series.
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

C **E** **S**

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

<i>external-distance</i>	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
<i>internal-distance</i>	Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200
<i>local-distance</i>	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 S-Series.
Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	Introduced on E-Series TeraScale



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.

maximum-paths

C **E** **S** 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

ebgp	Enter the keyword ebgp to enable multipath support for External BGP routes.
ibgp	Enter the keyword ibgp to enable multipath support for Internal BGP routes.
<i>number</i>	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

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 If you enable this command, use the [capture bgp-pdu max-buffer-size](#) command to recompute the best path.

neighbor activate

C **E** **S** 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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Identify a peer group by name.

	activate	Enter the keyword activate to enable the identified neighbor or 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 S-Series.
	Version 8.2.1.0	Introduced on E-Series ExaScale
	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.	

neighbor advertisement-interval

C **E** **S** 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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
<i>seconds</i>	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 S-Series.
	Version 8.2.1.0	Introduced on E-Series ExaScale
	Version 7.4.1.0	Introduced on E-Series TeraScale

neighbor allowas-in

C **E** **S**

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 S-Series.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale

neighbor default-originate

C **E** **S**

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

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

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

C **E** **S**

Assign a character string describing the neighbor or group of neighbors (peer group).

Syntax

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

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

neighbor distribute-list

C **E** **S**

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

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).

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	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	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 ebgp-multihop

C **E** **S** 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*]

To disallow and disconnect connections, use the **no neighbor** { *ipv6-address* | *peer-group-name* } **ebgp-multihop** [*ttl*] command.

Parameters	<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group.
	<i>ttl</i>	(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 S-Series.
	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

C **E** **S** 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	<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	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 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 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

C **E** **S** 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	<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
	<i>as-path-name</i>	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 out	Enter the keyword in to filter inbound BGP routes. Enter the keyword out to filter outbound BGP routes.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

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

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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group.
<i>maximum</i>	Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
<i>threshold</i>	(OPTIONAL) Enter a number to be used as a percentage of the <i>maximum</i> value. When the number of prefixes reaches this percentage of the <i>maximum</i> 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*

Command Modes ROUTER BGPV6-ADDRESS FAMILY

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

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.

Related Commands

[show ip bgp ipv6 unicast summary](#) Displays the current BGP configuration.

neighbor X:X:X::X password

C **E** **T** **S** Enable TCP MD5 Authentication for an IPv6 BGP peer session.

Syntax **neighbor x:x:x::x password** { 7 <encrypt-pass> | <clear-pass >

To return to the default setting, use the **no neighbor x:x:x::x password** command.

Parameters

<i>encrypt-pass</i>	Enter the encrypted password.
<i>clear-pass</i>	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 S-Series.
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

C **E** **S** 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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	(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 S-Series.
Version 8.2.1.0	Introduced on E-Series ExaScale
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 peer-group (assigning peers)

C **E** **S**

Allows you to assign one peer to a existing peer group.

Syntax `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::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 S-Series.
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.
show ip bgp ipv6 unicast peer-group	View BGP peers.
show ip bgp ipv6 unicast neighbors	View BGP neighbors configurations.

neighbor peer-group (creating group)

C **E** **S** 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 `peer-group-name` Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

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 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 an indirectly connected AS to a neighbor or peer group.
neighbor shutdown	Disable a peer or peer group.

neighbor peer-group passive

C **E** **S** 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 `peer-group-name` Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

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 After you configure a peer group as passive, you must assign it a subnet using the [neighbor subnet](#) command.

Related Commands

neighbor subnet	Assign a subnet to a dynamically-configured BGP neighbor.
---------------------------------	---

neighbor remote-as

C **E** **S** Create and specify the remote peer to the BGP neighbor.

Syntax **neighbor** { *ipv6-address* | *peer-group-name* } **remote-as** *number*

To delete a remote AS entry, use the **no neighbor** { *ipv6-address* | *peer-group-name* } **remote-as** *number* command.

Parameters

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
<i>number</i>	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 S-Series.
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

C **E** **S** 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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	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 S-Series.
	Version 8.2.1.0	Introduced on E-Series ExaScale
	Version 7.4.1.0	Introduced on E-Series TeraScale

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



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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group.
<i>map-name</i>	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 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 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

C **E** **S**

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 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.
All routers in the peer group receive routes from a route reflector.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

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

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

C **E** **S**

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.

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 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

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

neighbor shutdown

C **E** **S**

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 S-Series.
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

C **E** **T** **S**

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 S-Series
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

<i>subnet-number</i>	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.
<i>mask</i>	Enter a prefix mask in / prefix-length format (/x).

Defaults

Not configured.

Command Modes

ROUTER BGP

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

neighbor timers

C **E** **S**

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Syntax `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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group to set the timers for all routers within the peer group.
<i>keepalive</i>	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. Range: 1 to 65535 Default: 60 seconds
<i>holdtime</i>	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

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

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.

neighbor update-source

C **E** **S**

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	<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	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	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	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	<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	Enter the name of the peer group to disable all routers within the peer group.
	<i>weight</i>	Enter a number as the weight. Range: 0 to 65535 Default: 0

Defaults 0

Command Modes ROUTER BGP

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 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

C **E** **S**

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::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 S-Series.

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.

Related Commands

[redistribute](#)

Redistribute routes into BGP.

network backdoor

C **E** **S**

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: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.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

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 Though FTOS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

redistribute

C **E** **S**

Redistribute routes into BGP.

Syntax **redistribute** { **connected** | **static** } [**route-map** *map-name*]

To disable redistribution, use the **no redistribute** { **connected** | **static** } 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 (OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map.
map-name
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 S-Series.
Version 8.2.1.0 Introduced on E-Series ExaScale
Version 7.4.1.0 Introduced on E-Series TeraScale

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]`

To stop redistribution of IS-IS routes, use the **no redistribute isis** command.

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.

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 S-Series.
Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	Introduced on E-Series TeraScale

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 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 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

C **E** **S**

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

<i>as-number</i>	Enter the AS number. Range: 1 to 65535.
------------------	--

Defaults Not enabled.

Command Modes CONFIGURATION

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

show capture bgp-pdu neighbor

C **E** **S**

Display BGP packet capture information for an IPv6 address on the E-Series.

Syntax **show capture bgp-pdu neighbor** *ipv6-address*

Parameters

<i>ipv6-address</i>	Enter the IPv6 address (X: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 S-Series. 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

C **E** **S**

View the current ROUTER BGP configuration.

Syntax **show config**

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Example

```
FTOS(conf-router_bgp)#show conf
!
router bgp 18508
 neighbor RR-CLIENT peer-group
 neighbor RR-CLIENT remote-as 18508
 neighbor RR-CLIENT no shutdown
 neighbor RR-CLIENT-PASSIV peer-group passive
 neighbor RR-CLIENT-PASSIV remote-as 18508
 neighbor RR-CLIENT-PASSIV subnet 9000::9:0/120
 neighbor RR-CLIENT-PASSIV no shutdown
 neighbor 1109::33 remote-as 18508
 neighbor 1109::33 update-source Loopback 101
 neighbor 1109::33 no shutdown
 neighbor 2222::220 remote-as 18508
 neighbor 2222::220 route-reflector-client
 neighbor 2222::220 update-source Loopback 100
 neighbor 2222::220 no shutdown
 neighbor 4000::33 remote-as 18508
 neighbor 4000::33 no shutdown
 neighbor 4000::60 remote-as 18508
 neighbor 4000::60 no shutdown
 neighbor 9000::1:2 remote-as 640
 no neighbor 9000::1:2 activate
 neighbor 9000::1:2 no shutdown

!
FTOS#
```

show ip bgp ipv6 unicast

C **E** **S** View the current BGP routing table for the E-Series.

Syntax `show ip bgp ipv6 unicast [network [network-mask] [longer-prefixes]]`

Parameters

<i>network</i>	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
<i>network-mask</i>	(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 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 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

C **E** **S** View BGP neighbors in a specific cluster.

Syntax `show ip bgp ipv6 unicast cluster-list [cluster-id]`

Parameters

<i>cluster-id</i>	(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 S-Series.
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

C **E** **S**

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

<i>community-number</i>	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords local-AS to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords no-advertise to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords no-export to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

EXEC
EXEC Privilege

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

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

C **E** **S**

View routes that are affected by a specific community list.

Syntax `show ip bgp ipv6 unicast community-list community-list-name [exact-match]`

Parameters

<i>community-list-name</i>	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 S-Series.
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

C **E** **S** 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 S-Series.
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

C **E** **S** Display BGP internal information for IPv6 Unicast address family.

Syntax **show ip bgp ipv6 unicast detail**

Defaults none

Command Modes EXEC
EXEC Privilege

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

show ip bgp ipv6 unicast extcommunity-list

C **E** **S** 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 S-Series.
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

C **E** **S**

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 S-Series.
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

C **E** **S**

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: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 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 S-Series.
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

C **E** **S**

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 S-Series.

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

C **E** **S**

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

Version 8.4.1.0	Added support for IPv4 multicast and IPv6 unicast address families
Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on S-Series
Version 7.7.1.0	Introduced 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 6.3.1.0	The output is changed to display the total number of advertised prefixes

Example

```

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 29-78. Command Example fields: show ip bgp ipv6 unicast neighbors

Lines beginning with	Description
BGP neighbor	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.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: <ul style="list-style-type: none"> 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.

Table 29-78. Command Example fields: show ip bgp ipv6 unicast neighbors

Lines beginning with	Description
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 IPv6 Unicast 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 ipv6 unicast](#)

View the current BGP routing table.

show ip bgp ipv6 unicast peer-group

C **E** **S**

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**

<i>peer-group-name</i>	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword detail to view peer-group-specific information for the IPv6 address family.
summary	(OPTIONAL) Enter the keyword summary to view status information of the peers in that peer group. The output is the same as that found in show ip bgp ipv6 unicast summary command

Command Modes

EXEC

EXEC Privilege

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

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-PASSIV, 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

C **E** **S** Allows you to view the status of all BGP connections.

Syntax **show ip bgp ipv6 unicast summary**

Command Modes EXEC
EXEC Privilege

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

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     1         35        32        0       0     0    00:16:42 0
9000::6:2     2         35        32        0       0     0    00:16:39 0
9000::7:2     3         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    44        19        0       0     0    00:16:41 0
9000::a:2     18508    35        32        0       0     0    00:16:43 0
9000::b:14    18508    29        29        0       0     0    00:13:01 0
FTOS#

```

show ip bgp next-hop

C **E** **S**

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
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

Example

```
FTOS#show ip bgp next-hop
  Next-hop      Via                               RefCount  Cost   Flaps  Time Elapsed
  9000::5:2     9000::5:2, Gi 8/38              2         0     0 00:23:22
  9000::6:2     9000::6:2, Gi 8/38              2         0     0 00:23:22
  9000::7:2     9000::7:2, Gi 8/38              2         0     0 00:23:22
  9000::8:2     9000::8:2, Gi 8/38              2         0     0 00:23:22
  9000::9:2     9000::9:2, Gi 8/38             6000      0     0 00:23:16
  9000::a:2     9000::a:2, Gi 8/38              2         0     0 00:23:22
FTOS#
```

show ip bgp paths

C **E** **S**

View all the BGP path attributes in the BGP database.

Syntax `show ip bgp paths [regexp regular-expression]`

Parameters **regexp** Enter a regular expression then use one or a combination of the following characters to match:
regular-expression

- `.` = (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 S-Series.
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

C **E** **S** 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 S-Series.
Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	Introduced on E-Series TeraScale

show ip bgp paths community

C **E** **S** 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 S-Series.
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

C **E** **S** 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 S-Series.
Version 8.2.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	Introduced on E-Series TeraScale

show ip bgp regexp

C **E** **S**

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

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

timers bgp

C **E** **S**

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

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

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). FTOS 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

C **E** **S** 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.

Parameters

ipv6 Enter the keyword **ipv6** to specify the address family as IPv6.

unicast Enter the keyword **unicast** to specify multicast as SAFI.

Defaults IPv6 Unicast

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 8.4.2.1 Introduced on C-Series and S-Series.

Version 7.4.1.0 Introduced on E-Series TeraScale

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

C **E** **S** 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** 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				
Command History	<table border="0"> <tr> <td>Version 8.4.2.1</td> <td>Introduced on C-Series and S-Series.</td> </tr> <tr> <td>Version 7.4.1.0</td> <td>Introduced on E-Series TeraScale</td> </tr> </table>	Version 8.4.2.1	Introduced on C-Series and S-Series.	Version 7.4.1.0	Introduced on E-Series TeraScale
Version 8.4.2.1	Introduced on C-Series and S-Series.				
Version 7.4.1.0	Introduced on E-Series TeraScale				
Usage Information	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.</p>				

bgp dampening

C **E** **S** 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	<p><i>half-life time</i> (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.</p> <p>Range: 1 to 45. Default: 15 minutes</p> <p>route-map <i>map-name</i> (OPTIONAL) Enter the keyword route-map followed by the name of a configured route map.</p> <p>Only match commands in the configured route map are supported.</p>
-------------------	---

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 8.4.2.1	Introduced on C-Series and S-Series.
Version 7.4.1.0	Introduced on E-Series TeraScale

clear ip bgp ipv6 unicast

C **E** **S** Reset MBGP sessions.

Syntax `clear ip bgp ipv6 unicast * ipv6-address prefix-length [dampening | flap-statistics] peer-group]`

Parameters	*	Enter the character * to clear all peers.
	<i>ipv6-address prefix-length</i>	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
	dampening	(OPTIONAL) Enter the keyword dampening to clear route flap dampening information.
	flap-statistics	(OPTIONAL) Enter the keyword flap-statistics to reset the flap statistics on all prefixes from that neighbor.
	peer-group	(OPTIONAL) Enter the keyword peer-group to clear all members of a peer-group.

Command Modes EXEC Privilege

Command History	Version 8.4.2.0	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced

clear ip bgp ipv6 unicast dampening

C **E** **S** Clear information on route dampening.

Syntax `clear ip bgp dampening ipv6 unicast [network network-mask]`

Parameters	<i>network</i>	(OPTIONAL) Enter the IPv6 network address in X:X:X:X format.
	<i>network-mask</i>	If you enter the network address, then enter the network mask, from 0 to 128.

Command Modes EXEC Privilege

Command History	Version 8.4.2.1	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale

clear ip bgp ipv6 unicast flap-statistics

C **E** **S** 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	<i>network</i>	(OPTIONAL) Enter the IPv6 network address in X:X:X:X format to clear flap statistics.
	filter-list list	(OPTIONAL) Enter the keyword filter-list followed by the name of a configured AS-PATH list (max 16 characters).

regex (OPTIONAL) Enter the keyword **regex** followed by regular expressions. Use one or a combination of the following:

regex

- (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 8.4.2.0	Introduced on C-Series and S-Series.
Version 7.4.1.0	Introduced

debug ip bgp ipv6 unicast dampening

C **E** **S** 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 8.4.2.1	Introduced on C-Series and S-Series.
Version 7.4.1.0	Introduced on E-Series TeraScale

debug ip bgp ipv6 unicast peer-group updates

C **E** **S** 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

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.

Command Modes	EXEC Privilege	
Command History	Version 8.4.2.1	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale

debug ip bgp ipv6 unicast updates

C **E** **S** 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	<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X:X format followed by the prefix length in the /x format.
	<i>prefix-length</i>	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	Version 8.4.2.1	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale

distance bgp

C **E** **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	<i>external-distance</i>	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
	<i>internal-distance</i>	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 S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale



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.

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:x:x:x::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 S-Series.
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

C **E** **S**

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 S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

neighbor default-originate

C **E** **S**

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 *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

Command History

Version 8.4.2.1 Introduced on C-Series and S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

neighbor distribute-list

C **E** **S** 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

<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
<i>prefix-list-name</i>	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

Version 8.4.2.1	Introduced on C-Series and S-Series.
Version 7.4.1.0	Introduced on E-Series TeraScale

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

C **E** **S** 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.

Parameters

<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	Enter the name of the peer group to apply the filter to all routers in the peer group.
<i>access-list-name</i>	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).
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 BGPV6-ADDRESS FAMILY	
Command History	Version 8.4.2.1	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale

neighbor maximum-prefix

C **E** **S** 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

<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the X:X:X:X format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
<i>maximum</i>	Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
<i>threshold</i>	(OPTIONAL) Enter a number to be used as a percentage of the <i>maximum</i> value. When the number of prefixes reaches this percentage of the <i>maximum</i> 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

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History	Version 8.4.2.1	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale

neighbor next-hop-self

C **E** **S** 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	<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	(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 S-Series.
	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

C **E** **S** 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	<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
	<i>peer-group-name</i>	(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 S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale

neighbor route-map

C **E** **S** 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	<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zeros.
-------------------	---------------------	---

<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
<i>map-name</i>	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 S-Series.
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

C **E** **S** 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

<i>ipv6-address</i>	(OPTIONAL) Enter the IPv6 address in the x:x:x:x format. The :: notation specifies successive hexadecimal fields of zeros.
<i>peer-group-name</i>	(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 BGPV6-ADDRESS FAMILY

Command History

Version 8.4.2.1	Introduced on C-Series and S-Series.
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

C **E** **S**

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** 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.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version 8.4.2.1	Introduced on C-Series and S-Series.
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.

Related Commands [redistribute](#) Redistribute routes into BGP.

redistribute

C **E** **S**

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 (OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map.
map-name

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 S-Series.
 Version 7.4.1.0 Introduced on E-Series TeraScale

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

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 S-Series.
 Version 7.4.1.0 Introduced on E-Series TeraScale

Example

```
FTOS#show ip bgp ipv6 unicast
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 - redistrib-
uted, n - network Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network                Next Hop                Metric      LocPrf Weight Path
```

```

h   dead:1::/100      5ffe:10::3      0      0 1 i
h   dead:2::/100      5ffe:11::3      0      0 1 i
*>  dead:2::/100      5ffe:10::3      0      0 1 i
*   dead:2::/100      5ffe:11::3      0      0 1 i
*>  dead:3::/100      5ffe:10::3      0      0 1 i
*   dead:3::/100      5ffe:11::3      0      0 1 i
h   dead:4::/100      5ffe:10::3      0      0 1 i
h   dead:4::/100      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

```

FTOS#

Table 29-79. show ip bgp Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

**Related
Commands**

[show ip bgp ipv6 unicast community](#) View BGP communities.

show ip bgp ipv6 unicast cluster-list

C **E** **S**

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 S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast community

C **E** **S**

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 (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise Enter the keywords **no-advertise** to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.

no-export Enter the keywords **no-export** to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes EXEC
EXEC Privilege

Command History
Version 8.4.2.1 Introduced on C-Series and S-Series.
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

C **E** **S** View routes that are affected by a specific community list.

Syntax `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 S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast dampened-paths

C **E** **S** 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 S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast detail

C **E** **S** Display detailed BGP information.

Syntax `show ip bgp ipv6 unicast detail`

Command Modes EXEC
EXEC Privilege

Command History
Version 8.4.2.1 Introduced on C-Series and S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

Example R2_Training#show ip bgp ipv6 unicast detail

```
Detail information for BGP Node
bgpNdp 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics 327741 :
NhLocAS 1 : NdState 2 : NdrPMPPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 : NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP 0x41a19088
```

```

NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25000
: NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP : NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 : NdModCommP
0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 : NdComSortHdp
0x41a19d04 : NdUpdAFMsk 0 : AFRstSe
t 0x41a1a298 : NHopDfrdHdp 0x41a1a3e0 : NumNhDfrd 0 : CfgHdrAFMsk 1
AFChkNetTmrP 0x41ee705c : AFRTdamp 0 : AlwaysCmpMed 0 : LocrHld 10 : LocrRem
10 : softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : Fatals 0 : ConnExps 0 : HldExps 0 : KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 : TxNotifs 0
BadEvts 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP 0x41a1b6d4 : RxOp-
CodeP 0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP 0x41a1b750 : TxOp-
CodeP 0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP 0x41a1b7b8 : LogN-
brChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl 0 : AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 : CleanRibTmrP
0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP 0x41ee713c :
FastExtFallover 1 : FastIntFallove
r 0 : EnforcelstAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpiCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 : NonDet 0 : Dfrd-
PathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 : IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 : MaxeorExtInt 361
FixedPartCrt 1 : VarParCrt 1
Packet Capture max allowed length 40960000 : current length 0

```

```

Peer Grp List
Nbr List
Confed Peer List

```

Address Family specific Information

```

AFIndex 2
NdSpFlag 0x41a190b2 : AFRttP 0x41a0de00 : NdRTMMkrP 0x41a19d68 : NdRTMAFT-
blVer 0 : NdRibCtxAddr 1101110720
NdRibCtxAddrLen 255 : NdAFPprefix 0 : NdAfNLRIP 0 : NdAFNLRILen 0 : NdAFWPtRP
0
NdAFWLen 0 : NdAfNH : NdAFRedRttP 0x41a4e000 : NdRecCtxAdd 1101110900
NdRedCtxAddrLen 255 : NdAfRedMkrP 0x41a19ec8 : AFAggRttP 0x41a4e200 : AfAggC-
txAddr 1101111060 : AfAggrCtxAddrLen 255
AfNumAggrPfx 0 : AfNumAggrASSet 0 : AfNumSuppmap 0 : AfNumAggrValidPfx 0 :
AfMPathRttP 0x41a4e300
MpathCtxAddr 1101111172 : MpathCtxAddrLen 255 : AfEorSet 0x41a1a198 : NumD-
frdPfx 0
AfActPeerHd 0x41a1a3cc : AfExtDist 1101112320 : AfIntDist 200 : AfLocDist 200
AfNumRRc 0 : AfRR 0 : AfNetRttP 0x41a0df00 : AfNetCtxAddr 1101112424 :
AfNetCtxAddrLen 255
AfNwCtxAddr 1101112475 : AfNwCtxAddrLen 255 : AfNetBKDrRttP 0x41a4e100 :
AfNetBKDRcnt 0 : AfDampHLife 0

```

```
AfDampReuse 0 : AfDampSupp 0 : AfDampMaxHld 0 : AfDampCeiling 0 : AfDampRmapP
0x41a1a548
AfNumDamped 0 : AfNumHist 0 : AfNumTotalHist 0 : AfDfrdRtLstP 0x41a1b624 :
AfDfrdNodeCnt 0 : softRecfgAf 0x41a1b5dc : softRecfgCfgAf 0x41a1b5f8
AfCfgCnt 0 : AfRedistCfg 0 : IBGP_Mpath 0 : EBGP_Mpath 0 : DebugInPfList :
DebugOutPfList
```

show ip bgp ipv6 unicast filter-list

C **E** **S**

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 S-Series.
 Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast flap-statistics

C **E** **S**

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* (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 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 S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

Example

```
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 - redistrib-
uted, n - network Origin codes: i - IGP, e - EGP, ? - incomplete
```

	Network	From	Flaps	Duration	Reuse	Path
h	dead:1::/100	5ffe:10::3	1	00:03:20		1 i
h	dead:1::/100	5ffe:11::3	1	00:03:20		1 i
h	dead:4::/100	5ffe:10::3	1	00:04:39		1 i
h	dead:4::/100	5ffe:11::3	1	00:04:39		1 i

```
FTOS#
```

show ip bgp ipv6 unicast inconsistent-as

C **E** **S**

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 S-Series.
Version 7.4.1.0 Introduced on E-Series TeraScale

show ip bgp ipv6 unicast neighbors

C **E** **S**

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 S-Series.
Version 7.5.1.0 Modified: Added **detail** option; added information to output.
Version 7.4.1.0 Introduced on E-Series TeraScale

Example 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

  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
Foreign host: 5ffe:11::3, Foreign port: 36800

```

FTOS#

Table 29-80. show ip bgp neighbors Command Fields

Lines beginning with	Description
BGP neighbor	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.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: <ul style="list-style-type: none"> 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.

Table 29-80. show ip bgp neighbors Command Fields (Continued)

Lines beginning with	Description
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.
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 IPv6 Unicast as the address family.
BGP table version	Displays the which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefix 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 ipv6 unicast](#)

View the current BGP routing table.

show ip bgp ipv6 unicast peer-group

C **E** **S**

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***peer-group-name*

(OPTIONAL) Enter the name of a peer group to view information about that peer group only.

summary(OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group.The output is the same as that found in [show ip bgp ipv6 unicast summary](#) command**Command Modes**

EXEC

EXEC Privilege

Command History	Version 8.4.2.1	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale
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

C **E** **S** Allows you to view the status of all BGP connections.

Syntax **show ip bgp ipv6 unicast summary**

Command Modes
EXEC
EXEC Privilege

Command History	Version 8.4.2.1	Introduced on C-Series and S-Series.
	Version 7.4.1.0	Introduced on E-Series TeraScale

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 Pfx	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/
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 29-81. show ip bgp summary Command Fields

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries and route paths and the amount of memory used to process those entries.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The show ip bgp ipv6 unicast community command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.

Table 29-81. show ip bgp summary Command Fields

Field	Description
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	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.
Up/Down	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.
State/Pfx	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.

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 *FTOS Configuration Guide*.



Note: The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

Commands

The following are the FTOS commands to enable IS-IS.

- adjacency-check
- advertise
- area-password
- clear config
- clear isis
- clns host
- debug isis
- debug isis adj-packets
- debug isis local-updates
- debug isis snp-packets
- debug isis spf-triggers
- debug isis update-packets
- default-information originate
- description
- distance
- distribute-list in
- distribute-list out

- distribute-list redistributed-override
- domain-password
- graceful-restart ietf
- graceful-restart interval
- graceful-restart t1
- graceful-restart t2
- graceful-restart t3
- graceful-restart restart-wait
- hello padding
- hostname dynamic
- ignore-lsp-errors
- ip router isis
- ipv6 router isis
- isis circuit-type
- isis csnp-interval
- isis hello-interval
- isis hello-multiplier
- isis hello padding
- isis ipv6 metric
- isis metric
- isis network point-to-point
- isis password
- isis priority
- is-type
- log-adjacency-changes
- lsp-gen-interval
- lsp-mtu
- lsp-refresh-interval
- max-area-addresses
- max-lsp-lifetime
- maximum-paths
- metric-style
- multi-topology
- net
- passive-interface
- redistribute
- redistribute bgp
- redistribute ospf
- router isis
- set-overload-bit
- 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

E Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

Syntax **adjacency-check**

To disable adjacency check, use the **no adjacency-check** command.

Defaults Enabled

Command Modes ROUTER ISIS (*for IPv4*)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History Version 7.5.1.0 Introduced on E-Series

Usage Information Use this command to perform protocol-support consistency checks on hello packets. The adjacency-check is enabled by default.

advertise

E 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

level1-into-level2	Enter the keyword level1-into-level2 to advertise Level 1 routes into Level 2 LSPs. This is the default.
level2-into-level1	Enter the keyword level2-into-level1 to advertise Level 2 inter-area routes into Level 1 LSPs. Described in RFC 2966.
<i>prefix-list-name</i>	Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

Defaults **level1-into-level2** (Level 1 to Level 2 leaking enabled.)

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 You cannot disable leaking from one level to another, *however* you can regulate the rate flow from one level to another via an IP Prefix list. If the IP Prefix list is not configured, all routes are leaked.

Additional information can be found in IETF RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*.

area-password

E 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

E Clear IS-IS configurations that display under the **router isis** heading of the [show running-config](#) command output.

Syntax `clear config`

Command Modes ROUTER ISIS

Usage Information Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

Related Commands

copy	Use this command to save the current configuration to another location.
----------------------	---

clear isis

E Restart the IS-IS process. All IS-IS data is cleared.

Syntax `clear isis [tag] [* | database | traffic]`

Parameters

<i>tag</i>	(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

E 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

<i>name</i>	Enter an alphanumeric string to identify the name-to-NSAP mapping.
<i>nsap</i>	Enter a specific NSAP address that will be associated with the <i>name</i> parameter.

Defaults Not configured.

Command Modes ROUTER ISIS

Usage Information Use this command to configure a shortcut name that can be 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

E Enable debugging for all IS-IS operations.

Syntax `debug isis`

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

- E** 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:
C-Series and **S-Series** Range: 1-128
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 VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC Privilege

debug isis local-updates

- E** 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:
C-Series and **S-Series** Range: 1-128
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 VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC Privilege

debug isis snp-packets

- E** Enable debugging on a specific interface and provides diagnostic information to debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets.

Syntax `debug isis snp-packets [interface]`

To turn off debugging, enter the **no debug isis snp-packets [interface]** command.

Parameters

- interface* (OPTIONAL) Identifies the interface type slot/port as one of the following:
- For a 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 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

- E** Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

Syntax `debug isis spf-triggers`

To turn off debugging, enter **no debug isis spf-triggers**.

Command Modes EXEC Privilege

debug isis update-packets

- E** 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	<p><i>interface</i> (OPTIONAL) Identifies the interface type slot/port as one of the following:</p> <ul style="list-style-type: none"> 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 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

E 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	<p>always (OPTIONAL) Enter the keyword always to have the default route always advertised</p> <p>metric <i>metric</i> (OPTIONAL) Enter the keyword metric followed by a number to assign to the route. Range: 0 to 16777215</p> <p>route-map <i>map-name</i> (OPTIONAL) A default route will be generated by the routing process if the route map is satisfied.</p>
-------------------	--

Defaults Not configured.

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 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

C **E** **S**

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

E

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.

Parameters

weight The administrative distance value indicates the reliability of a routing information source.
Range: 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.)
Default: 115

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.

Defaults *weight* = 115

Command Modes ROUTER ISIS (*for IPv4*)
CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Usage Information The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

distribute-list in

E Filter network prefixes received in updates.

Syntax `distribute-list prefix-list-name in [interface]`

To return to the default values, enter the **no distribute-list *prefix-list-name* in [*interface*]** command.

Parameters

prefix-list-name

Specify the prefix list to filter prefixes in routing updates.

interface

(OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a1- 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 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 (*for IPv6*)

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

Related Commands

distribute-list out	Suppress networks from being advertised in updates.
redistribute	Redistributes routes from one routing domain to another routing domain.

distribute-list out

E Suppress network prefixes from being advertised in outbound updates.

Syntax `distribute-list prefix-list-name out [connected | bgp as number | ospf process-id | rip | static]`

To return to the default values, enter the **no distribute-list *prefix-list-name* out [bgp *as number* | connected | ospf *process-id* | rip | static]** command.

Parameters

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 keyword ospf followed by 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*)

Command History	Version 7.5.1.0	Introduced IPv6 ISIS support
	Version 6.3.1.0	Introduced

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

E 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*)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History	Version 7.8.1.0	Introduced IPv6 ISIS support
	Version 6.3.1.0	Introduced

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

E 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

<code>hmac-md5</code>	(OPTIONAL) Enter the keyword hmac-md5 to encrypt the password using MD5.
<code>encryption-type</code>	(OPTIONAL) Enter 7 to encrypt the password using DES.
<code>password</code>	Enter an alphanumeric string up to 16 characters long. If you do not specify an encryption type or hmac-md5 keywords, the password is processed as plain text which provides limited security.

Defaults No default password.

Command Modes ROUTER ISIS

Usage Information The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands

area-password	Configure an IS-IS area authentication password.
isis password	Configure the authentication password for an interface.

graceful-restart ietf

E Enable Graceful Restart on an IS-IS router.

Syntax `graceful-restart ietf`

To return to the default, use the **no graceful-restart ietf** command.

Parameters

<code>ietf</code>	Enter ietf to enable Graceful Restart on the IS-IS router.
-------------------	---

Defaults Default is Graceful Restart disabled

Command Modes ROUTER ISIS

Command History

Version 8.3.1.0	Introduced on the E-Series
-----------------	----------------------------

Usage Information A Restart TLV included in every Graceful Restart enabled router's HELLO PDUs. This enables the (re)starting as well as the existing ISIS peers to detect the GR capability of the routers on the connected network. A flag in the Restart TLV contains Restart Request (RR), Restart Acknowledge (RA) and Suppress Adjacency Advertisement (SA) bit flags.

The ISIS Graceful Restart enabled router can co-exist in mixed topologies where some routers are Graceful Restart enabled and others are not. For neighbors that are not Graceful Restart enabled, the restarting router brings up the adjacency per the usual methods.

graceful-restart interval

- E** 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

- E** Set the Graceful Restart wait time before unacknowledged restart requests are generated. This is the interval before the system sends a Restart Request (an IIH with RR bit set in Restart TLV) until the CSNP is received from the helping router.

Syntax `graceful-restart t1 {interval seconds | retry-times value}`

To return to the default, use the **no graceful-restart t1** command.

Parameters

interval Enter the keyword **interval** to set the wait time.
Range: 5-120 seconds
Default: 5 seconds

retry-times Enter the keyword **retry-times** to set the number of times the request interval is extended until a CSNP is received from the helping router.
Range: 1-10 attempts
Default: 1

Defaults Refer to parameters above.

Command Modes ROUTER ISIS

Command History Version 8.3.1.0 Introduced on the E-Series

graceful-restart t2

- E** 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

- E** 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 **adjacency** Enter the keyword **adjacency** so that the restarting router receives the remaining time value from its peer and adjusts its T3 value accordingly if user has configured this option.

manual Enter the keyword **manual** to specify a time value that the restarting router uses.
Range: 50-120 seconds
default: 30 seconds

Defaults manual, 30 seconds

Command Modes ROUTER ISIS

Command History Version 8.3.1.0 Introduced on the E-Series

Usage Information 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

E 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

E Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

Syntax `hello padding [multi-point | point-to-point]`

To return to default, use **no hello padding [multi-point | point-to-point]**.

Parameters

multi-point (OPTIONAL) Enter the keyword **multi-point** to pad only LAN hello PDUs.
point-to-point (OPTIONAL) Enter the keyword **point-to-point** to pad only point-to-point PDUs.

Defaults Both LAN and point-to-point hello PDUs are padded.

Command Modes ROUTER ISIS

**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

E Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

Syntax **hostname dynamic**

To disable this command, enter **no hostname dynamic**.

Defaults Enabled.

Command Modes ROUTER ISIS

Usage Information Use this command to build name-to-system ID 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

E Ignore LSPs with bad checksums instead of purging those LSPs.

Syntax **ignore-lsp-errors**

To return to the default values, enter **no ignore-lsp-errors**.

Defaults In IS-IS, the default deletes LSPs with internal checksum errors (no ignore-lsp-errors).

Command Modes ROUTER ISIS

Usage Information IS-IS normally purges LSPs with an incorrect data link checksum, causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This could cause disruption to your system operation.

ip router isis

E 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

E 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

net	Configure an IS-IS network entity title (NET) for a routing process.
is-type	Assign a type for a given area.

isis circuit-type

E Configure the adjacency type on interfaces.

Syntax `isis circuit-type {level-1 | level-1-2 | level-2-only}`

To return to the default values, enter **no isis circuit-type**.

Parameters

level-1 You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors.
You cannot form Level 2 adjacencies on this interface.

level-1-2	You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, then a Level 2 adjacency is established. This is the default.
level-2-only	You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

Defaults level-1-2

Command Modes INTERFACE

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

E Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

Syntax **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

E 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

E 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

E 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

E Assign metric to an interface for use with IPv6 information.

Syntax **isis ipv6 metric** *default-metric* [**level-1** | **level-2**]

To return to the default values, enter **no ipv6 isis metric** [*default-metric*] [**level-1** | **level-2**] command.

Parameters	<i>default-metric</i>	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 Force10 recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis metric

E Assign a metric to an interface.

Syntax `isis metric default-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)

Command Modes INTERFACE

Usage Information

Dell Force10 recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis network point-to-point

E 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

isis password

E 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	<i>encryption-type</i>	(OPTIONAL) Enter 7 to encrypt the password using DES.
	hmac-md5	(OPTIONAL) Enter the keyword hmac-md5 to encrypt the password using MD5.
	<i>password</i>	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

E Set priority of the designated router you select.

Syntax **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	<i>value</i>	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 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

E Configure IS-IS operating level for a router.

Syntax **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

E 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

E 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.
	<i>interval seconds</i>	Enter the maximum number of seconds between LSP generations. Range: 0 to 120 seconds Default: 5 seconds
	<i>initial_wait_interval seconds</i>	(OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. Range: 0 to 120 seconds Default: 1 second
	<i>second_wait_interval seconds</i>	(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

E 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

<i>size</i>	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

E 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

E Configure manual area addresses.

Syntax `max-area-addresses number`

To return to the default values, enter **no max-area-addresses**.

Parameters

number	Set the maximum number of manual area addresses. Range: 3 to 6. Default: 3
---------------	--

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

E 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

seconds	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
----------------	---

Defaults 1200 seconds

Command Modes ROUTER ISIS

Usage Information Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval.

The *seconds* parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.

Related Commands [lsp-refresh-interval](#) Use this command to set the link-state packet (LSP) refresh interval.

maximum-paths

E Allows you to configure the maximum number of equal cost paths allowed in a routing table.

Syntax `maximum-paths number`

To return to the default values, enter **no maximum-paths**.

Parameters `number` Enter a number as the maximum number of parallel paths an IP routing installs in a routing table.
Range: 1 to 16.
Default: 4

Defaults 4

Command Mode ROUTER ISIS (*for IPv4*)
CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History
Version 7.8.1.0 Introduced MT ISIS support
Version 6.3.1.0 Introduced

metric-style

E Configure a router to generate and accept old-style, new-style, or both styles of type, length, and values (TLV).

Syntax `metric-style { narrow [transition] | transition | wide [transition] } [level-1 | level-2]`

To return to the default values, enter the **no metric-style { narrow [transition] | transition | wide [transition] } [level-1 | level-2]** command.

Parameters

- narrow** Allows you to configure the E-Series to generate and accept old-style TLVs.
Metric range: 0 to 63
- transition** Allows you to configure the E-Series to generate both old-style and new-style TLVs.
Metric range: 0 to 63
- wide** Allows you to configure the E-Series to generate and accept only new-style TLVs.
Metric range: 0 to 16777215
- level-1** Enables the metric style on Level 1.
- level-2** Enables the metric style on Level 2.

Defaults `narrow`; if no Level is specified, Level-1 and Level-2 are configured.

Command Modes ROUTER ISIS

Usage Information If you enter the **metric-style wide** command, the FTOS generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs. The new-style TLVs have wider metric fields than old-style TLVs.

Related Commands [isis metric](#) Use this command to configure a metric for an interface.

multi-topology

- E** Enables Multi-Topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

Syntax **multi-topology [transition]**

To return to a single topology configuration, enter **no multi-topology [transition]**.

Parameters transition

Defaults Disabled

Command Mode CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

Command History Version 7.8.1.0 Introduced

net

- E** 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

- E** 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 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

E 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 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.
metric <i>metric-value</i>	(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 { external internal }	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. You must specify one of the following: <ul style="list-style-type: none"> • 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 <i>map-name</i>	(OPTIONAL) If the route-map argument is not entered, all routes are redistributed. If a <i>map-name</i> value is not specified, then no routers are imported.

Defaults **metric** *metric-value* = 0; **metric-type**= internal; **level-2**

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 are passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the [metric-style](#) command. If the [metric-style](#) command is set for narrow or transition mode and the metric value in the [redistribute](#) command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the [metric-style](#) command is set for wide mode, an the metric value in the [redistribute](#) command is advertised.

Related Commands

[default-information originate](#)

Generate a default route for the IS-IS domain.

[distribute-list out](#)

Suppress networks from being advertised in updates. Redistributed routing information is filtered by this command.

redistribute bgp

E 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

<i>AS number</i>	Enter a number that corresponds to the Autonomous System number. Range: 1 to 65355
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: <ul style="list-style-type: none"> external internal
route-map map-name	<i>map-name</i> 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 <i>map-name</i> , 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 (<i>for IPv4</i>) CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)				
Example	<pre> FTOS(conf)#router is FTOS(conf-router_isis)#redistribute bgp 1 level-1 metric 32 metric-type external route-map rmap-isis-to-bgp FTOS(conf-router_bgp)#show running-config isis ! router isis redistribute bgp 1 level-1 metric 32 metric-type external route-map rmap-isis-to-bgp </pre>				
Command History	<table border="0"> <tr> <td>Version 7.5.1.0</td> <td>Introduced IPv6 ISIS support</td> </tr> <tr> <td>Version 6.3.1.0</td> <td>Introduced</td> </tr> </table>	Version 7.5.1.0	Introduced IPv6 ISIS support	Version 6.3.1.0	Introduced
Version 7.5.1.0	Introduced IPv6 ISIS support				
Version 6.3.1.0	Introduced				
Usage Information	BGP to IS-IS redistribution supports “match” options using route maps. The metric value, level, and metric-type of redistributed routes can be set by the redistribution command. More advanced “set” options can be performed using route maps.				

redistribute ospf

E Redistribute routing information from an OSPF process.

Syntax **redistribute ospf** *process-id* [**level-1** | **level-1-2** | **level-2**] [**match** {**internal** | **external**}] [**metric** *metric-value*] [**metric-type** {**external** | **internal**}] [**route-map** *map-name*]

To return to the default values, enter the **no redistribute ospf** *process-id* [**level-1** | **level-1-2** | **level-2**] [**match** {**internal** | **external**}] [**metric** *metric-value*][**metric-type** {**external** | **internal**}] [**route-map** *map-name*] command.

Parameters

<i>process-id</i>	Enter a number that corresponds to the OSPF process ID to be redistributed. Range: 1 to 65355
metric <i>metric-value</i>	(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: <ul style="list-style-type: none"> • external • internal
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This is the default.

match {external | internal} (OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are

- **internal**
- **external**

route-map map-name *map-name* is an identifier for a configured route map.

The route map should filter imported routes from the source routing protocol to the current routing protocol.

If you do not specify a *map-name*, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.

Defaults As above

Command Modes ROUTER ISIS (*for IPv4*)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

Version 7.5.1.0	Introduced IPv6 ISIS support
Version 6.3.1.0	Introduced

Usage Information How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the [metric-style](#) command. If the [metric-style](#) command is set for narrow mode and the metric value in the [redistribute ospf](#) command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the [metric-style](#) command is set for wide mode, an the metric value in the [redistribute ospf](#) command is advertised.

router isis

E Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

Syntax **router isis** [*tag*]

To disable IS-IS routing, enter **no router isis** [*tag*].

Parameters *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

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

ip router isis	Configure IS-IS routing processes for IP on interfaces and attach an area designator to the routing process.
net	Configure an IS-IS network entity title (NET) for a routing process.
is-type	Assign a type for a given area.

set-overload-bit

- E** Configure the router to set the overload bit in its non-pseudonode LSPs. This prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

Syntax **set-overload-bit**

To return to the default values, enter **no set-overload-bit**.

Defaults Not set.

Command Mode ROUTER ISIS (*for IPv4*)

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Usage Information Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.

Command History

Version 7.8.1.0	Introduced MT ISIS support
Version 6.3.1.0	Introduced

show config

- E** 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*)

Example 1 (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
  set-overload-bit
  spf-interval level-1 100 15 20
  spf-interval level-2 120 20 25
  exit-address-family
```

Example 2
(address-family-ipv6 mode)

```

FTOS(conf-router_isis-af_ipv6)#show conf
!
address-family ipv6 unicast
maximum-paths 16
multi-topology transition
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family

```

show isis database

E Display the IS-IS link state database.

Syntax `show isis database [level-1 | level-2] [local] [detail | summary] [/spid]`

Parameters

level-1 (OPTIONAL) Displays the Level 1 IS-IS link-state database.

level-2 (OPTIONAL) Displays the Level 2 IS-IS link-state database.

local (OPTIONAL) Displays local link-state database information.

detail (OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.

summary (OPTIONAL) Summary of link-state database information displays when specified.

spid (OPTIONAL) Display only the specified LSP.

Command Modes

EXEC
EXEC Privilege

Example

```

FTOS#show isis database

IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
ISIS.00-00     * 0x00000006  0xCF43        580            0/0/0

IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
ISIS.00-00     * 0x00000006  0xCF43        580            0/0/0
!
FTOS#show isis database detail ISIS.00-00

IS-IS Level-1 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
ISIS.00-00     * 0x0000002B  0x853B        1075           0/0/0
  Area Address: 49.0000.0001
  NLPID:        0xCC 0x8E
  IP Address:   10.1.1.1
  IPv6 Address: 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 (MT-IPv6) 1011::/64
Metric: 10          IPv6 1511::/64
Metric: 10          IP 10.1.1.0 255.255.255.0
Hostname:          ISIS

```

IS-IS Level-2 Link State Database

```

LSPID              LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
ISIS.00-00         * 0x0000002D  0xB2CD        1075           0/0/0
  Area Address: 49.0000.0001
  NLPID:           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 30-82. Command Example Fields

Field	Description
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.

Table 30-82. Command Example Fields

Field	Description
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

E 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

```
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

E Display IS-IS host names configured or learned on the E-Series.

Syntax `show isis hostname`

Command Modes EXEC

EXEC Privilege

Example

```

FTOS#show isis hostname
System Id          Dynamic Name    Static Name
*F100.E120.0013 Force10      ISIS
FTOS#

```

show isis interface

E Display detailed IS-IS interface status and configuration information.

Syntax `show isis interface [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 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 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

```

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-3.02
    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--

```

show isis neighbors

E Display information about neighboring (adjacent) routers.

Syntax `show isis neighbors [level-1 | level-2] [detail] [interface]`

Parameters

- level-1** (OPTIONAL) Displays information about Level 1 IS-IS neighbors.
- level-2** (OPTIONAL) Displays information about Level 2 IS-IS neighbors.
- 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 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

```
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
FTOS#
```

Table 30-83. show isis neighbors Command Example Fields

Field	Description
System Id	The value that identifies a system in an area.
Interface	The interface, slot, and port in which the router was discovered.
State	The value providing status about the adjacency state. The valid values are Up and Init.
Type	This value displays the adjacency type (Layer 2, Layer 2 or both), and.
Priority	IS-IS priority advertised by the neighbor. The neighbor with highest priority becomes the designated router for the interface.
Uptime	Displays the interfaces uptime.
Circuit Id	The neighbor's interpretation of the designated router for the interface.

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

E Display IS-IS routing information.

Syntax `show isis protocol`

Command Modes EXEC

EXEC Privilege

Example

```
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

E 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 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

```

FTOS#sho is 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 30-84. Command Example Fields

Item	Description
Level-1/Level-2 Hellos (sent/rcvd)	Displays the number of Hello packets sent and received.
PTP Hellos (sent/rcvd)	Displays the number of point-to-point Hellos sent and received.
Level-1/Level-2 LSPs sourced (new/refresh)	Displays the number of new and refreshed LSPs.
Level-1/Level-2 LSPs flooded (sent/rcvd)	Displays the number of flooded LSPs sent and received.
Level-1/Level-2 LSPs CSNPs (sent/rcvd)	Displays the number of CSNP LSPs sent and received.
Level-1/Level-2 LSPs PSNPs (sent/rcvd)	Displays the number of PSNP LSPs sent and received.
Level-1/Level-2 DR Elections	Displays the number of times designated router elections ran.
Level-1/Level-2 SPF Calculations	Displays the number of shortest path first calculations.
LSP checksum errors received	Displays the number of checksum errors LSPs received.
LSP authentication failures	Displays the number of LSP authentication failures.

spf-interval



Specify the minimum interval between Shortest Path First (SPF) calculations.

Syntax `spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]`

To restore default values, use the **no spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]** command.

Parameters

level-1	(OPTIONAL) Enter the keyword level-1 to apply the configuration to Level-1 SPF calculations.
level-2	(OPTIONAL) Enter the keyword level-2 to apply the configuration to Level-2 SPF calculations.
<i>interval seconds</i>	Enter the maximum number of seconds between SPF calculations. Range: 0 to 120 seconds Default: 10 seconds
<i>initial_wait_interval seconds</i>	(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. Range: 0 to 120 seconds Default: 5 second
<i>second_wait_interval seconds</i>	(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. Range: 0 to 120 seconds Default: 5 seconds

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 Force10's implementation of Link Aggregation Control Protocol (LACP) for the creation of dynamic link aggregation groups (LAGs — called *port-channels* in FTOS parlance). For static LAG commands, refer to the section [Port Channel Commands](#) in the Interfaces chapter), based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

Commands in this chapter generally are supported on all three Dell Force10 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 FTOS option provides hitless dynamic LACP states (no noticeable impact to dynamic LACP states after an RPM failover) on E-Series. Refer to [redundancy protocol](#) in the High Availability chapter.

clear lacp counters

C E S 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 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	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 on E-Series
Related Commands	show lacp Display the lacp configuration

debug lacp

C **E** **S**

Debug LACP (configuration, events etc.)

Syntax `debug lacp [config | events | pdu [in | out | [interface [in | out]]]]`

To disable LACP debugging, use the **no debug lacp [config | events | pdu [in | out | [interface [in | out]]]]** command.

Parameters

config (OPTIONAL) Enter the keyword **config** to debug the LACP configuration.

events (OPTIONAL) Enter the keyword **events** to debug LACP event information.

pdu in | out (OPTIONAL) Enter the keyword **pdu** to debug LACP Protocol Data Unit information. Optionally, enter an **in** or **out** parameter to:

- Receive enter **in**
- Transmit enter **out**

interface in | out (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.

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	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 on E-Series
------------------------	--

lacp long-timeout

C **E** Configure a long timeout period (30 seconds) for an LACP session.

Syntax **lacp long-timeout**

To reset the timeout period to a short timeout (1 second), use the **no lacp long-timeout** command.

Defaults 1 second

Command Modes INTERFACE (*conf-if-po-number*)

Command History

Version 7.6.1.0	Support added for S-Series
Version 7.5.1.0	Support added for C-Series
Version 7.5.1.0	Introduced on E-Series

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

C **E** **S** Configure the port priority to influence which ports will be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Syntax **lacp port-priority** *priority-value*

To return to the default setting, use the **no lacp port-priority** *priority-value* command.

Parameters

<i>priority-value</i>	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

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 on E-Series

lacp system-priority

C **E** **S**

Configure the LACP system priority.

Syntax `lacp system-priority priority-value`

Parameters *priority-value* Enter the system-priority value. The higher the value, the lower the priority.
Range: 1 to 65535
Default: 32768

Defaults 32768

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 6.2.1.1	Introduced on E-Series

port-channel mode

C **E** **S**

Configure the LACP port channel mode.

Syntax `port-channel number mode [active] [passive] [off]`

Parameters

number Enter the keyword **port-channel** followed by a number:
C-Series and **S-Series** Range: 1-128
E-Series Range: 1 to 255 for TeraScale and 1 to 512 for ExaScale.

active Enter the keyword **active** to set the mode to the active state.*

passive Enter the keyword **passive** to set the mode to the passive state.*

off Enter the keyword **off** to set the mode to the off state.*

* The LACP modes are defined in the table below.

Defaults **off**

Command Modes INTERFACE

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

Usage Information The LACP modes are defined in the following table.

Table 31-85. LACP Modes

Mode	Function
active	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.

passive	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.
off	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.

port-channel-protocol lacp

C **E** **S** 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

C **E** **S** 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 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
Version 7.5.1.0 Support added for C-Series
Version 6.2.1.1 Introduced

Example 1
(port-channel-number)

```
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   Admin: State ACEHJLMP Key 1      Priority 128
          Oper: State ACEGIKNP Key 1      Priority 128
  Partner Admin: State BDFHJLMP Key 0      Priority 0
          Oper: State BCEGIKNP Key 1      Priority 128
FTOS#
```

Example 2
(sys-id)

```
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
(counter)

```
FTOS#show lacp 1 counters
```

```
-----
Port          LACP PDU          Marker PDU          Unknown  Illegal
              Xmit    Recv            Xmit    Recv            Pkts Rx  Pkts Rx
-----
Gi 10/6      200      200             0        0                0        0
FTOS#
```

Related
Commands

[clear lacp counters](#)

Clear the LACP counters.

[show interfaces port-channel](#)

Display information on configured Port Channel groups.

Layer 2

Overview

This chapter describes commands to configure Layer 2 features. It contains the following sections:

- [MAC Addressing Commands](#)
- [Virtual LAN \(VLAN\) Commands](#)

The commands that are supported on each platform are indicated by these characters, where appropriate, under each command heading: **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](#)
- [show mac learning-limit](#)

clear mac-address-table dynamic

C **E** **S** 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 <i>mac-address</i>	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 <i>interface</i>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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.
vlan <i>vlan-id</i>	Enter the keyword vlan followed by a VLAN ID number from 1 to 4094.

Command Modes 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

mac accounting destination

E 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**.

Parameters

mac-address	Enter the MAC address in the nn:nn:nn:nn:nn:nn format to count Layer 2 packets or bytes sent to that MAC address.
vlan <i>vlan-id</i>	Enter the keyword vlan followed by the VLAN ID to count Layer 2 packets or bytes sent to the VLAN. Range: 1 to 4094.
bytes	(OPTIONAL) Enter the keyword bytes to count only bytes
packets	(OPTIONAL) Enter the keyword packets to count only packets.

Defaults Not configured.

Command Modes INTERFACE (available on physical interfaces only)

Command History Version 7.4.1.0 Introduced on E-Series

Usage Information You must place the interface in Layer 2 mode (using the [switchport](#) command) prior to configuring the [mac accounting destination](#) command.

mac-address-table aging-time

C **E** **S** 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

C **E** **S**

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

mac-address

Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.

output *interface*

Enter the keyword **output** followed by one of the following interfaces:

- 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 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*

Enter the keyword **vlan** followed by a VLAN ID.
Range:1 to 4094.

Defaults Not configured.

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

Related Commands

[show mac-address-table](#) Displays the MAC address table.

mac-address-table station-move threshold

C **E**

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

E Reduce the amount of time FTOS 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 FTOS 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

C **E** **S** Ensure that ARP refreshes the egress interface when a station move occurs due to a topology change.

Syntax [no] **mac-address-table station-move refresh-arp**

Defaults 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 Refer to the “NIC Teaming” section of the Layer 2 chapter in the *FTOS Configuration Guide* for details on using this command.

mac cam fib-partition

E 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 MAC CAM for MAC address learning. With this configuration, no MAC ACLs are processed.
<i>slot-number</i>	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

C **E** **S** Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

Syntax `mac learning-limit address_limit [vlan vlan-id] [dynamic] [no-station-move | station-move]`

Parameters

<i>address_limit</i>	Enter the maximum number of MAC addresses learned. Range: 1 to 1000000
vlan <i>vlan-id</i>	On the 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.
station-move	(OPTIONAL) Enter the keyword station-move to allow a station move on learned MAC addresses.

Defaults 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

Command History

Version 8.3.1.0	Added vlan option on E-Series.
Version 8.2.1.0	Introduced on S-Series
Version 7.7.1.0	Introduced on C-Series; added station-move option
Version 6.5.1.0	Added support for MAC Learning-Limit on LAG

Usage Information This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

If the **vlan** option is not specified, 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, unconfigure the existing configuration first and then reapply the limit with a lower value.

Although you can convert manually-configured MAC addresses to sticky MAC addresses ([mac learning-limit no-station-move](#)), it is not recommended.

Related Commands

clear counters	Clear counters used in the show interface command
clear mac-address-table dynamic	Clear the MAC address table of all MAC address learned dynamically.
show mac learning-limit	Display MAC learning-limit configuration.

mac learning-limit learn-limit-violation

C **E** **S**

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

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 station-move-violation

C **E** **S**

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

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

Defaults

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

C **E** **S** 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)

E 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

linecard slot (REQUIRED) Enter the keyword **linecard** followed by a slot number to select the linecard for which to gather information.
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.
E-Series range: 0 or 1

count (REQUIRED) Enter the keyword **count** to display CAM usage by interface type.

interface <i>interface</i>	(OPTIONAL) Enter the keyword interface followed by the interface type, slot and port information: <ul style="list-style-type: none"> 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: <p>E-Series Range: 1 to 255 for TeraScale and 1 to 512 for ExaScale.</p> 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 <i>vlan-id</i>	(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

C Display the results of the BCMI2 check command.

Syntax **show cam maccheck linecard** *slot port-set port-pipe*

Parameters

linecard *slot* (REQUIRED) Enter the keyword **linecard** followed by a slot number to select the linecard for which to gather information.
C300 range: 0 to 7; **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

Command Modes
EXEC
EXEC Privilege

Command History
Version 7.6.1.0 Introduced on C-Series

Example 1

```

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=0xffff,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_I
D=0,REMOTE_TRUNK=0,L3=0,MAC_BLOCK_INDEX=0,STATIC_BIT=1,RPE=0,MIR-
ROR=0,VALID=1,EVEN_PARITY=0,HITDA=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,S
CP=0,TGID_LO=0,PORT_TGID=0,TGID_PORT=0,T=0,TGID_HI=0,L2MC_PTR=0,MODULE_ID=0x
10,REMOTE_TRUNK=0,L3=0,MAC_BLOCK_INDEX=0,STATIC_BIT=0,RPE=0,MIR-
ROR=0,VALID=1,EVEN_PARITY=1,HITDA=1,HITSA=1>
```

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

Usage Information

Use this command to check various flags associated with each MAC address in the CAM.

The previous example 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 (**0xffff**), as shown in the examples below. 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 2 (show mac-address-table)

```
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 3 (show cam mac linecard)

```
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)

C **E** 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 (C150); 0 to 8 (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 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.

static

(OPTIONAL) Enter the keyword **static** to display only those MAC address 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 7.5.1.0 Added support for C-Series
pre-Version 6.2.1.1 Introduced on E-Series

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         0      00:01:e8:0d:b7:3b    LOCAL_DA  1e000
1         1         0      00:01:e8:0d:b7:3a    LOCAL_DA  1e000
101       0         0      00:01:e8:00:04:00    SYSTEM_STATIC  01c05
102       0         0      01:80:00:00:00:00    SYSTEM_STATIC  01c05
103       0         0      01:00:0c:cc:cc:cc    SYSTEM_STATIC  01c01
104       0         0      01:80:c2:00:00:02    SYSTEM_STATIC  01c02
105       0         0      01:80:c2:00:00:0e    SYSTEM_STATIC  01c01
106       0         0      00:01:e8:0d:b7:68    SYSTEM_STATIC  DROP
107       0         0      00:01:e8:0d:b7:67    SYSTEM_STATIC  DROP
108       0         0      00:01:e8:0d:b7:66    SYSTEM_STATIC  DROP
109       0         0      00:01:e8:0d:b7:65    SYSTEM_STATIC  DROP
110       0         0      00:01:e8:0d:b7:64    SYSTEM_STATIC  DROP
111       0         0      00:01:e8:0d:b7:63    SYSTEM_STATIC  DROP
112       0         0      00:01:e8:0d:b7:62    SYSTEM_STATIC  DROP
113       0         0      00:01:e8:0d:b7:61    SYSTEM_STATIC  DROP
114       0         0      00:01:e8:0d:b7:60    SYSTEM_STATIC  DROP
115       0         0      00:01:e8:0d:b7:5f    SYSTEM_STATIC  DROP
116       0         0      00:01:e8:0d:b7:5e    SYSTEM_STATIC  DROP
117       0         0      00:01:e8:0d:b7:5d    SYSTEM_STATIC  DROP
FTOS#
```

show cam mac stack-unit

S 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 <i>unit_number</i>	(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 <i>port-pipe</i>	(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 <i>mac-addr</i>	(OPTIONAL) Enter the keyword address followed by a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
dynamic	(OPTIONAL) Enter the keyword dynamic to display only those MAC addresses learned dynamically by the switch.
static	(OPTIONAL) Enter the keyword static to display only those MAC address specifically configured on the switch.
interface <i>interface</i>	(OPTIONAL) Enter the keyword interface followed by the interface type, slot and port information: <ul style="list-style-type: none">• 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 <i>vlan-id</i>	(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

show mac-address-table

C **E** **S** 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

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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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.
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 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 1

```
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
FTOS#
```


Table 32-86. show mac-address-table Information

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static) or learned (Dynamic).
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: <ul style="list-style-type: none"> • gi—Gigabit Ethernet followed by a slot/port. • po—Port Channel followed by a number. Range: 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).

**Example 2
(count)**

```

FTOS#show mac-address-table count
MAC Entries for all vlans :
Dynamic Address Count :           5
Static Address (User-defined) Count : 0
Total MAC Addresses in Use:       5
FTOS#

```

Table 32-87. show mac-address-table count Information

Line Beginning with	Description
MAC Entries...	Displays the number of MAC entries learnt per VLAN.
Dynamic Address...	Lists the number of dynamically learned MAC addresses.
Static Address...	Lists the number of user-defined MAC addresses.
Total MAC...	Lists the total number of MAC addresses used by the switch.

**Related
Commands**

[show mac-address-table aging-time](#) Display MAC aging time.

show mac-address-table aging-time



Display the aging times assigned to the MAC addresses on the switch.

Syntax

show mac-address-table aging-time [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*

On the E-Series, enter the keyword **vlan** followed by the VLAN ID to display the MAC address aging time for MAC addresses on the VLAN.
Range: 1 to 4094.

Command Modes

EXEC

EXEC Privilege

Command History	Version 8.3.1.0	Added the vlan option on the E-Series.
	Version 7.7.1.0	Introduced on C-Series and S-Series
	pre-Version 6.2.1.1	Introduced on E-Series
Example	<pre>FTOS#show mac-address-table aging-time Mac-address-table aging time : 1800 FTOS#</pre>	
Related Commands	show mac-address-table	Display the current MAC address configuration.

show mac accounting destination

E 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]] [vlan vlan-id]`

Parameters	<i>mac-address</i>	(OPTIONAL) Enter the MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
	interface <i>interface</i>	(OPTIONAL) Enter the keyword interface followed by the interface type, slot and port information: <ul style="list-style-type: none"> 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 <i>vlan-id</i>	(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 Force10 Monitor MIB. For more information on enabling SNMP, refer to Chapter 3 of the *FTOS Configuration Guide*.



Note: Currently, the Force10 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 Force10 MONITOR MIB. For example:

```
% snmpwalk -C c -v 2c -c public 133.33.33.131 enterprise.6027.3.3.3
```

Example FTOS-1#sh mac accounting destination interface gigabitethernet 2/1

Destination	Out	Port	VLAN	Packets	Bytes
00:44:00:00:00:02	Te	11/0	1000	10000	5120000
00:44:00:00:00:01	Te	11/0	1000	10000	5120000

```

00:22:00:00:00:00 Te 11/0 1000 10000 5120000
00:44:00:00:00:02 Te 11/0 2000 10000 5120000
00:44:00:00:00:01 Te 11/0 2000 10000 5120000

FTOS-1#

```

Related Commands [show mac accounting access-list](#) Display MAC access list configurations and counters (if configured).

show mac cam

E 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

```

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 32-88. show mac cam Information

Field	Description
Slot	Lists the active line card slots.
Type	Lists the type of line card present in the slot.
MAC CAM Size	Displays the total CAM size available. 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.
MAC FIB Entries	Displays the amount and percentage of CAM available for MAC addresses.
MAC ACL Entries	Displays the amount and percentage of CAM available for MAC ACLs.

show mac learning-limit

C **E** 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 (OPTIONALY) Enter the keyword **violate-action** to display the MAC learning limit violation status.

detail (OPTIONAL) Enter the keyword **detail** to display the MAC learning limit in detail.

interface interface

(OPTIONAL) Enter the keyword **interface** with the following keywords and slot/port or number information:

- For a 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 Port Channel interface, enter the keyword **port-channel** followed by a number:

C-Series Range: 1-128

E-Series Range: 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 8.3.1.0 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:

```
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:

```
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
Forcel0#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](#)

Refer also to [VLAN Stacking](#) and VLAN-related commands, such as [portmode hybrid](#), in [Chapter 25, 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
Version 7.6.1.0 Introduced on C-Series and S-Series
Version 6.3.1.0 Introduced on E-Series

Related Commands [show vlan](#) Display VLAN configuration.

default vlan-id

C **E** **S**

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

<i>vlan-id</i>	Enter the VLAN ID number of the VLAN to become the new Default VLAN. Range: 1 to 4094. Default: 1
----------------	---

Defaults The Default VLAN is VLAN 1.

Command Modes CONFIGURATION

Command History

Version 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

interface vlan	Configure a VLAN.
--------------------------------	-------------------

default-vlan disable

C **E** **S**

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

E **X**

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 line cards/port-pipes) by default.

Command Modes CONFIGURATION

Command History

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

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, IP 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 1107787777
Internet address is not set
MTU 1554 bytes, IP 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, 10000000 bytes
Output Statistics:
    200000 packets, 20800000 bytes
Time since last interface status change: 01:36:01
FTOS#
```

Usage Information FTOS 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

C **E** **S**

Assign a name to the VLAN.

Syntax

name *vlan-name*

To remove the name from the VLAN, enter **no name**.

Parameters

vlan-name Enter up to 32 characters as the name of the VLAN.

Defaults

Not configured.

Command Modes

INTERFACE VLAN

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 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

C **E** **S**

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

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

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

- Version 7.8.1.0 Augmented to display PVLAN data for C-Series and S-Series; revised output to include Description field to display user-entered VLAN description
- Version 7.6.1.0 Introduced on S-Series; revised output to display Native VLAN
- Version 7.5.1.0 Introduced on C-Series
- pre-Version 6.2.1.1 Introduced on E-Series

Example 1

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		
	2	Active		U Po1(Gi 13/0) T Po20(Gi 13/6), Gi 13/25 T Gi 13/7
	3	Active		T Po20(Gi 13/6) T Gi 13/7 U Gi 13/1
	4	Active		U Po2(Gi 13/2) T Po20(Gi 13/6) T Gi 13/7
	5	Active		T Po20(Gi 13/6) T Gi 13/7 U Gi 13/3
	6	Active		U Po3(Gi 13/4) T Po20(Gi 13/6) T Gi 13/7
	7	Active		T Po20(Gi 13/6) T Gi 13/7 U Gi 13/5
P	100	Active		T Po1(Gi 0/1)

```

C 101 Inactive T Gi 0/2
I 102 Inactive T Gi 0/3
FTOS# T Gi 0/4

```

Table 32-89. show vlan Information

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

**Example 2
(show vlan id)**

```
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
```

```

NUM      Status      Description      Q Ports
40      Active
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
```

```

NUM      Status      Description      Q Ports
41      Active
T Gi 13/47

```

```
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
```

```

NUM      Status      Description      Q Ports
42      Active
U Gi 13/47
FTOS#

```

**Example 3
(show vlan brief)**

```

FTOS#show vlan br
VLAN Name                               STG   MAC Aging IP Address
-----
1                                         0     1800      unassigned
2                                         0     1800      2.2.2.2/24
3                                         0     1800      3.3.3.2/24
FTOS#

```

**Example 4
(Using VLAN
Name)**

```

FTOSconf)#interface vlan 222
FTOS(conf-if-vl-222)#name test
FTOS(conf-if-vl-222)#do show vlan name test

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
    x - Dot1x untagged, X - Dot1x tagged
    G - GVRP tagged, M - Vlan-stack

      NUM      Status      Description                               Q Ports
      222      Inactive
FTOS(conf-if-vl-222)#
FTOS#

```

**Related
Commands**

[vlan-stack compatible](#) Enable the Stackable VLAN feature on the selected VLAN.

[interface vlan](#) Configure a VLAN.

tagged



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

Syntax

tagged *interface*

To remove a tagged interface from a VLAN, use **no tagged interface** command.

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 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**

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

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

track ip *interface*

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

Parameters

interface Enter the following keywords and slot/port or number information:

- For a 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 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.

Defaults

Not configured

Command Modes

INTERFACE VLAN

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

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

[interface vlan](#) Configure a VLAN.
[tagged](#) Specify which interfaces in a VLAN are tagged.

untagged



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

Syntax `untagged interface`

To remove an untagged interface from a VLAN, use the **no untagged interface** command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a 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 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

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

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

interface vlan	Configure a VLAN.
tagged	Specify which interfaces in a VLAN are tagged.

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 FTOS implementation of LLDP is based on IEEE standard 801.1ab.

The basic LLDP commands are supported by FTOS on all Dell Force10 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.

Refer to the Link Layer Discovery Protocol chapter of the *FTOS Configuration Guide* for details on implementing LLDP/LLDP-MED.

advertise dot1-tlv

C **E** **S** 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

port-protocol-vlan-id	Enter the keyword port-protocol-vlan-id to advertise the port protocol VLAN identification TLV.
port-vlan-id	Enter the keyword port-vlan-id to advertise the port VLAN identification TLV.
vlan-name	Enter the keyword vlan-name to advertise the vlan-name TLV. This keyword is only supported on C-Series and S-Series.

Defaults Disabled

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

Command History

Version 7.7.1.0	Introduced on S-Series, added vlan-name option.
Version 7.6.1.0	Introduced on C-Series
Version 7.4.1.0	Introduced on 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 dot3-tlv

C **E** **S** Advertise dot3 TLVs (Type, Length, Value).

Syntax advertise dot3-tlv {max-frame-size}

To remove advertised dot3-tlv, use the no advertise dot3-tlv {max-frame-size} command.

Parameters

max-frame-size	Enter the keyword max-frame-size to advertise the dot3 maximum frame size.
----------------	---

Defaults No default values or behavior

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

advertise management

C **E** **S** 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-description to advertise the system description 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

C **E** **S** Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

Syntax clear lldp counters *interface*

Parameters

interface	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none">• 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.
------------------	---

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

clear lldp neighbors

C **E** **S**

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.

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

debug lldp interface

C **E** **S**

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.

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

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

disable

C **E** **S** 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

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

hello

C **E** **S** 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

<code>seconds</code>	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

C **E** **S**

Set LLDP to receive or transmit.

Syntax

mode {tx | rx}

To return to the default, use the `no mode {tx | rx}` command.

Parameters

tx Enter the keyword `tx` to set the mode to transmit.

rx Enter the keyword `rx` to set the mode to receive.

Defaults

Both transmit and receive

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

[protocol lldp \(Configuration\)](#) Enable LLDP globally.

[show lldp neighbors](#) Display the LLDP neighbors

multiplier

C **E** **S**

Set the number of consecutive misses before LLDP declares the interface dead.

Syntax

multiplier *integer*

To return to the default, use the `no multiplier integer` command.

Parameters

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

Defaults

4 x hello

Command Modes

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

protocol lldp (Configuration)

C **E** **S**

Enable LLDP globally on the switch.

Syntax

protocol lldp

To disable LLDP globally on the chassis, use the `no protocol lldp` command.

Defaults	Disabled	
Command Modes	CONFIGURATION (conf-lldp)	
Command History	Version 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

protocol lldp (Interface)

C **E** **S** Enter the LLDP protocol in the INTERFACE mode.

Syntax [no] protocol lldp

To return to the global LLDP configuration mode, use the **no protocol lldp** command from the Interface mode.

Defaults LLDP is not enabled on the interface.

Command Modes 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

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

C **E** **S** Display LLDP neighbor information for all interfaces or a specified interface.

Syntax show lldp neighbors [*interface*] [detail]

Parameters	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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.
	<i>detail</i>	(OPTIONAL) Enter the keyword detail to display all the TLV information, timers, and LLDP tx and rx counters.

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
```

Usage Information Omitting the keyword `detail` displays only the remote chassis ID, Port ID, and Dead Interval.

show lldp statistics

C E S Display the 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

C E S 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](#)

FTOS 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: **C** **S**

The E-Series generally supports the commands, too, as indicated by the **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 Force10 system is an LLDP-MED network connectivity device.

With regard to connected endpoint devices, LLDP-MED provides network connectivity devices with the ability to:

- manage inventory
- manage Power over Ethernet (POE)
- identify physical location
- identify network policy

advertise med guest-voice

C **E** **S**

Configure the system to advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support interactive voice services.

Syntax `advertise med guest-voice { vlan-id layer2_priority DSCP_value } | { priority-tagged number }`

To return to the default, use the `no advertise med guest-voice { vlan-id layer2_priority DSCP_value } | { priority-tagged number }` command.

Parameters

<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
<i>layer2_priority</i>	Enter the Layer 2 priority. Range: 0 to 7
<i>DSCP_value</i>	Enter the DSCP value. Range: 0 to 63
<i>priority-tagged number</i>	Enter the keyword <code>priority-tagged</code> 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

C **E** **S**

Configure the system to advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data.

Syntax `advertise med guest-voice-signaling { vlan-id layer2_priority DSCP_value } | { priority-tagged number }`

To return to the default, use the `no advertise med guest-voice-signaling { vlan-id layer2_priority DSCP_value } | { priority-tagged number }` command.

Parameters	<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
	<i>layer2_priority</i>	Enter the Layer 2 priority. Range: 0 to 7
	<i>DSCP_value</i>	Enter the DSCP value. Range: 0 to 63
	<i>priority-tagged number</i>	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 location-identification

C **E** **S** Configure the system to advertise a location identifier.

Syntax advertise med location-identification { coordinate-based *value* | civic-based *value* | ecs-elin *value* }

To return to the default, use the no advertise med location-identification { coordinate-based *value* | civic-based *value* | ecs-elin *value* } command.

Parameters	<i>coordinate-based value</i>	Enter the keyword coordinate-based followed by the coordinated based location in hexadecimal value of 16 bytes.
	<i>civic-based value</i>	Enter the keyword civic-based followed by the civic based location in hexadecimal format. Range: 6 to 255 bytes
	<i>ecs-elin value</i>	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

Usage Information	ECS —Emergency Call Service such as defined by TIA or National Emergency Numbering Association (NENA)	
	ELIN —Emergency Location Identification Number, a valid North America Numbering Plan format telephone number supplied for ECS purposes.	
Related Commands	debug lldp interface	Debug LLDP
	show lldp neighbors	Display the LLDP neighbors
	show running-config lldp	Display the LLDP running configuration

advertise med power-via-mdi

C **S** Configure the system to advertise the Extended Power via MDI TLV.

Syntax advertise med power-via-mdi
To return to the default, use the no advertise med power-via-mdi command.

Defaults unconfigured

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 7.7.1.0	Introduced on S-Series
Version 7.6.1.0	Introduced on C-Series

Usage Information Advertise the Extended Power via MDI on all ports that are connected to an 802.3af powered, LLDP-MED endpoint device.

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 softphone-voice

C **E** **S** Configure the system to advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone.

Syntax advertise med softphone-voice { *vlan-id 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	<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
	<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). Range: 0 to 7

	<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). Range: 0 to 63
	<i>priority-tagged number</i>	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 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	<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
	<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). Range: 0 to 7
	<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). Range: 0 to 63
	<i>priority-tagged number</i>	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

C **E** **S**

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

<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). Range: 0 to 7
<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). Range: 0 to 63
<i>priority-tagged number</i>	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

C **E** **S**

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

<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). Range: 0 to 7
<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). Range: 0 to 63

	<i>priority-tagged number</i>	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 voice



Configure the system to advertise a dedicated IP telephony handset or other appliances supporting interactive voice services.

Syntax `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	<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
	<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). Range: 0 to 7
	<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). Range: 0 to 63
	<i>priority-tagged number</i>	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 voice-signaling

C **E** **S**

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

<i>vlan-id</i>	Enter the VLAN ID. Range: 1 to 4094
<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). Range: 0 to 7
<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). Range: 0 to 63
<i>priority-tagged number</i>	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

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*]

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: **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 VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

group-address (OPTIONAL) Enter the group address in the **x:x:x:x::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 mld interface	Display the IPv6 MLD interface

debug ipv6 mld

E Enable debugging on IPv6 MLD packets.

Syntax debug 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 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	
Command History	Version 7.4.1.0	Introduced

ipv6 mld explicit-tracking

E 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)

Command History Version 7.4.1.0 Introduced

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

E 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

E 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.

Parameters *seconds* Enter the querier timeout in seconds.
Range: 60 - 300
Default: 255

Defaults 255 seconds

Command Modes INTERFACE (conf-if)

Command History Version 7.4.1.0 Introduced

ipv6 mld query-interval

E 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

<i>seconds</i>	Enter the interval in seconds. Range: 1 - 18000 Default: 125
----------------	--

Defaults 125 seconds

Command Modes INTERFACE (conf-if)

Command History

Version 7.4.1.0	Introduced
-----------------	------------

ipv6 mld query-max-resp-time

E 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

<i>seconds</i>	Enter the interval in seconds. Range: 1 - 25 Default: 10
----------------	--

Defaults 10 seconds

Command Modes INTERFACE (conf-if)

Command History

Version 7.4.1.0	Introduced
-----------------	------------

ipv6 mld static-group

E 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	<i>group-address</i>	(OPTIONAL) Enter the multicast group address in the X:X:X::X format. The :: notation specifies successive hexadecimal fields of zero.
	exclude <i>source-address</i>	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 <i>source-address</i>	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

E 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 FTOS supports MLD version 2 and is backward compatible with MLD version 1.

show ipv6 mld groups

E View the configured MDL groups.

Syntax show ipv6 mld groups [detail] [explicit] [link-local] [*group-address*] [interface *interface* [detail]] [summary]

Parameters	explicit	Enter this keyword to display explicit tracking information.
	link-local	Enter this keyword to display link-local groups.
	<i>group-address</i>	Enter the group address for which you want to display information.
	interface <i>interface</i>	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	<pre> FTOS#show ipv6 mld groups vlan 100 link-local ? detail Detailed information Pipe through a command <cr> ===== 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 [output omitted] </pre>

show ipv6 mld interface

E View the configured MDL interfaces.

Syntax show ipv6 mld interface [*interface*]

Parameters

interface Enter the keyword **interface** to display the configured MDL interfaces. Optionally, enter the [*interface*] 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 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

```
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

E 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

E 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

E 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

ipv6 mld snooping explicit-tracking

E 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 [show ipv6 mld snooping groups](#) Display the IPv6 MLD Snooping group information.

ipv6 mld snooping mrouter

E 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: <ul style="list-style-type: none">• 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 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-*n*)

Command History Version 7.4.1.0 Introduced

ipv6 mld snooping querier

E Enable the MLD querier processing for the VLAN interface.

Syntax ipv6 mld snooping querier

To disable the querier feature, use the `no ipv6 mld snooping querier` command.

Defaults Disabled

Command Modes INTERFACE VLAN (conf-if-vl-*n*)

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

E Display the IPv6 MLD Snooping group information.

Syntax show ipv6 mld snooping groups [*group-address*] [explicit] [link-local] [summary] [vlan]

Parameters

<i>group-address</i>	(OPTIONAL) Enter the multicast group address in the x:x: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

Example

```
FTOS#show ipv6 mld snooping groups summary
MLD snooping connected groups summary:
(*,G) routes :12
FTOS#
```


show ipv6 mld snooping mrouter

E Display information on the MLD Snooping router.

Syntax show ipv6 mld snooping mrouter [vlan]

Parameters **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

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. FTOS supports MSDP commands on the E-Series only, as indicated by the **E** 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

E Reset the TCP connection to the peer and clear all the peer statistics.

Syntax `clear ip msdp peer {peer address}`

Parameters *peer address* Enter the peer address in a dotted decimal format (A.B.C.D.)

Defaults Not configured

Command Modes EXEC Privilege

Command History Version 6.2.1.1 Introduced

clear ip msdp sa-cache

E 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

<i>group-address</i>	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

E Turn on MSDP debugging.

Syntax debug ip msdp {event *peer address* | packet *peer address* | pim}

To turn debugging off, use the no debug ip msdp {event *peer address* | packet *peer address* | pim} command.

Parameters

event <i>peer address</i>	Enter the keyword event followed by the peer address in a dotted decimal format (A.B.C.D.).
packet <i>peer address</i>	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

Command History

Version 6.2.1.1	Introduced
-----------------	------------

ip msdp cache-rejected-sa

E 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

<i>number</i>	Enter the number of rejected SA entries to cache. Range: 0 to 32766
---------------	--

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced
-----------------	------------

Related Commands [show ip msdp sa-cache rejected-sa](#) Display the rejected SAs in the SA cache.

ip msdp default-peer

E Define a default peer from which to accept all Source-Active (SA) messages.

Syntax ip msdp default-peer *peer address* [*list name*]

To remove the default peer, use the `no ip msdp default-peer { peer address } list name` command.

Parameters

<i>peer address</i>	Enter the peer address in a dotted decimal format (A.B.C.D.)
<i>list name</i>	Enter this keyword and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version 7.8.1.0	Added the <code>list</code> option, and removed the <code>prefix-list</code> option.
Version 6.2.1.1	Introduced

Usage Information If a list is not specified, all SA messages received from the default peer are accepted. You can enter multiple default peer commands.

ip msdp log-adjacency-changes

E 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

E 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

<i>name</i>	Enter a string of up to 16 characters long for as the mesh group name.
<i>peer address</i>	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

E 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	<i>interface</i>	<p>Enter the following keywords and slot/port or number information:</p> <ul style="list-style-type: none"> • 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 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 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	CONFIGURATION	
Command History	Version 6.2.1.1	Introduced

ip msdp peer

E 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	<i>peer address</i>	Enter the peer address in a dotted decimal format (A.B.C.D.)
	<i>connect-source interface</i>	<p>(OPTIONAL) Enter the keyword connect-source followed by one of the interfaces and slot/port or number information:</p> <ul style="list-style-type: none"> • 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 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 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.

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.

Related Commands

ip msdp sa-limit	Configure the MSDP SA Limit
clear ip msdp peer	Clear the MSDP peer.
show ip msdp	Display the MSDP information

ip msdp redistribute

E 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 <i>acl-name</i>	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 sa-filter

E 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

E 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 50000

Defaults Default 50000

Command Modes CONFIGURATION

Command History Version 7.5.1.0 Introduced

Usage Information

FTOS counts the SA messages originated by itself and those received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking). If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in FTOS will continue to be accepted. To enforce the limit in such situation, use the clear ip msdp sa-cache command.

Related Commands

[ip msdp peer](#) Configure the MSDP peer
[clear ip msdp peer](#) Clear the MSDP peer.
[show ip msdp](#) Display the MSDP information

ip msdp shutdown

E 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

E 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

E Display the MSDP peer status, SA cache, or peer summary.

Syntax show ip msdp {*peer peer address* | *sa-cache* | *summary*}

Parameters

<i>peer peer address</i>	Enter the keyword peer followed by the peer address in a dotted decimal format (A.B.C.D.)
<i>sa-cache</i>	Enter the keyword sa-cache to display the Source-Active cache.
<i>summary</i>	Enter the keyword summary to display a MSDP peer summary.

Defaults Not configured

Command Modes EXEC

EXEC Privilege

Command History Version 6.2.1.1 Introduced

Example 1 (peer)

```

FTOS#show ip msdp peer 100.1.1.1
Peer Addr: 100.1.1.1
  Local Addr: 100.1.1.2(639)  Connect Source: none
  State: Established Up/Down Time: 00:00:08
  Timers: KeepAlive 60 sec, Hold time 75 sec
  SourceActive packet count (in/out): 0/0
  SAs learned from this peer: 0
  SA Filtering:
    Input (S,G) filter: none
    Output (S,G) filter: none
FTOS#

```

Example 2 (sa-cache)

```

FTOS#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
GroupAddr      SourceAddr      RPAAddr      LearnedFrom      Expire UpTime
224.1.1.1      172.21.220.10  172.21.3.254  172.21.3.254    102 00:02:52
FTOS#

```

Example 3 (summary)

```

FTOS#show ip msdp summary
Peer Addr Local Addr State      Source SA Up/Down      Description
72.30.1.2 72.30.1.1  Established none      0 00:00:03  peer1
72.30.2.2 72.30.2.1  Established none      0 00:00:03  peer2
72.30.3.2 72.30.3.1  Established none      0 00:00:02  test-peer-3
FTOS#

```

show ip msdp sa-cache rejected-sa

E Display the rejected SAs in the SA cache.

Syntax show ip mdsp sa-cache rejected-sa

Defaults No default values or behavior

Command Modes EXEC

EXEC Privilege

Command History Version 7.4.1.0 Introduced

Example

```

FTOS#sh ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache 200 rejected SAs received, cache-size 1000
UpTime      GroupAddr      SourceAddr      RPAAddr      LearnedFrom      Reason
00:00:13    225.1.2.1      10.1.1.3        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.2      10.1.1.4        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.3      10.1.1.3        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.4      10.1.1.4        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.5      10.1.1.3        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.6      10.1.1.4        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.7      10.1.1.3        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.8      10.1.1.4        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.9      10.1.1.3        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.10     10.1.1.4        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.11     10.1.1.3        110.1.1.1    13.1.1.2         Rpf-Fail
00:00:13    225.1.2.11     10.1.1.3        110.1.1.1    13.1.1.2         Rpf-Fail

```

00:00:13	225.1.2.12	10.1.1.4	110.1.1.1	13.1.1.2	Rpf-Fail
00:00:13	225.1.2.13	10.1.1.3	110.1.1.1	13.1.1.2	Rpf-Fail
00:00:13	225.1.2.14	10.1.1.4	110.1.1.1	13.1.1.2	Rpf-Fail
00:00:13	225.1.2.15	10.1.1.3	110.1.1.1	13.1.1.2	Rpf-Fail
00:00:13	225.1.2.16	10.1.1.4	110.1.1.1	13.1.1.2	Rpf-Fail
00:00:13	225.1.2.17	10.1.1.3	110.1.1.1	13.1.1.2	Rpf-Fail
00:00:13	225.1.2.18	10.1.1.4	110.1.1.1	13.1.1.2	Rpf-Fail
00:00:13	225.1.2.19	10.1.1.3	110.1.1.1	13.1.1.2	Rpf-Fail
FTOS#					

Multiple Spanning Tree Protocol (MSTP)

Overview

Multiple Spanning Tree Protocol (MSTP), as implemented by FTOS, conforms to IEEE 802.1s. MSTP is supported by FTOS on all Dell Force10 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 edge-port`
- `tc-flush-standard`

debug spanning-tree mstp

C **E** **S** 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 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 MSTP events.

Command Modes EXEC Privilege

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#debug spanning-tree mstp bpdu gigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

description

C **E** **S** 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	pre-7.7.1.0	Introduced
Related Commands	protocol spanning-tree mstp	Enter Multiple SPANNING TREE mode on the switch.

disable

C **E** **S** 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
	Version 6.5.1.0	Introduced

Related Commands [protocol spanning-tree mstp](#) Enter MULTIPLE SPANNING TREE mode.

forward-delay

C **E** **S** The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

Syntax **forward-delay** *seconds*

To return to the default setting, enter **no forward-delay**.

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

C **E** **S**

Set the time interval between generation of Multiple Spanning Tree Bridge Protocol Data Units (BPDUs).

Syntax **hello-time** *seconds*

To return to the default value, enter **no hello-time**.

Parameters

<i>seconds</i>	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

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.
max-age	Change the wait time before MSTP refreshes protocol configuration information.

max-age

C **E** **S**

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

<i>max-age</i>	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

C **E** **S**

Configure the maximum hop count.

Syntax **max-hops** *number*

To return to the default values, enter **no max-hops**.

Parameters

<i>range</i>	Enter a number for the maximum hop count. Range: 1 to 40 Default: 20
--------------	--

Defaults 20 hops

Command Modes MULTIPLE SPANNING TREE

Command History

Version 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 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

C **E** **S**

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 <i>instance</i>	Enter the Multiple Spanning Tree Protocol Instance Range: zero (0) to 63
vlan <i>range</i>	Enter the keyword vlan followed by the identifier range value. Range: 1 to 4094
bridge-priority <i>priority</i>	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

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

Usage Information By default, all VLANs are mapped to MST instance zero (0) unless you use the **vlan range** command to map it to a non-zero instance.

name

C **E** **S** 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* 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

C **E** **S** 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

C **E** **S** 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

C **E** **S**

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

```
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

C **E** **S**

View the Multiple Spanning Tree configuration.

Syntax `show spanning-tree mst configuration`

Command Modes EXEC

EXEC Privilege

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#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

C **E** **S** View the Multiple Spanning Tree instance.

Syntax `show spanning-tree msti [instance-number [brief]] [guard]`

Parameters

<i>instance-number</i>	[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 8.4.2.1	The optional guard keyword was added.
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 Example 2 (with EDS & LBK))

Example 1

```
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
(with EDS & LBK)**

```
FTOS#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID    Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Interface
  Name      PortID  Prio Cost    Sts Cost      Designated
-----
Gi 0/0     128.257 128 20000  EDS 0        32768 0001.e801.6aa8 128.257
Interface
  Name      Role    PortID  Prio Cost    Sts Cost      Link-type Edge Boundary
-----
Gi 0/0     ErrDis 128.257 128 20000  EDS 0        P2P      No   No
```

```
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
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
(msti guard)**

```
FTOS#show spanning-tree msti 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 36-90. show spanning-tree msti guard Command Information

Field	Description
Interface Name	MSTP interface
Instance	MSTP instance
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut)
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard)

spanning-tree

C **E** **S** 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

C **E** **S** 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

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

spanning-tree mstp edge-port

C **E** **S** Configures the interface as an Multiple Spanning Tree edge port and optionally a Bridge Protocol Data Unit (BPDU) guard.

Syntax **spanning-tree mstp edge-port [bpduguard [shutdown-on-violation]]**

Parameters

mstp edge-port Enter the keywords **mstp** followed by 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.

Command Modes INTERFACE

Command History

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.

tc-flush-standard

C **E** **S** 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 Added support for S-Series

Version 7.5.1.0 Added support for C-Series

Version 6.5.1.0 Introduced

Usage Information

By default FTOS implements an optimized flush mechanism for MSTP. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, 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-routing](#)
- [ip multicast-limit](#)
- [mac-flood-list](#)
- [mtrace](#)
- [queue backplane multicast](#)
- [restrict-flooding](#)
- [show ip mroute](#)
- [show ip rpf](#)
- [show queue backplane multicast](#)

clear ip mroute

C **E** **S**

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

<i>group-address</i>	Enter multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
[<i>source-address</i>]	
*	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

E **X** 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

<i>vlan vlan-id</i>	Enter a VLAN ID to clear information learned through PIM-SM snooping about a specified VLAN. Valid VLAN IDs: 1 to 4094.
<i>group-address</i> [<i>source-address</i>]	(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.
*	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.
[show ip pim tib](#) Show the PIM Tree Information Base.

ip mroute

C **E** **S** Assign a static mroute.

Syntax ip mroute *destination mask* { *ip-address* | null 0 | { {bgp| ospf} *process-id* | isis | rip | static } { *ip-address* | tag | null 0 } } [distance]

To delete a specific static mroute, use the command ip mroute *destination mask* { *ip-address* | null 0 | { {bgp| ospf} *process-id* | isis | rip | static } { *ip-address* | tag | null 0 } } [distance].

To delete all mroutes matching a certain mroute, use the no ip mroute *destination mask* command.

Parameters

<i>destination</i>	Enter the IP address in dotted decimal format of the destination device.
<i>mask</i>	Enter the mask in slash prefix formation (/x) or in dotted decimal format.
null 0	(OPTIONAL) Enter the null followed by zero (0).

[protocol [process-id | tag] ip-address] (OPTIONAL) Enter one of the routing protocols:

- Enter the BGP as-number followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.
Range: 1-65535
- Enter the OSPF process identification number followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.
Range: 1-65535
- Enter the IS-IS alphanumeric tag string followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.
- Enter the RIP IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.

static ip-address (OPTIONAL) Enter the Static IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.

ip-address (OPTIONAL) Enter the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.

distance (OPTIONAL) Enter a number as the distance metric assigned to the mroute.
Range: 0 to 255

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

E 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-routing

C **E** **S** 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.

ip multicast-limit

C **E** **S** 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](#) View the IGMP groups.

mac-flood-list

E Provide 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

<i>mac-address</i>	Enter a multicast MAC address in hexadecimal format.
<i>mac-mask</i>	Enter the MAC Address mask.
vlan <i>vlan-list</i>	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 <i>min-speed</i>	(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

E Trace a multicast route from the source to the receiver.

Syntax `mtrace {source-address/hostname} {destination-address/hostname} {group-address}`

Parameters

source-address/hostname Enter the source IP address in dotted decimal format (A.B.C.D).

destination-address/hostname Enter the destination (receiver) IP address in dotted decimal format (A.B.C.D).

group-address Enter the multicast group address in dotted decimal format (A.B.C.D).

Command Modes EXEC Privilege

Command History

Version 7.5.1.0 Expanded to support originator

Version 7.4.1.0 Expanded to support intermediate (transit) router

E-Series legacy command

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). FTOS supports the Mtrace client and transmit functionality.

As an Mtrace client, FTOS transmits Mtrace queries, receives, parses and prints out the details in the response packet received.

As an Mtrace transit or intermediate router, FTOS returns the response to Mtrace queries. Upon receiving the Mtrace request, FTOS computes the RPF neighbor for the source, fills in the request and the 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

E Reallocate 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

```
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

E **T**

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 *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 VMANs.

**Related
Commands**

[mac-flood-list](#)

Flood multicast frames with specified MAC addresses to all ports in a VLAN.

show ip mroute

C **E** **S**

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

static

(OPTIONAL) Enter the keyword **static** to view static multicast routes.

group-address
[*source-address*]

(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.

active [*rate*]

(OPTIONAL) Enter the keyword **active** to view only active multicast routes. Enter a rate to view active routes over the specified rate.

Range: 0 to 10000000

count	(OPTIONAL) Enter the keyword count to view the number of multicast routes and packets on the E-Series.
snooping [vlan <i>vlan-id</i>] [<i>group-address</i>] [<i>source-address</i>]]	(OPTIONAL) E-Series ExaScale only: Enter the keyword snooping 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.
summary	(OPTIONAL) Enter the keyword summary to view routes in a tabular format.

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

E-Series legacy command

Example 1 (static)

```
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 (snooping)

```
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 (show ip mroute)

```
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 37-91. show ip mroute Command Example Fields

Field	Description
(S,G)	Displays the forwarding entry in the multicast route table.
uptime	Displays the amount of time the entry has been in the multicast forwarding table.
Incoming interface	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
Outgoing interface list:	Lists the interfaces that meet one of the following: <ul style="list-style-type: none"> • a directly connected member of the Group • statically configured member of the Group • received a (*,G) or (S,G) Join message

show ip rpf

C **E** **S**

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

```

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 queue backplane multicast

E 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 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

E 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* 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.
[*source-address*]
* 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

E 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

E 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

E View IPv6 multicast routes.

Syntax 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.
 [*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 1

```
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 00:01:08
  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 2
(mroute active)**

```
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 3
(mroute count
group)**

```
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 4
(mroute count
source)**

```
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

E Display the Multicast MLD information.

Syntax show ipv6 mroute [mld [*group-address* | all | vlan *vlan-id*]]

Parameters

mld	(OPTIONAL) Enter the keyword <code>mld</code> to display Multicast MLD information.
<i>group-address</i>	(OPTIONAL) Enter the multicast group address in the <code>X:X:X:X</code> format. The <code>::</code> notation specifies successive hexadecimal fields of zero.
all	(OPTIONAL) Enter the keyword <code>all</code> to view all the MLD information.
vlan <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>vlan</code> followed by the VLAN ID to view MLD VLAN information.

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

E 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 Version 7.4.1.0 Introduced

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`
- `ipv6 nd suppress-ra`
- `ipv6 neighbor`
- `show ipv6 neighbors`

clear ipv6 neighbors

- E** 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	<i>ipv6-address</i>	Enter the IPv6 address of the neighbor in the X:X:X:X::X format to remove a specific IPv6 neighbor. The :: notation specifies successive hexadecimal fields of zero.
	interface <i>interface</i>	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: <ul style="list-style-type: none"> 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 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

- E** 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:

Thomson, S. and T. Narten, “IPv6 Address Autoconfiguration”, RFC 2462, December 1998.

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

E 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

C **E** **S** 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

- E** 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:

Thomson, S. and T. Narten, “IPv6 Address Autoconfiguration”, RFC 2462, December 1998.

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

- E** 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

<i>ipv6-address</i>	Enter the IPv6 address in the X:X:X::X format followed by the prefix length in the / x format.
<i>prefix-length</i>	Range: /0 to /128 The :: notation specifies successive hexadecimal fields of zeros
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

- E** 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 `seconds` Enter the lifetime value in seconds.
Range: 0 to 9000

Defaults 9000 seconds

Command Modes INTERFACE

ipv6 nd reachable-time

- E** 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 `milliseconds` Enter the reachability time in milliseconds.
Range: 0 to 3600000

Defaults 3600000 milliseconds

Command Modes INTERFACE

ipv6 nd suppress-ra

E 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.

Defaults Enabled

Command Modes INTERFACE

ipv6 neighbor

E Configure a static entry in the IPv6 neighbor discovery.

Syntax **ipv6 neighbor** { *ipv6-address* } { **interface** *interface* } { *hardware_address* }

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the **no ipv6 neighbor** { *ipv6-address* } { **interface** *interface* } command.

Parameters

ipv6-address

Enter the IPv6 address of the neighbor in the **x:x:x::x** format.

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 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

E Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the CP (control processor).

Syntax `show ipv6 neighbors [ipv6-address] [cpu {rp1 [ipv6-address] | rp2 [ipv6-address]}] [interface interface]`

- Parameters**
- ipv6-address** Enter the IPv6 address of the neighbor in the **x:x:x:x** format. 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 FTOS#show ipv6 neighbors

IPv6 Address	Expires(min)	Hardware Address	State	Interface	VLAN	CPU
fe80::201:e8ff:fe17:5bc6	1439	00:01:e8:17:5b:c6	STALE	Gi 1/9	-	CP
fe80::201:e8ff:fe17:5bc7	1439	00:01:e8:17:5b:c7	STALE	Gi 1/10	-	CP
fe80::201:e8ff:fe17:5bc8	1439	00:01:e8:17:5b:c8	STALE	Gi 1/11	-	CP
fe80::201:e8ff:fe17:5caf	0.3	00:01:e8:17:5c:af	REACH	Po 1	-	CP
fe80::201:e8ff:fe17:5cb0	1439	00:01:e8:17:5c:b0	STALE	Po 32	-	CP
fe80::201:e8ff:fe17:5cb1	1439	00:01:e8:17:5c:b1	STALE	Po 255	-	CP
fe80::201:e8ff:fe17:5cae	1439	00:01:e8:17:5c:ae	STALE	Gi 1/3	Vl 100	CP
fe80::201:e8ff:fe17:5cae	1439	00:01:e8:17:5c:ae	STALE	Gi 1/5	Vl 1000	CP
fe80::201:e8ff:fe17:5cae	1439	00:01:e8:17:5c:ae	STALE	Gi 1/7	Vl 2000	CP

FTOS#

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](#)
- [IPv6 Object Tracking Commands](#)

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

C **E** **S**

Enables debugging for tracked objects.

Syntax `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

Version 8.4.1.0 Introduced

Example

Command Example: **debug track**

```
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
```

delay

C **E** **S**

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

seconds 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.

Defaults 0 seconds

Command Modes

OBJECT TRACKING (*conf_track_object-id*)

Command History

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

text Enter a description to identify a tracked object (80 characters maximum).

Defaults

No default behavior or values

Command Modes

OBJECT TRACKING (conf_track_ *object-id*)

Command History

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.

show running-config track

C **E** **S** 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).
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 VRFs is displayed.

Command Modes EXEC Privilege

Command History

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.

Example 1

```
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

```

Table 39-92. Command Example Description: show track

show track Output	Description
Track <i>object-id</i>	Displays the number of the tracked object.
Interface <i>type slot/port</i> IP route <i>ip-address</i> IPv6 route <i>ipv6-address</i>	Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.
<i>object</i> is Up/Down	Up/Down state of tracked object; for example, IPv4 interface, reachability or metric threshold of an IP route.
<i>number</i> changes, last change <i>time</i>	Number of times that the state of the tracked object has changed and the time since the last change in <i>hours:minutes:seconds</i>
First hop interface	Displays the type and slot/port number of the first-hop interface of the tracked route.
Tracked by	Client that is tracking an object's state; for example, VRRP.

**Example 2
(brief)**

```
FTOS>show track brief
```

ResId	Resource	Parameter	State	LastChange
1	IP route reachability	10.16.0.0/16	Up	00:01:08
2	Interface line-protocol	Ethernet0/2	Down	00:05:00
3	Interface ip routing	VLAN100	Up	01:10:05

Table 39-93. Command Example Description: show track brief

show track Output	Description
ResID	Number of the tracked object
Resource	Type of tracked object
Parameter	Detailed description of the tracked object
State	Up or Down state of the tracked object
Last Change	Time since the last change in the state of the tracked object

threshold metric



Configure the metric threshold used to determine the UP and/or DOWN state of a tracked IPv4 or IPv6 route.

Syntax `threshold metric {up number | down number}`

To return to the default setting, enter `no threshold metric {up number | down number}`.

Parameters

object-id Enter the ID number of the tracked object. Range: 1 to 65535.

up number 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.

down number 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.

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

C **E** **S**

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

C **E** **S**

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.
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.
[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.

Usage Information

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.

track ip route reachability



Configure object tracking on the reachability of an IPv4 route.

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**.

Parameters

<i>object-id</i>	Enter the ID number of the tracked object. Range: 1 to 65535.
<i>ip-address/prefix-len</i>	Enter an IPv4 address in dotted decimal format. Valid IPv4 prefix lengths are from /0 to /32.
<i>vrf vrf-name</i>	(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.

Usage Information

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.

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 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 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](#)

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

C **E** **S** 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

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 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 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](#) 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.

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

C **E** **S** 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

<i>object-id</i>	Enter the ID number of the tracked object. Range: 1 to 65535.
isis <i>resolution-value</i>	Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
ospf <i>resolution-value</i>	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 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, FTOS 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

show running-config track	Display configuration information about tracked objects.
show track	Display information about tracked objects, including configuration, current state, and clients which track the object.
track interface ipv6 routing	Configure object tracking on the routing status of an IPv6 Layer 3 interface.
track ipv6 route metric threshold	Configure object tracking on the threshold of an IPv6 route metric.
track ipv6 route reachability	Configure object tracking on the reachability of an IPv6 route.

Example 1 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 39-94. Command Example Description: show track ipv6 route

show track ipv6 route Output	Description
Track <i>object-id</i>	Displays the number of the tracked object.
Interface <i>type slot/port</i> IP route <i>ip-address</i> IPv6 route <i>ipv6-address</i>	Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.
<i>object</i> is Up/Down	Up/Down state of tracked object; for example, IPv4 interface, reachability or metric threshold of an IP route.
<i>number</i> changes, last change <i>time</i>	Number of times that the state of the tracked object has changed and the time since the last change in <i>hours:minutes:seconds</i>
First hop interface	Displays the type and slot/port number of the first-hop interface of the tracked route.
Tracked by	Client that is tracking an object's state; for example, VRRP.

**Example 2
(brief)**

```

FTOS#show track ipv6 route brief

ResID  Resource                               Parameter                               State  LastChange
2      IPv6 route metric threshold 2040::/64                               Up     00:02:36
3      IPv6 route reachability   2050::/64                               Up     00:02:36

```

Table 39-95. Command Example Description: show track ipv6 route brief

show track ipv6 route brief Output	Description
ResID	Number of the tracked object
Resource	Type of tracked object
Parameter	Detailed description of the tracked object
State	Up or Down state of the tracked object
Last Change	Time since the last change in the state of the tracked object

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 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 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

C **E** **S** 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

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:X: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.

[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, 3333:100:200:300:400::/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:X: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, 3333:100:200:300:400::/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 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

<i>object-id</i>	Enter the ID number of the tracked object. Range: 1 to 65535.
isis <i>resolution-value</i>	Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
ospf <i>resolution-value</i>	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, FTOS 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   

Open Shortest Path First version 3 (OSPFv3) for IPv6 is supported on platforms  



Note: The C-Series supports OSPFv3 with FTOS 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: FTOS 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 Force10 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](#)
- [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](#)
- [show ip ospf database nssa-external](#)
- [show ip ospf database opaque-area](#)
- [show ip ospf database opaque-as](#)
- [show ip ospf database opaque-link](#)
- [show ip ospf database router](#)
- [show ip ospf database summary](#)
- [show ip ospf interface](#)
- [show ip ospf neighbor](#)
- [show ip ospf routes](#)
- [show ip ospf statistics](#)
- [show ip ospf topology](#)
- [show ip ospf virtual-links](#)
- [summary-address](#)
- [timers spf](#)

area default-cost



Set the metric for the summary default route generated by the area border router (ABR) into the stub area. Use this command on the border routers at the edge of a stub area.

Syntax `area area-id default-cost cost`

To return default values, use the **no area *area-id* default-cost** command.

Parameters

area-id Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.

cost Specifies the stub area's advertised external route metric.

Range: zero (0) to 65535.

Defaults

cost = 1; no areas are configured.

Command Modes

ROUTER OSPF

Command History

Version 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

In FTOS, *cost* is defined as reference bandwidth/bandwidth.

Related Commands

[area stub](#) Create a stub area.

area nssa

C **E** **S**

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

C **E** **S**

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
Version 7.5.1.0	Introduced on C-Series
pre-Version 6.1.1.1	Introduced on E-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

area stub	Create a stub area.
router ospf	Enter the ROUTER OSPF mode to configure an OSPF instance.

area stub

C **E** **S** 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

<i>area-id</i>	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

router ospf	Enter the ROUTER OSPF mode to configure an OSPF instance.
-----------------------------	---

area virtual-link

C **E** **S** Set a virtual link and its parameters.

Syntax **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*]

To delete a virtual link, use the **no area** *area-id* **virtual-link** *router-id* command.

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.

Parameters	<i>area-id</i>	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.
	<i>router-id</i>	Specify an ID (IP address in dotted decimal format) associated with a virtual link neighbor.
	authentication-key [<i>encryption-type</i>] <i>key</i> message-digest-key <i>keyid</i> md5 [<i>encryption-type</i>] <i>key</i>	(OPTIONAL) Choose between two authentication methods: <ul style="list-style-type: none"> Enter the keyword authentication-key to enable simple authentication followed by an alphanumeric string up to 8 characters long. Optionally, for the <i>encryption-type</i> variable, enter the number 7 before entering the <i>key</i> string to indicate that an encrypted password will follow. Enter the keyword message-digest-key followed by a number from 1 to 255 as the <i>keyid</i>. After the <i>keyid</i>, enter the keyword md5 followed by the <i>key</i>. The <i>key</i> is an alphanumeric string up to 16 characters long. Optionally, for the <i>encryption-type</i> variable, enter the number 7 before entering the <i>key</i> string to indicate that an encrypted password will follow.
	dead-interval <i>seconds</i>	(OPTIONAL) Enter the keyword dead-interval followed by a number as the number of <i>seconds</i> for the interval. Range: 1 to 8192. Default: 40 seconds.
	hello-interval <i>seconds</i>	(OPTIONAL) Enter the keyword hello-interval followed by the number of <i>seconds</i> for the interval. Range: 1 to 8192. Default: 10 seconds.
	retransmit-interval <i>seconds</i>	(OPTIONAL) Enter the keyword retransmit-interval followed by the number of <i>seconds</i> for the interval. Range: 1 to 8192. Default: 5 seconds.
	transmit-delay <i>seconds</i>	(OPTIONAL) Enter the keyword transmit-delay followed by the number of <i>seconds</i> for the interval. Range: 1 to 8192. Default: 1 second.
Defaults	dead-interval <i>seconds</i> = 40 seconds; hello-interval <i>seconds</i> = 10 seconds; retransmit-interval <i>seconds</i> = 5 seconds; transmit-delay <i>seconds</i> = 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 discontinuous areas.	
	You cannot enable both authentication options. Choose either the authentication-key or message-digest-key option.	

auto-cost

C **E** **S**

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

<i>ref-bw</i>	(OPTIONAL) Specify a reference bandwidth in megabits per second. Range: 1 to 4294967 Default: 100 megabits per second.
---------------	--

Defaults 100 megabits per second.

Command Modes ROUTER OSPF

Command History

Version 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

clear ip ospf

C **E** **S**

Clear all OSPF routing tables.

Syntax **clear ip ospf** *process-id* [**process**]

Parameters

<i>process-id</i>	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
process	(OPTIONAL) Enter the keyword process to reset the OSPF process.

Command Modes EXEC Privilege

Command History

Version 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

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 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.

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 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

debug ip ospf



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

Syntax `debug ip ospf process-id [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.

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

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

Example

```
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 40-96. Output Descriptions for debug ip ospf process-id packet

Field	Description
8:14	Displays the time stamp.
OSPF	Displays the OSPF process ID: instance ID.
v:	Displays the OSPF version. FTOS supports version 2 only.
t:	Displays the type of packet sent: <ul style="list-style-type: none"> • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
l:	Displays the packet length.
rid:	Displays the OSPF router ID.
aid:	Displays the Autonomous System ID.
chk:	Displays the OSPF checksum.
aut:	States if OSPF authentication is configured. One of the following is listed: <ul style="list-style-type: none"> • 0 - no authentication configured • 1 - simple authentication configured using the <code>ip ospf authentication-key</code> command) • 2 - MD5 authentication configured using the <code>ip ospf message-digest-key</code> command.
auk:	If the <code>ip ospf authentication-key</code> command is configured, this field displays the key used.
keyid:	If the <code>ip ospf message-digest-key</code> command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.
dst:	Displays the destination IP address.
netmask:	Displays the destination IP address mask.
pri:	Displays the OSPF priority

Table 40-96. Output Descriptions for debug ip ospf process-id packet

Field	Description
N, MC, E, T	Displays information available in the Options field of the HELLO packet: <ul style="list-style-type: none"> • N + (N-bit is set) • N - (N-bit is not set) • MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets) • MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets) • E + (router is able to accept AS External LSAs) • E - (router cannot accept AS External LSAs) • T + (router can support TOS) • T - (router cannot support TOS)
hi:	Displays the amount of time configured for the HELLO interval.
di:	Displays the amount of time configured for the DEAD interval.
dr:	Displays the IP address of the designated router.
bdr:	Displays the IP address of the Border Area Router.

default-information originate



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

Syntax `default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]`

To return to the default values, enter **no default-information originate**.

Parameters

always	(OPTIONAL) Enter the keyword always to specify that default route information must always be advertised.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword metric followed by a number to configure a metric value for the route. Range: 1 to 16777214
metric-type <i>type-value</i>	(OPTIONAL) Enter the keyword metric-type followed by an OSPF link state type of 1 or 2 for default routes. The values are: <ul style="list-style-type: none"> • 1 = Type 1 external route • 2 = Type 2 external route.
route-map <i>map-name</i>	(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

C **E** **S**

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

C **E** **S**

Add a description about the selected OSPF configuration.

Syntax **description** *description*

To remove the OSPF description, use the **no description** command.

Parameters *description* Enter a text string description to identify the OSPF configuration (80 characters maximum).

Defaults No default behavior or values

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 [show ip ospf asbr](#) Display VLAN configuration.

distance

C **E** **S**

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.

Parameters

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

Defaults

110

Command Modes

ROUTER OSPF

Command History

Version 7.8.1.0	Introduced support for Multi-Process OSPF. 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	Introduced on S-Series
Version 7.5.1.0	Introduced on C-Series
pre-Version 6.1.1.1	Introduced on E-Series

distance ospf

C **E** **S**

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

external dist3	(OPTIONAL) Enter the keyword external followed by a number to specify a distance for external type 5 and 7 routes. Range: 1 to 255 Default: 110.
inter-area dist2	(OPTIONAL) Enter the keyword inter-area followed by a number to specify a distance metric for routes between areas. Range: 1 to 255 Default: 110.
intra-area dist1	(OPTIONAL) Enter the keyword intra-area followed by a number to specify a distance metric for all routes within an area. Range: 1 to 255 Default: 110.

Defaults

external dist3 = 110; **inter-area dist2** = 110; **intra-area dist1** = 110.

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 specify a distance for routes learned from other routing domains, use the redistribute command.	

distribute-list in

C **E** **S** Apply a filter to incoming routing updates from OSPF to the routing table.

Syntax **distribute-list** *prefix-list-name* **in** [*interface*]

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

Parameters	<i>prefix-list-name</i>	Enter the name of a configured prefix list.
	<i>interface</i>	(OPTIONAL) Enter one of the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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 VLAN, enter the keyword vlan followed by a number from 1 to 4094.

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

distribute-list out

C **E** **S**

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

prefix-list-name Enter the name of a configured prefix list.

bgp (OPTIONAL) Enter the keyword **bgp** to specify that BGP routes are distributed.*

connected (OPTIONAL) Enter the keyword **connected** to specify that connected routes are distributed.

isis (OPTIONAL) Enter the keyword **isis** to specify that IS-IS routes are distributed.*

rip (OPTIONAL) Enter the keyword **rip** to specify that RIP routes are distributed.*

static (OPTIONAL) Enter the keyword **static** to specify that only manually configured routes are distributed.

* 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

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

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

C **E**

FTOS, 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

Version 7.5.1.0 Introduced on C-Series

pre-Version 6.1.1.1 Introduced on E-Series

fast-convergence

C **E** **S**

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

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

Defaults None.

Command Modes ROUTER OSPF

Command History

Version 7.8.1.0 Introduced on all platforms.

Usage Information

The higher this parameter is set, the faster OSPF converge takes place. Note that the faster the convergence, the more frequent the route calculations and updates. This will impact CPU utilization and may impact adjacency stability in larger topologies.

Generally, convergence level 1 meets most convergence requirements. Higher convergence levels should only be selected following consultation with Dell Force10 technical support.

flood-2328

C **E** **S**

Enable RFC-2328 flooding behavior.

Syntax **flood-2328**

To disable, use the **no flood-2328** command.

Defaults Disabled

Command Modes ROUTER OSPF

Command History

Version 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 and E-Series

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 (refer to Section 13 of the RFC). When multiple direct links connect two routers, the RFC-2328 flooding algorithm generates significant redundant information across all links.

By default, FTOS implements an enhanced flooding procedure that dynamically and intelligently determines when to optimize flooding. Whenever possible, the OSPF task attempts to reduce flooding overhead by selectively flooding on a subset of the interfaces between two routers.

When **flood-2328** is enabled, this command configures FTOS to flood LSAs on all interfaces.

graceful-restart grace-period

C **E** **S** 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

Command Modes ROUTER OSPF

Command History

Version 7.8.1.0	Introduced for S-Series Introduced support for Multi-Process OSPF.
Version 7.5.1.0	Introduced on C-Series
pre-Version 6.1.1.1	Introduced on E-Series

graceful-restart helper-reject

C **E** **S** 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

C **E** **S** 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
Version 7.5.1.0	Introduced on C-Series
pre-Version 6.1.1.1	Introduced on E-Series

graceful-restart role

C **E** **S** 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 is a helper only during graceful restart.
role restart-only	(OPTIONAL) Enter the keywords restart-only to specify the OSPF router is 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

C **E** **S**

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

<i>seconds</i>	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

C **E** **S**

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

<i>encryption-type</i>	(OPTIONAL) Enter 7 to encrypt the key.
<i>key</i>	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

<i>cost</i>	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

<i>seconds</i>	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

C **E** **S**

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

<i>seconds</i>	Enter the number of seconds 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

C **E** **S**

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

<i>keyid</i>	Enter a number as the key ID. Range: 1 to 255.
<i>key</i>	Enter a continuous character string as the password.

Defaults No MD5 authentication is 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 To change to a different key on the interface, enable the new key while the old key is still enabled. The FTOS will send two packets: the first packet authenticated with the old key, and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, you must delete the old key. Dell Force10 recommends keeping only one key per interface.



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

ip ospf mtu-ignore

C **E** **S** 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	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 network

C **E** **S** Set the network type for the interface.

Syntax **ip ospf network { broadcast | point-to-point }**

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

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

C **E** **S** Set the priority of the interface to determine the Designated Router for the OSPF network.

Syntax **ip ospf priority** *number*

To return to the default setting, enter **no ip ospf priority**.

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

C **E** **S** Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

Syntax **ip ospf retransmit-interval** *seconds*

To return to the default values, 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

C **E** **S** Set the estimated time elapsed to send a link state update packet on the interface.

Syntax **ip ospf transmit-delay** *seconds*

To return to the default value, enter **no ip ospf transmit-delay**.

Parameters

<i>seconds</i>	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

C **E** **S** 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

Version 8.4.1.0	Introduced for IPv6.
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

maximum-paths

C **E** **S**

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

<i>number</i>	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

C **E** **S**

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

<i>ip-address</i>	Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
<i>mask</i>	Enter a network mask in /prefix format. (/x)
<i>area-id</i>	Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range: 0 to 65535 IP address format: dotted decimal format A.B.C.D. Note: If the area ID is smaller than 65535, it 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.

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 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



Suppress both receiving and sending routing updates on an interface.

Syntax `passive-interface {default | interface}`

To enable both the receiving and sending routing, enter the **no passive-interface interface** command.

To return all OSPF interfaces (current and future) to active, enter the **no passive-interface default** command.

Parameters**default**

Enter the keyword **default** to make all OSPF interfaces (current and future) passive.

interface

Enter the following keywords and slot/port or number information:

- For a 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 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

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	Modified to include the default keyword.
pre-Version 6.1.1.1	Introduced on E-Series

Usage Information

Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in OSPF updates sent via other interfaces.

The default keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the **no passive-interface interface** command. The no form of this command is inserted into the configuration for individual interfaces when the **no passive-interface interface** command is issued while **passive-interface default** is configured.

This command behavior has changed as follows:

passive-interface interface

- The previous **no passive-interface interface** is removed from the running configuration.
- The ABR status for the router is updated.
- Save **passive-interface interface** into the running configuration.

passive-interface default

- All present and future OSPF interface are marked as *passive*.
- Any adjacency are explicitly terminated from all OSPF interfaces.
- All previous **passive-interface interface** commands are removed from the running configuration.
- All previous **no passive-interface interface** commands are removed from the running configuration.

no passive-interface interface

- Remove the interface from the passive list.
- The ABR status for the router is updated.
- If **passive-interface default** is specified, then save **no passive-interface interface** into the running configuration.

No passive-interface default

- Clear everything and revert to the default behavior.
- All previously marked passive interfaces are removed.
- May update ABR status.

redistribute



Redistribute information from another routing protocol throughout the OSPF process.

Syntax `redistribute { connected | rip | 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

connected	Enter the keyword connected to specify that information from active routes on interfaces is redistributed.
rip	Enter the keyword rip to specify that RIP routing information is redistributed.
static	Enter the keyword static to specify that information from static routes is redistributed.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword metric followed by a number. Range: 0 (zero) to 16777214.
metric-type <i>type-value</i>	(OPTIONAL) Enter the keyword metric-type followed by one of the following: <ul style="list-style-type: none">• 1 = OSPF External type 1• 2 = OSPF External type 2
route-map <i>map-name</i>	(OPTIONAL) Enter the keyword route-map followed by the name of the route map.
tag <i>tag-value</i>	(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 [default-information originate](#) Generate a default route into the OSPF routing domain.

redistribute bgp

C **E** **S**

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

Version 7.8.1.3	Introduced Route Map for BGP Redistribution to OSPF
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	Modified to include the default keyword.
pre-Version 6.1.1.1	Introduced on E-Series

redistribute isis

C **E** **S**

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.

level-1-2 (OPTIONAL) Enter the keyword **level-1-2** to redistribute both IS-IS Level-1 and Level-2 routes.

level-2 (OPTIONAL) Enter the keyword **level-2** to redistribute only IS-IS Level-2 routes.

metric *metric-value* (OPTIONAL) Enter the keyword **metric** followed by a number.
Range: 0 (zero) to 4294967295.

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

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 IS-IS is not supported on S-Series platforms.

router-id

C **E** **S** Use this command to configure a fixed router ID.

Syntax **router-id** *ip-address*

To remove the fixed router ID, use the **no router-id** *ip-address* command.

Parameters *ip-address* Enter the router ID in the IP address format

Defaults This command has no default behavior or values.

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

Example

```

FTOS(conf)#router ospf 100
FTOS(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/n]:
FTOS(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
FTOS(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/n]:
FTOS#

```

Usage Information

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If 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

C **E** **S**

Enter the ROUTER OSPF mode to configure an OSPF instance.

Syntax

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

```
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

C **E** **S**

Display the non-default values in the current OSPF configuration.

Syntax

show config

Command Modes

ROUTER OSPF

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 FTOS(conf-router_ospf)#show config
!
router ospf 3
 passive-interface FastEthernet 0/1
FTOS(conf-router_ospf)#

show ip ospf

C **E** **S**

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

Version 7.9.1.0	Introduced VRF
Version 7.9.1.0	Introduced VRF
Version 7.8.1.0	Introduced support of Multi-Process OSPF.
Version 7.8.1.0	Introduced <i>process-id</i> 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
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.

If you delete all the [network area](#) commands for Area 0, the [show ip ospf](#) command output will not list Area 0.

Example

```
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 boundaryrouter
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 40-97. Command Output Descriptions: show ip ospf *process-id*

Line Beginning with	Description
“Routing Process...”	Displays the OSPF process ID and the IP address associated with the process ID.
“Supports only...”	Displays the number of Type of Service (TOS) rouse supported.
“SPF schedule...”	Displays the delay and hold time configured for this process ID.
“Number of...”	Displays the number and type of areas configured for this process ID.

Related Commands

show ip ospf database	Displays information about the OSPF routes configured.
show ip ospf interface	Displays the OSPF interfaces configured.
show ip ospf neighbor	Displays the OSPF neighbors configured.
show ip ospf virtual-links	Displays the OSPF virtual links configured.

show ip ospf asbr



Display all ASBR routers visible to OSPF.

Syntax `show ip ospf process-id asbr`

Parameters

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

Defaults No default values or behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 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 FTOS#show ip ospf lasbr

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 example 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

C **E** **S** Display all LSA information. If OSPF is not enabled on the switch, no output is generated.

Syntax **show ip ospf process-id database [database-summary]**

Parameters

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

database-summary (OPTIONAL) Enter the keywords **database-summary** to the display the number of LSA types in each area and the total number of LSAs.

Command Modes

EXEC
EXEC Privilege

Command History

Version 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 FTOS>show ip ospf 1 database

```
OSPF Router with ID (11.1.2.1) (Process ID 1)
  Router (Area 0.0.0.0)
  Link ID          ADV Router      Age         Seq#           Checksum      Link count
  11.1.2.1         11.1.2.1       673        0x80000005    0x707e        2
  13.1.1.1         13.1.1.1       676        0x80000097    0x1035        2
  192.68.135.2     192.68.135.2   1419       0x80000294    0x9cbd        1

  Network (Area 0.0.0.0)
  Link ID          ADV Router      Age         Seq#           Checksum
  10.2.3.2         13.1.1.1       676        0x80000003    0x6592
  10.2.4.2         192.68.135.2   908        0x80000055    0x683e

  Type-5 AS External
  Link ID          ADV Router      Age         Seq#           Checksum      Tag
  0.0.0.0         192.68.135.2   908        0x80000052    0xeb83        100
  1.1.1.1         192.68.135.2   908        0x8000002a    0xbd27        0
  10.1.1.0        11.1.2.1       718        0x80000002    0x9012        0
```

```

10.1.2.0      11.1.2.1      718      0x80000002    0x851c      0
10.2.2.0      11.1.2.1      718      0x80000002    0x7927      0
10.2.3.0      11.1.2.1      718      0x80000002    0x6e31      0
10.2.4.0      13.1.1.1      1184     0x80000068    0x45db      0
11.1.1.0      11.1.2.1      718      0x80000002    0x831e      0
11.1.2.0      11.1.2.1      718      0x80000002    0x7828      0
12.1.2.0      192.68.135.2  1663     0x80000054    0xd8d6      0
13.1.1.0      13.1.1.1      1192     0x8000006b    0x2718      0
13.1.2.0      13.1.1.1      1184     0x8000006b    0x1c22      0
172.16.1.0    13.1.1.1      148      0x8000006d    0x533b      0
FTOS>

```

Table 40-98. Command Output Description: show ip ospf *process-id* database

Field	Description
Link ID	Identifies the router ID.
ADV Router	Identifies the advertising router's ID.
Age	Displays the link state age.
Seq#	Identifies the link state sequence number. This number enables you to identify old or duplicate link state advertisements.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Link count	Displays the number of interfaces for that router.

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
 FTOS#show ip ospf 100 database asbr-summary
 OSPF Router with ID (1.1.1.10) (Process ID 100)
 Summary Asbr (Area 0.0.0.0)
 LS age: 1437
 Options: (No TOS-capability, No DC, E)
 LS type: Summary Asbr
 Link State ID: 103.1.50.1
 Advertising Router: 1.1.1.10
 LS Seq Number: 0x8000000f
 Checksum: 0x8221
 Length: 28
 Network Mask: /0
 TOS: 0 Metric: 2

 LS age: 473
 Options: (No TOS-capability, No DC, E)
 LS type: Summary Asbr
 Link State ID: 104.1.50.1
 Advertising Router: 1.1.1.10
 LS Seq Number: 0x80000010
 Checksum: 0x4198
 Length: 28
 --More--

Table 40-99. Command Output Descriptions: show ip ospf database asbr-summary

Item	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> • 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.

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
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

```
FTOS#show ip ospf 1 database external

          OSPF Router with ID (20.20.20.5) (Process ID 1)

          Type-5 AS External

LS age: 612
Options: (No TOS-capability, No DC, E)
LS type: Type-5 AS External
Link State ID: 12.12.12.2
Advertising Router: 20.31.3.1
LS Seq Number: 0x80000007
Checksum: 0x4cde
Length: 36
Network Mask: /32
    Metrics Type: 2
    TOS: 0
    Metrics: 25
    Forward Address: 0.0.0.0
    External Route Tag: 43

LS age: 1868
Options: (No TOS-capability, DC)
LS type: Type-5 AS External
Link State ID: 24.216.12.0
Advertising Router: 20.20.20.8
```



```

LS Seq Number: 0x80000005
Checksum: 0xa00e
Length: 36
Network Mask: /24
  Metrics Type: 2
  TOS: 0
  Metrics: 1
  Forward Address: 0.0.0.0
  External Route Tag: 701

```

F TOS#

Table 40-100. Command Example Descriptions: show ip ospf process-id database external

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> • 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.
Metrics Type	Displays the external type.
TOS	Displays the TOS options. Option 0 is the only option.
Metrics	Displays the LSA metric.
Forward Address	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.
External Route Tag	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.

**Related
Commands**

[show ip ospf database](#)

Displays OSPF database information.

show ip ospf database network

C **E** **S** Display the network (type 2) LSA information.

Syntax `show ip ospf process-id database network [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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: <ul style="list-style-type: none"> 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 <i>ip-address</i>	(OPTIONAL) Enter the keywords adv-router <i>ip-address</i> 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 FTOS#show ip ospf 1 data network

```
OSPF Router with ID (20.20.20.5) (Process ID 1)
```

```
Network (Area 0.0.0.0)
```

```
LS age: 1372
Options: (No TOS-capability, DC, E)
LS type: Network
Link State ID: 202.10.10.2
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000006
Checksum: 0xa35
Length: 36
Network Mask: /24
  Attached Router: 20.20.20.8
  Attached Router: 20.20.20.9
  Attached Router: 20.20.20.7
```

```
Network (Area 0.0.0.1)
```

```
LS age: 252
Options: (TOS-capability, No DC, E)
LS type: Network
Link State ID: 192.10.10.2
Advertising Router: 192.10.10.2
```

```

LS Seq Number: 0x80000007
Checksum: 0x4309
Length: 36
Network Mask: /24
    Attached Router: 192.10.10.2
    Attached Router: 20.20.20.1
    Attached Router: 20.20.20.5
FTOS#

```

Table 40-101. Command Example Descriptions: show ip ospf process-id database network

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> 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.
Checksum	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Length	Displays the Fletcher checksum of an LSA's complete contents.
Network Mask	Displays the length in bytes of the LSA.
Attached Router	Identifies the IP address of routers attached to the network.

Related Commands

[show ip ospf database](#)

Displays OSPF database information.

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

C **E** **S** 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

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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: <ul style="list-style-type: none"> 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
<i>adv-router ip-address</i>	(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

```
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 40-102. Command Example Descriptions: show ip ospf *process-id* database opaque-area

Item	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> 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.
Opaque Type	Displays the Opaque type field (the first 8 bits of the Link State ID).
Opaque ID	Displays the Opaque type-specific ID (the remaining 24 bits of the Link State ID).

**Related
Commands**

[show ip ospf database](#)

Displays OSPF database information.

show ip ospf database opaque-as

C **E** **S**

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-link

C **E** **S**

Display the opaque-link (type 9) LSA information.

Syntax `show ip ospf process-id database opaque-link [link-state-id] [adv-router ip-address]`

Parameters

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

link-state-id (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs
- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router ip-address (OPTIONAL) Enter the keyword **adv-router** followed by the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

EXEC

EXEC Privilege

Command History

Version 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 router

C **E** **S** Display the router (type 1) LSA information.

Syntax `show ip ospf process-id database router [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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: <ul style="list-style-type: none">the network's IP address for Type 3 LSAs or Type 5 LSAsthe router's OSPF router ID for Type 1 LSAs or Type 4 LSAsthe default destination (0.0.0.0) for Type 5 LSAs
adv-router <i>ip-address</i>	(OPTIONAL) Enter the keywords adv-router <i>ip-address</i> 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

```
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 40-103. Command Example Descriptions: show ip ospf process-id database router

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> 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.

Table 40-103. Command Example Descriptions: show ip ospf process-id database router

Item	Description
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: (Link ID)	Identifies the type of network to which the router is connected. 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.

show ip ospf database summary

C **E** **S**

Display the network summary (type 3) LSA routing information.

Syntax**show ip ospf process-id database summary** [*link-state-id*] [**adv-router** *ip-address*]**Parameters***process-id*Enter the OSPF Process ID to show a specific process.
If no Process ID is entered, command applies only to the first OSPF process.*link-state-id*

(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs
- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router
ip-address(OPTIONAL) Enter the keywords **adv-router** *ip-address* to display only the LSA information about that router.**Command Modes**

EXEC

EXEC Privilege

Command History

Version 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 FTOS#show ip ospf 100 database summary

                OSPF Router with ID (1.1.1.10) (Process ID 100)

                Summary Network (Area 0.0.0.0)

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

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

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

FTOS#

```

Table 40-104. Command Example Descriptions: show ip ospf *process-id* database summary

Items	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> 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 40-104. Command Example Descriptions: show ip ospf *process-id* database summary

Items	Description
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.

**Related
Commands**

[show ip ospf database](#)

Displays OSPF database information.

show ip ospf interface



Display the OSPF interfaces configured. If OSPF is not enabled on the switch, no output is generated.

Syntax

show ip ospf *process-id* interface [*interface*]

Parameters

- process-id* Enter the OSPF Process ID to show a specific process.
If no Process ID is entered, command applies only to the first OSPF process.
- interface* (OPTIONAL) Enter the following keywords and slot/port or number information:
- For 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 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 the VLAN ID. The range is from 1 to 4094.

Command Modes

EXEC

EXEC Privilege

**Command
History**

- | | |
|---------------------|--|
| Version 7.8.1.0 | Introduced <i>process-id</i> 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 |
| 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 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 DROTHER, Priority 1
  Designated Router (ID) 192.168.253.5, Interface address 192.168.0.4
  Backup Designated Router (ID) 192.168.253.3, Interface address 192.168.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:08
  Neighbor Count is 3, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.253.5 (Designated Router)
  Adjacent with neighbor 192.168.253.3 (Backup Designated Router)

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

Table 40-105. Command Example Descriptions: show ip ospf *process-id* interface

Line beginning with	Description
GigabitEthernet...	This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.
Internet Address...	This line displays the IP address, network mask and area assigned to this interface.
Process ID...	This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.
Transmit Delay...	This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
Designated Router...	This line displays the ID of the Designated Router and its interface address.
Backup Designated...	This line displays the ID of the Backup Designated Router and its interface address.
Timer intervals...	This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
Hello due...	This line displays the amount time till the next Hello packet is sent out this interface.
Neighbor Count...	This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.

show ip ospf neighbor

C **E** **S** Display the OSPF neighbors configured.

Syntax `show ip ospf process-id neighbor`

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

Command Modes EXEC
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

```
FTOS#show ip ospf 34 neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface	Area
20.20.20.7	1	FULL/DR	00:00:32	182.10.10.3	Gi 0/0	0.0.0.2
192.10.10.2	1	FULL/DR	00:00:37	192.10.10.2	Gi 0/1	0.0.0.1
20.20.20.1	1	FULL/DROTHER	00:00:36	192.10.10.4	Gi 0/1	0.0.0.1

FTOS#

Table 40-106. Command Example Descriptions: show ip ospf process-id neighbor

Row Heading	Description
Neighbor ID	Displays the neighbor router ID.
Pri	Displays the priority assigned neighbor.
State	Displays the OSPF state of the neighbor.
Dead Time	Displays the expected time until FTOS declares the neighbor dead.
Address	Displays the IP address of the neighbor.
Interface	Displays the interface type slot/port information.
Area	Displays the neighbor's area (process ID).

show ip ospf routes



Display routes as calculated by OSPF and stored in OSPF RIB.

Syntax `show ip ospf process-id routes`

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

Defaults 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 is useful in isolating routing problems between OSPF and RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, then likely the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, type1 cost is not displayed.

Example FTOS#show ip ospf 100 route

Prefix	Cost	Nexthop	Interface	Area	Type
1.1.1.1	1	0.0.0.0	Lo 0	0	Intra-Area
3.3.3.3	2	13.0.0.3	Gi 0/47	1	Intra-Area
13.0.0.0	1	0.0.0.0	Gi 0/47	0	Intra-Area
150.150.150.0	2	13.0.0.3	Gi 0/47	-	External
172.30.1.0	2	13.0.0.3	Gi 0/47	1	Intra-Area

FTOS#

show ip ospf statistics



Display OSPF statistics.

Syntax `show ip ospf process-id statistics global | [interface name {neighbor router-id}]`

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

global Enter the keyword **global** to display the packet counts received on all running OSPF interfaces and packet counts received and transmitted by all OSPF neighbors.

interface name (OPTIONAL) Enter the keyword **interface** followed by one of the following interface keywords and slot/port or number information:

- For a 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 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.

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

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
Version 7.4.1.0 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

```
FTOS#show ip ospf 1 statistics global
```

```

  OSPF Packet Count
      Total      Error      Hello      DDiscr      LSReq      LSUpd      LSAck
RX      10         0         8         2         0         0         0
TX      10         0        10         0         0         0         0

  OSPF Global Queue Length
      TxQ-Len      RxQ-Len      Tx-Mark      Rx-Mark
Hello-Q           0         0         0         2
LSR-Q             0         0         0         0
Other-Q           0         0         0         0
Error packets (Only for RX)

Intf-Down          0  Non-Dr          0  Self-Org          0
Wrong-Len          0  Invl-d-Nbr       0  Nbr-State         0
Auth-Err           0  MD5-Err         0  Chksum            0
Version            0  AreaMis         0  Conf-Issues       0
No-Buffer          0  Seq-No          0  Socket             0
Q-Overflow         0  Unkown-Pkt      0

Error packets (Only for TX)

Socket Errors          0
FTOS#
```

Table 40-107. Command Example Descriptions: show ip ospf statistics *process-id* global

Row Heading	Description
Total	Displays the total number of packets received/transmitted by the OSPF process
Error	Displays the error count while receiving and transmitting packets by the OSPF process
Hello	Number of OSPF Hello packets
DDiscr	Number of database description packets
LSReq	Number of link state request packets
LSUpd	Number of link state update packets
LSAck	Number of link state acknowledgement packets
TxQ-Len	The transmission queue length
RxQ-Len	The reception queue length
Tx-Mark	The highest number mark in the transmission queue
Rx-Mark	The highest number mark in the reception queue
Hello-Q	The queue, for transmission or reception, for the hello packets
LSR-Q	The queue, for transmission or reception, for the link state request packets.
Other-Q	The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.

Table 40-108. Error Definitions: show ip ospf statistics *process-id* global

Error Type	Description
Intf_Down	Received packets on an interface that is either down or OSPF is not enabled.
Non-Dr	Received packets with a destination address of ALL_DRS even though SELF is not a designated router
Self-Org	Receive the self originated packet
Wrong_Len	The received packet length is different to what was indicated in the OSPF header
Invlid-Nbr	LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer
Nbr-State	LSA, LSR, and LSU are received from a neighbor with stats less than the loading state
Auth-Error	Simple authentication error
MD5-Error	MD5 error
Cksum-Err	Checksum Error
Version	Version mismatch
AreaMismatch	Area mismatch
Conf-Issue	The received hello packet has a different hello or dead interval than the configuration
No-Buffer	Buffer allocation failure
Seq-no	A sequence no errors occurred during the database exchange process
Socket	Socket Read/Write operation error
Q-overflow	Packet(s) dropped due to queue overflow
Unknown-Pkt	Received packet is not an OSPF packet

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 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   Invld-Nbr      0   Nbr-State      0
Auth-Error     0   MD5-Error     0   Cksum-Err      0
Version        0   AreaMismatch  0   Conf-Issue     0
SeqNo-Err      0   Unkown-Pkt    0

Neighbor ID 9.1.1.2

           Hello      DDiscr      LSReq      LSUpd      LSAck
RX         59         3           1          1          1
TX         62         2           1          0          0

    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

C E S 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.

Example FTOS#show ip ospf 1 topology

```
Router ID      Flags      Cost      Nexthop      Interface     Area
3.3.3.3       E/B/-/    1         20.0.0.3     Gi 13/1       0
1.1.1.1       E/-/-/    1         10.0.0.1     Gi 7/1        1
FTOS#
```

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 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 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
FTOS#
```

Table 40-109. Command Example Descriptions: show ip ospf process-id virtual-links

Items	Description
“Virtual Link...”	This line specifies the OSPF neighbor to which the virtual link was created and the link’s status.
“Run as...”	This line states the nature of the virtual link.
“Transit area...”	This line identifies the area through which the virtual link was created, the interface used, and the cost assigned to that link.
“Transmit Delay...”	This line displays the transmit delay assigned to the link and the State of the OSPF neighbor.
“Timer intervals...”	This line displays the timer values assigned to the virtual link. The timers are Hello is hello-interval, Dead is dead-interval, Wait is transmit-delay, and Retransmit is retransmit-interval.
“Hello due...”	This line displays the amount of time until the next Hello packet is expected from the neighbor router.
“Adjacency State...”	This line displays the adjacency state between neighbors.

summary-address

C **E** **S** 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

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. 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

<i>delay</i>	Enter a number as the delay. Range: 0 to 4294967295. Default: 5 seconds
<i>holdtime</i>	Enter a number as the hold time. Range: 0 to 4294967295. Default: 10 seconds.

Defaults *delay* = 5 seconds; *holdtime* = 10 seconds

Command Modes ROUTER OSPF

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

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 FTOS 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 Force10 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](#)
- [ipv6 ospf area](#)
- [ipv6 ospf authentication](#)
- [ipv6 ospf cost](#)
- [ipv6 ospf dead-interval](#)
- [ipv6 ospf encryption](#)
- [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

area <i>area-id</i>	Area for which OSPFv3 traffic is to be authenticated. For <i>area-id</i> , you can enter a number or an IPv6 prefix.
ipsec spi <i>number</i>	Security Policy index (SPI) value that identifies an IPsec security policy. Range: 256 to 4294967295.
MD5 SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
<i>key-encryption-type</i>	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<i>key</i>	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).

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

[ipv6 ospf authentication](#)
[show crypto ipsec policy](#)

Configure an IPsec authentication policy on an OSPFv3 interface.

Display the configuration of IPsec authentication policies.

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 <i>area-id</i>	Area for which OSPFv3 traffic is to be encrypted. For <i>area-id</i> , you can enter a number or an IPv6 prefix.
ipsec spi <i>number</i>	Security Policy index (SPI) value that identifies an IPsec security policy. Range: 256 to 4294967295.
esp <i>encryption-algorithm</i>	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.
<i>key-encryption-type</i>	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<i>key</i>	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.
<i>authentication-algorithm</i>	Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1 .
<i>key-encryption-type</i>	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<i>key</i>	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

[ipv6 ospf encryption](#)

Configure an IPsec encryption policy on an OSPFv3 interface.

[show crypto ipsec policy](#)

Display the configuration of IPsec encryption policies.

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 **debug 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 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

Command History

Version 7.8.1.0 Added support for C-Series

Version 7.4.1.0 Introduced


```

Example 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 V1 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 V1 1000



FTOS#

```

Table 40-110. debug ip ospf Output Fields

Field	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version.
Type:	Displays the type of packet sent: <ul style="list-style-type: none"> • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
Length:	Displays the packet length.
Router ID:	Displays the OSPF3 router ID.
Area ID:	Displays the Area ID.
Chksum:	Displays the OSPF3 checksum.

default-information originate

  Configure FTOS to generate a default external route into the OSPFv3 routing domain.

Syntax **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

Version 7.8.1.0	Added support for C-Series
Version 7.4.1.0	Introduced

Related Commands [redistribute](#) Redistribute routes from other routing protocols into OSPFv3.

ipv6 ospf area

C **E** 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

<i>process-id</i>	Enter the process identification number.
area <i>area-id</i>	Specify the OSPF area. Range: 0 to 65535

Defaults No default values or behavior

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced
-----------------	------------

ipv6 ospf authentication

E **T** 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

null	Causes an authentication policy configured for the area to not be inherited on the interface.
ipsec spi <i>number</i>	Security Policy index (SPI) value that identifies an IPsec security policy. Range: 256 to 4294967295.
MD5 SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).

	<i>key-encryption-type</i>	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
	<i>key</i>	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).
Default	Not configured.	
Command Modes	INTERFACE	
Command History	Version 8.4.2.0	Introduced
Usage Information	<p>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.</p> <p>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.</p> <p>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.</p>	
Related Commands	area authentication	Configure an IPsec authentication policy for an OSPFv3 area.
	show crypto ipsec policy	Display the configuration of IPsec authentication policies.
	show crypto ipsec sa ipv6	Display the security associations set up for OSPFv3 interfaces in authentication policies.

ipv6 ospf encryption

E **T** Configure an IPsec encryption policy for OSPFv3 packets on an IPv6 interface.

Syntax	ipv6 ospf encryption { null ipsec spi number esp encryption-algorithm [<i>key-encryption-type</i>] <i>key authentication-algorithm</i> [<i>key-encryption-type</i>] <i>key</i> }	
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).

<i>key</i>	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.
<i>authentication-algorithm</i>	Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1 .
<i>key-encryption-type</i>	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<i>key</i>	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).

Default Not configured.

Command Modes INTERFACE

Command History Version 8.4.2.0 Introduced

Usage Information 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.

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

C **E** Explicitly specify the cost of sending a packet on an inter.

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

Usage Information In general, the path cost is calculated as:

$$10^8 / \text{bandwidth}$$

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

C **E** Set the time interval since the last hello-packet was received from a router. After the time interval elapses, the neighboring routers declare the router down.

Syntax **ipv6 ospf dead-interval** *seconds*

To return to the default time interval, use the **no ipv6 ospf dead-interval** command.

Parameters

<i>seconds</i>	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 hello-interval

C **E** 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 *seconds* Enter a the time interval in seconds as the time between hello packets.
Range: 1 to 65535.
Default: 10 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 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

C **E** 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 *number* Enter a number as the priority.
Range: 0 to 255.
Default: 1

Defaults 1

Command Modes INTERFACE

Command History
Version 7.8.1.0 Added support for C-Series
Version 7.4.1.0 Introduced

Usage Information Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ipv6 router ospf

C **E** 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

C **E** 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 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.

Defaults Enabled, that is sending of routing updates are enabled by default

Command Modes ROUTER OSPFv3

Command History
Version 7.8.1.0 Added support for C-Series
Version 7.4.1.0 Introduced

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

bgp as number	Enter the keyword bgp followed by the autonomous system number. Range: 1 to 65535
connected	Enter the keyword connected to redistribute routes from physically connected interfaces.
static	Enter the keyword static redistribute manually configured routes.
metric metric-value	Enter the keyword metric followed by the metric value. Range: 0 to 16777214 Default: 20
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. If the route map is not configured, the default is deny (to drop all routes).
tag tag-value	(OPTIONAL) Enter the keyword tag to set the tag for routes redistributed into OSPFv3. Range: 0 to 4294967295 Default: 0

Default Not configured.

Command Modes ROUTER OSPFv3

Command History

Version 7.8.1.0	Added support for C-Series
Version 7.4.1.0	Introduced

Usage Information

To redistribute the default route (**x:x:x::x**), configure the [default-information originate](#) command.

Related Commands

[default-information originate](#) Configure default external route into OSPFv3

router-id



Designate a fixed 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	
Command History	Version 7.8.1.0	Added support for C-Series
	Version 7.4.1.0	Introduced
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

show crypto ipsec policy



Display the configuration of IPsec authentication and encryption policies.

Syntax `show crypto ipsec policy [name name]`

Parameters `name name` (OPTIONAL) Displays configuration details about a specified policy.

Defaults No default behavior or values

Command Modes EXEC
EXEC Privilege

Command History 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

```

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 : 123456789a123456789b123456789c123456789d12345678
Outbound ESP Cipher Key : 123456789a123456789b123456789c123456789d12345678
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       :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97e
Outbound AH Key      :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97e
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 :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97eb7c0c3080882
5fb5
Outbound ESP Auth Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97eb7c0c3080882
5fb5
Inbound ESP Cipher Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba10345a1039ba8f8a
Outbound ESP Cipher Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba10345a1039ba8f8a
Transform set        : esp-128-aes esp-sha1-hmac

```

Table 40-111. show crypto ipsec policy Command Fields

Field	Description
Policy name	Displays the name of an IPsec policy.
Policy refcount	Number of interfaces on the router that use the policy.
Inbound ESP SPI Outbound ESP SPI	The encapsulating security payload (ESP) security policy index (SPI) for inbound and outbound links.
Inbound ESP Auth Key Outbound ESP Auth Key	The ESP authentication key for inbound and outbound links.
Inbound ESP Cipher Key Outbound ESP Cipher Key	The ESP encryption key for inbound and outbound links.
Transform set	The set of security protocols and algorithms used in the policy.
Inbound AH SPI Outbound AH SPI	The authentication header (AH) security policy index (SPI) for inbound and outbound links.
Inbound AH Key Outbound AH Key	The AH key for inbound and outbound links.

show crypto ipsec sa ipv6

E **T** 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

```
FTOS#show crypto ipsec policy
FTOS#show crypto ipsec sa ipv6

Interface: TenGigabitEthernet 0/0
  Link Local address: fe80::201:e8ff:fe40:4d10
  IPSecv6 policy name: OSPFv3-1-500

  inbound ah sas
    spi : 500 (0x1f4)
    transform : ah-md5-hmac
    in use settings : {Transport, }
    replay detection support : N
    STATUS : ACTIVE

  outbound ah sas
    spi : 500 (0x1f4)
    transform : ah-md5-hmac
    in use settings : {Transport, }
    replay detection support : N
    STATUS : ACTIVE

  inbound esp sas

  outbound esp sas

Interface: TenGigabitEthernet 0/1
```

```

Link Local address: fe80::201:e8ff:fe40:4d11
IPSecv6 policy name: OSPFv3-1-600

inbound ah sas

outbound ah sas

inbound esp sas
spi : 600 (0x258)
transform : esp-des esp-shal-hmac
in use settings : {Transport, }
replay detection support : N
STATUS : ACTIVE

outbound esp sas
spi : 600 (0x258)
transform : esp-des esp-shal-hmac
in use settings : {Transport, }
replay detection support : N
STATUS : ACTIVE

```

Table 40-112. show crypto ipsec sa ipv6 Command Fields

Field	Description
Interface	IPv6 interface
Link local address	IPv6 address of interface
IPSecv6 policy name	Name of the IPsec security policy applied to the interface.
inbound/outbound ah	Authentication policy applied to inbound or outbound traffic.
inbound/outbound esp	Encryption policy applied to inbound or outbound traffic.
spi	Security policy index number used to identify the policy.
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (only transport mode is supported).
replay detection support	Y: An SA has enabled the replay detection feature. N: The replay detection feature is not enabled.
STATUS	ACTIVE: The authentication or encryption policy is enabled on the interface.

show ipv6 ospf database

C **E** Display the information related to an OSPFv3 database for a specified router including link-state advertisements (LSAs).

Syntax `show ipv6 ospf database [database-summary]`

Parameters **database-summary** (OPTIONAL) Enter the keywords **database-summary** to view just a summary of database LSA information.

Defaults No default behavior or values

Command Modes EXEC
EXEC Privilege

Command History
Version 7.8.1.0 Added support for C-Series
Version 7.4.1.0 Introduced

Example

```
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
Originate New LSAS                  50
Rx New LSAS                          22
Ext LSA Count                        0
Rte Max Eq Cost Paths               10

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

FTOS#

```

show ipv6 ospf interface

C **E** View OSPFv3 interface information.

Syntax `show ipv6 ospf [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 Range: 1-128
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 VLAN, enter the keyword **vlan** followed by a number from 1 to 4094

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.8.1.0 Added support for C-Series
Version 7.4.1.0 Introduced

Example

```

FTOS#show ipv6 ospf interface gigabitethernet 1/0
GigabitEthernet 1/0 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5
FTOS#

```

show ipv6 ospf neighbor

C **E** 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 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.

Defaults No default behavior or values

Command Modes EXEC
EXEC Privilege

Command History
Version 7.8.1.0 Added support for C-Series
Version 7.4.1.0 Introduced

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 FTOS 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

Related Commands

[ip redirect-list](#) Enable an IP Redirect List

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

show cam pbr	Display the content of the PBR CAM.
show ip redirect-list	Display the redirect-list configuration.

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 *redirect-list-name* Enter the name of a redirect list.

Defaults No default behavior or values

Command Modes CONFIGURATION

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 6.5.3.0	Introduced on the E-Series ExaScale

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

<i>ip-protocol-number</i>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
<i>protocol-type</i>	Enter one of the following keywords as the protocol type: <ul style="list-style-type: none">• icmp for Internet Control Message Protocol• ip for Any Internet Protocol• tcp for Transmission Control Protocol• udp for User Datagram Protocol
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	Enter a network mask in /prefix format (/x).
any	Enter the keyword any to specify that all traffic is subject to the filter.
host <i>ip-address</i>	Enter the keyword host followed by the IP address to specify a host IP address.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>bit</i>	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: <ul style="list-style-type: none">• ack = acknowledgement• fin = finish (no more data from the user)• psh = push function• rst = reset the connection• syn = synchronize sequence number• urg = urgent field
<i>operator</i>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: <ul style="list-style-type: none">• 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 <i>port</i> 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

redirect



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

<i>ip-address</i>	Enter the IP address of the forwarding router.
sonet slot/port	Enter the keyword sonet followed by the slot/port information.
<i>ip-protocol-number</i>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
<i>protocol-type</i>	Enter one of the following keywords as the protocol type: <ul style="list-style-type: none"> • icmp for Internet Control Message Protocol • ip for Any Internet Protocol • tcp for Transmission Control Protocol • udp for User Datagram Protocol
<i>bit</i>	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: <ul style="list-style-type: none"> • ack = acknowledgement • fin = finish (no more data from the user) • psh = push function • rst = reset the connection • syn = synchronize sequence number • urg = urgent field
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>operator</i>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operands: <ul style="list-style-type: none"> • 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 7.4.1.0	Added the bit variable for TCP protocols only
Version 6.5.3.0	Introduced on the E-Series ExaScale

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

<i>sequence-number</i>	Enter a number from 1 to 65535.
permit	Enter the keyword permit assign the sequence to the permit list.
redirect	Enter the keyword redirect to assign the sequence to the redirect list.
<i>ip-address</i>	Enter the IP address of the forwarding router.
sonet slot/port	Enter the keyword sonet followed by the slot/port information.
<i>ip-protocol-number</i>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
<i>protocol-type</i>	Enter one of the following keywords as the protocol type: <ul style="list-style-type: none">• icmp for Internet Control Message Protocol• ip for Any Internet Protocol• tcp for Transmission Control Protocol• udp for User Datagram Protocol
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	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.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>bit</i>	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: <ul style="list-style-type: none">• ack = acknowledgement• fin = finish (no more data from the user)• psh = push function• rst = reset the connection• syn = synchronize sequence number• urg = urgent field
<i>operator</i>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: <ul style="list-style-type: none">• 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 <i>port</i> 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	Added the bit variable and Permit and Redirect
Version 6.5.3.0	Introduced on the E-Series ExaScale

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.

linecard *slot-number* Enter the keyword **linecard** followed by 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 7.4.1.0 Introduced

Example

```
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 Index	Port	VlanID	Proto	Tcp Flag	Src Port	Dst Port	SrcIp	DstIp	Next-hop MAC	Egress Port

.
15230	_	10	TCP	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

[ip redirect-group](#) Apply a redirect group to an interface.

[show ip redirect-list](#) Display the redirect-list configuration.

[show cam-usage](#) Display the CAM usage on ACL, router, or switch.

show ip redirect-list

C **E** **S** 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 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**_X in FTOS 8.1.1.0. and later.

PIM-DM is supported on E-Series TeraScale **E**_T, C-Series **C**, and S-Series **S** platforms in FTOS 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](#)
- [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

C **E** **S** 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

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 8.1.1.0	Introduced on the E-Series ExaScale
Version 6.5.1.0	Introduced

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

[ip pim sparse-mode](#)

Configure sparse-mode

[show ip pim tib](#)

Display PIM tree information.

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****X** with FTOS 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`
- `show ip pim interface`
- `show ip pim neighbor`
- `show ip pim rp`
- `show ip pim snooping interface`

- [show ip pim snooping neighbor](#)
- [show ip pim snooping tib](#)
- [show ip pim summary](#)
- [show ip pim tib](#)
- [show running-config pim](#)

clear ip pim rp-mapping

C **E** **S** Used by the bootstrap router (BSR) to remove all or particular Rendezvous Point (RP) Advertisement.

Syntax clear ip pim rp-mapping *rp-address*

Parameters *rp-address* (OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D)

Command Modes EXEC Privilege

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on S-Series

clear ip pim tib

C **E** **S** Clear PIM tree information from the PIM database.

Syntax clear ip pim tib [*group*]

Parameters *group* (OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D)

Command Modes EXEC Privilege

Command History

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on S-Series

clear ip pim snooping tib

C **E** **S** 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

C **E** **S** 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

Command History Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.8.1.0 Introduced on S-Series

ip pim bsr-border

C **E** **S**

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Syntax ip pim bsr-border

To return to the default value, enter no ip pim bsr-border.

Defaults Disabled

Command Modes INTERFACE

Command History

Version 8.1.1.0

Introduced on E-Series ExaScale

Version 7.8.1.0

Introduced on C-Series on port-channels and S-Series.

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

C **E** **S**

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 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.

hash-mask-length

(OPTIONAL) Enter the hash mask length.

Range: zero (0) to 32

Default: 30

priority

(OPTIONAL) Enter the priority used in Bootstrap election process.

Range: zero (0) to 255

Default: zero (0)

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 7.8.1.0

Introduced on S-Series

Version 6.1.1.0

Added support for VLAN interface

ip pim dr-priority

C **E** **S** Change the Designated Router (DR) priority for the interface.

Syntax ip pim dr-priority *priority-value*

To remove the DR priority value assigned, use the no ip pim dr-priority command.

Parameters *priority-value* Enter a number. Preference is given to larger/higher number.
Range: 0 to 4294967294
Default: 1

Defaults 1

Command Modes INTERFACE

Command History
Version 8.1.1.0 Introduced on E-Series ExaScale
Version 7.8.1.0 Introduced on C-Series on port-channels and S-Series

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

E This feature permits configuration of Non-stop Forwarding (NSF 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.
restart-time	(OPTIONAL) Enter the keyword restart-time followed by the number of seconds estimated for the PIM speaker to restart. Range: 30 to 300 seconds Default: 180 seconds
stale-entry-time	(OPTIONAL) Enter the keyword stale-entry-time followed by the number of seconds for which entries are kept alive after restart. Range: 30 to 300 seconds Default: 60 seconds

Defaults as above

Command Modes CONFIGURATION

Command History
Version 8.2.1.0 Introduced on E-Series ExaScale. Added the **ipv6** option for E-Series.
Version 7.6.1.0 Introduced on E-Series

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

C **E** **S** 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

<i>ext-access-list</i>	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 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on C-Series on port-channels and S-Series
Version 7.7.1.0	Introduced on E-Series.

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 [ip access-list extended](#) Configure an access list based on IP addresses or protocols.

ip pim ingress-interface-map

C **E** **S** When the Dell Force10 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

<i>std-access-list</i>	Enter the name of a standard access list that permits the
------------------------	---

Defaults None

Command Modes	INTERFACE	
Command History	Version 8.4.1.0	Introduced
Example	<pre>FTOS(conf)# ip access-list standard map1 FTOS(config-std-nacl)# permit 224.0.0.1/24 FTOS(config-std-nacl)#exit FTOS(conf)#int gig 1/1 FTOS(config-if-gi-1/1)# ip pim ingress-interface-map map1</pre>	

ip pim neighbor-filter

C **E** **S** 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 *access-list* Enter the name of a standard access list. Maximum 16 characters.

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

Usage Information Do not enter this command before creating the access-list.

ip pim query-interval

C **E** **S** 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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on C-Series on port-channels and S-Series

ip pim register-filter

C **E** **S**

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

Version 7.8.1.0	Introduced on C-Series and S-Series
Version 7.6.1.0	Introduced

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

C **E** **S**

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

<i>address</i>	Enter the RP address in dotted decimal format (A.B.C.D).
<i>group-address group-address mask</i>	Enter the keyword group-address followed by a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.
<i>override</i>	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.

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 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.

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

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

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	<p>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.</p> <p>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.</p> <p>If enabled at the VLAN level, PIM-SM snooping requires that you also enter the no shutdown command to enable the interface.</p> <p>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.</p> <p>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.</p> <p>To display information about the operation of PIM-SM snooping on a switch, enter the show ip pim summary command.</p>	
Related Commands	show ip pim snooping tib	Display TIB information learned through PIM-SM snooping.

ip pim sparse-mode

C **E** **S** 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	Version 8.1.1.0	Introduced on E-Series ExaScale
	Version 7.8.1.0	Introduced on C-Series on port-channels and S-Series

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

C **E** **S** 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

<i>seconds</i>	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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced
Version 7.7.1.1	Introduced

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

C **E** 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

<i>value</i>	(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
-----------------	---------------------------------

Usage Information This is applicable to last hop routers on the shared tree towards the Rendezvous Point (RP).

no ip pim snooping dr-flood

E **X** Disable the flooding of multicast packets to the PIM designated router.

Syntax no ip pim snooping **dr-flood**

To re-enable the flooding of multicast packets to the PIM designated router, 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.

Related Commands

[ip pim snooping](#)

Enable PIM-SM snooping.

show ip pim bsr-router

C **E** **S** View information on the Bootstrap router.

Syntax show ip pim bsr-router

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

```
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



View information on the interfaces with IP PIM enabled.

Syntax show ip pim interface

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

```
E600-7-RPM0#show ip pim interface
Address          Interface Ver/  Nbr    Query  DR DR
                  Mode    Count Intvl  Prio
172.21.200.254  Gi 7/9  v2/S   0      30    1 172.21.200.254
172.60.1.2      Gi 7/11 v2/S   0      30    1 172.60.1.2
192.3.1.1       Gi 7/16 v2/S   1      30    1 192.3.1.1
192.4.1.1       Gi 13/5 v2/S   0      30    1 192.4.1.1
172.21.110.1    Gi 13/6 v2/S   0      30    1 172.21.110.1
172.21.203.1    Gi 13/7 v2/S   0      30    1 172.21.203.1
```

Table 43-113. show ip pim interface Command Example Fields

Field	Description
Address	Lists the IP addresses of the interfaces participating in PIM.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.
Ver/Mode	Displays the PIM version number and mode for each interface participating in PIM. <ul style="list-style-type: none">v2 = PIM version 2S = PIM Sparse mode
Nbr Count	Displays the number of PIM neighbors discovered over this interface.
Query Intvl	Displays the query interval for Router Query messages on that interface (configured with ip pim query-interval command).
DR Prio	Displays the Designated Router priority value configured on the interface (ip pim dr-priority command).
DR	Displays the IP address of the Designated Router for that interface.

show ip pim neighbor

C **E** **S** 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

```
FTOS#show ip pim neighbor
Neighbor          Interface      Uptime/Expires      Ver  DR
Address
127.87.3.4        Gi 7/16        09:44:58/00:01:24  v2   1 / S
FTOS#
```

Table 43-114. show ip pim neighbor Command Example Fields

Field	Description
Neighbor address	Displays the IP address of the PIM neighbor.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.
Uptime/expires	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).
Ver	Displays the PIM version number. <ul style="list-style-type: none"> v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. <ul style="list-style-type: none"> 1 = default Designated Router priority (use ip pim dr-priority) DR = Designated Router S = Sparse mode

show ip pim rp

C **E** **S** 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.
<i>group-address</i>	(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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on S-Series

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#
```

Example 3 (group-address)

```
FTOS#sh ip pim rp 229.1.2.1
Group          RP
229.1.2.1      165.87.20.4

FTOS#
```

show ip pim snooping interface

E **X** 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

```
FTOS#show ip pim snooping interface
Interface  Ver  Nbr  DR      DR
          Count  Prio
Vlan 2     v2   3    1      165.87.32.2
```

Table 43-115. show ip pim snooping interface Command Example Fields

Field	Description
Interface	Displays the VLAN interfaces with PIM-SM snooping enabled.
Ver/Mode	Displays the PIM version number for each VLAN interface with PIM-SM snooping enabled: <ul style="list-style-type: none"> v2 = PIM version 2 S = PIM Sparse mode
Nbr Count	Displays the number of neighbors learned through PIM-SM snooping on the interface.
DR Prio	Displays the Designated Router priority value configured on the interface (ip pim dr-priority command).
DR	Displays the IP address of the Designated Router for that interface.

show ip pim snooping neighbor

E **X** 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 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 43-116. show ip pim snooping neighbor Command Example Fields

Field	Description
Neighbor address	Displays the IP address of the neighbor learned through PIM-SM snooping.
Interface	Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.
Uptime/expires	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).
Ver	Displays the PIM version number. <ul style="list-style-type: none">v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. <ul style="list-style-type: none">1 = default Designated Router priority (use ip pim dr-priority)DR = Designated RouterS = Sparse mode

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 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 43-117. show ip pim snooping tib Command Example Fields

Field	Description
(S, G)	Displays the entry in the PIM multicast snooping database.
uptime	Displays the amount of time the entry has been in the PIM multicast route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: <ul style="list-style-type: none"> • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = FTOS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K = acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/source.
RPF neighbor	Displays the next hop from this interface towards the RP/source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: <ul style="list-style-type: none"> • a directly connect member of the Group. • statically configured member of the Group. • received a (*,G) Join message.

show ip pim summary

C **E** **S** 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

```
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 (*,G) 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

C **E** **S** 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

```
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 43-118. show ip pim tib Command Example Fields

Field	Description
(S, G)	Displays the entry in the multicast PIM database.
uptime	Displays the amount of time the entry has been in the PIM route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.

Table 43-118. show ip pim tib Command Example Fields (Continued)

Field	Description
flags	List the flags to define the entries: <ul style="list-style-type: none"> • D = PIM Dense Mode • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = FTOS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K = acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/source.
RPF neighbor	Displays the next hop from this interface towards the RP/source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: <ul style="list-style-type: none"> • a directly connect member of the Group. • statically configured member of the Group. • received a (*,G) Join message.

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

E 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:X:X::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

E 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

bsr (OPTIONAL) Enter the keyword **bsr** to invoke debugging of IPv6 PIM Candidate RP/BSR activities.

events (OPTIONAL) Enter the keyword **events** to invoke debugging of IPv6 PIM events.

group *group* (OPTIONAL) Enter the keyword **group** followed by the group address to invoke debugging on that specific group.

packet (OPTIONAL) Enter the keyword **packet** to invoke debugging of IPv6 PIM packets.

register [*group*] (OPTIONAL) Enter the keyword **register** and optionally the group address to invoke debugging of IPv6 PIM register messages for a particular group.

state (OPTIONAL) Enter the keyword **state** to view IPv6 PIM state changes.

timer [assert | hello | joinprune | register] (OPTIONAL) Enter the keyword **timer** to view IPv6 PIM timers. Enter one of the optional parameters:

- assert: to view the assertion timer.
- hello: to view the IPv6 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

Command History Version 7.4.1.0 Introduced

ipv6 pim bsr-border

E Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Syntax `ipv6 pim bsr-border`

Defaults Disabled

Command Modes INTERFACE

Command History Version 8.3.1.0 Introduced

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

E 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.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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 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.
<i>hash-mask-length</i>	(OPTIONAL) Enter the hash mask length for RP selection. Range: 0 to 128 Default: 126
<i>priority</i>	(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

E 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

<i>priority-value</i>	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

- E** 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

<code>access-list</code>	Enter the name of an extended access list.
<code>in</code>	Enter this keyword to apply the access list to inbound traffic.
<code>out</code>	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

- E** 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

<code>seconds</code>	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

E 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.

Defaults None

Command Modes CONFIGURATION

Command History Version 8.3.1.0 Introduced

Usage Information Do not enter this command before creating the access-list.

ipv6 pim register-filter

E 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

E 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*

To remove an RP address, use the **no ipv6 pim re-address** *address group-address mask override*.

Parameters *address* Enter the IPv6 RP address in the X:X:X:X format.
The :: notation specifies successive hexadecimal fields of zero.

group-address Enter the keyword **group-address** followed by the group address in the X:X:X::X format and then the mask in /nn format to assign that group address to the RP. The :: notation specifies successive hexadecimal fields of zero.

group-address mask

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.

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History Version 7.4.1.0 Introduced

Usage Information The RP addresses are stored in the order in which they are entered. RP addresses learnt 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.

ipv6 pim rp-candidate

E Specify an interface as an RP candidate.

Syntax **ipv6 pim rp-candidate** *interface* [*priority-value*]

Parameters

interface Enter the following keywords and slot/port or number information:

- For a 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 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.

priority-value (OPTIONAL) Enter a number as the priority of this RP Candidate, which is included in the Candidate-RP-Advertisements.
Range: 0 (highest) to 255 (lowest)

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History Version 7.4.1.0 Introduced

ipv6 pim sparse-mode

E 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

E 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

kbps Enter a traffic rate in kilobytes per second.
Range: 0 to 4294967 kbps
Default: 10 kbps

infinity Enter the keyword **infinity** to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).

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

E 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

```
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

E Display IPv6 PIM enabled interfaces.

Syntax **show ipv6 pim interface**

Command Modes EXEC
EXEC Privilege

Command History Version 7.4.1.0 Introduced

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

E Displays IPv6 PIM neighbor information.

Syntax **show ipv6 pim neighbor [detail]**

Parameters **detail** (OPTIONAL) Enter the keyword **detail** to displayed PIM neighbor detailed information.

Command Modes EXEC
EXEC Privilege

Command History Version 7.4.1.0 Introduced

Example

```
FTOS#show ipv6 pim neighbor detail
Neighbor                Interface    Uptime/Expires    Ver  DR
Address
fe80::201:e8ff:fe00:6265 Gi 10/3        00:07:39/00:01:42 v2   1 / S
165:87:50::6
FTOS#
```

show ipv6 pim rp

E View all IPv6 multicast groups-to-rendezvous point (RP) mappings.

Syntax `show ipv6 pim rp [mapping | group-address]`

Parameters

mapping (OPTIONAL) Enter the keyword **mapping** to display the multicast groups-to-RP mapping and information on how RP is learnt.

group-address (OPTIONAL) Enter the multicast group address in the X:X:X::X format to view RP mappings for a specific group.

The :: notation specifies successive hexadecimal fields of zero.

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.4.1.0 Introduced

Example 1 (pim rp)

```
FTOS#show ipv6 pim rp
Group                RP
ff0e::225:1:2:1     14::1
ff0e::225:1:2:2     14::1
ff0e::226:1:2:1     14::1
ff0e::226:1:2:2     14::1
FTOS#
```

Example 2 (pim rp mapping)

```
FTOS#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 14::1, v2
  Info source: 14::1, via bootstrap, priority 192
  Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
  RP: 14::2, v2
FTOS#
```


show ipv6 pim tib

E 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 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 — **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****X** with FTOS 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

C **E** **S** 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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on S-Series
Version 7.7.1.0	Introduced on C-Series.
Version 7.5.1.0	Introduced on E-Series.

Usage Information FTOS 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.

FTOS 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, FTOS 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

C **E** **S** 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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.8.1.0	Introduced on S-Series
Version 7.7.1.0	Introduced on C-Series.
Version 7.5.1.0	Introduced on E-Series.

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

E 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 Version 7.5.1.0 Introduced

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, FTOS supports SSM for configured group range as well as default SSM range.

show ipv6 pim ssm-range

E 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)

Overview

FTOS supports Power over Ethernet (PoE), as described by IEEE 802.3af, on C-Series and S-Series systems (S25V and S50V models), as indicated by the **C** and **S** characters, respectively, that appear below each command heading.

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

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 Force10, and it is attached to the Current Sharing terminal, you can 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 `[no] power budget stack-unit 0-7 321-790`

Enter **no power budget stack-unit 0-7** to disable the use of power for PoE from the external power supply on the designated stack member.

Parameters

<code>0-7</code>	Enter the stack unit ID, from 0 to 7, of the stack member that you want to configure.
<code>321-790</code>	After entering the stack unit number, enter a value representing the watts to be used for PoE. Range: 321 to 790

Defaults 320W (i.e., redundancy mode)

Command Modes CONFIGURATION

Command History

Version 7.7.1.0	Introduced on S-Series
-----------------	------------------------

Usage Information Setting a value above 320 causes a warning to be displayed that 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, 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 15.4 watts).

max_milliwatts (OPTIONAL) Enter the number of milliwatts to be the maximum amount of power that a port can provide.
Range: 5000 to 15400 (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 15.4 watts).

Defaults no (power is disabled to the port)

Command Modes INTERFACE

Command History

Version 7.7.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on 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.

FTOS treats powered devices rated as Class 0, 3, or 4 the same.

Related Commands

[power inline priority](#) Set the PoE 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 PoE priority of the selected port.

Syntax [no] **power inline priority** {**critical** | **high** | **low**}

Parameters

critical Enter the keyword **critical** to set the PoE priority of the port to the highest level.

high Enter the keyword **high** to set the PoE priority of the port to the second highest level.

low Enter the keyword **low** to set the PoE priority of the port to the lowest level.

Defaults none

Command Modes INTERFACE

Command History

Version 7.7.1.0 Introduced on 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:

$$\text{PoE_off_priority} = \text{static_or_auto_prio} * 10000 + (\text{user/LLDP-MED}) \text{ priority} * 1000 + \text{slotId} * 100 + \text{portId}$$

where:

- static_prio = 0
- auto_prio = 1

The lower the value of PoE_off_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 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 “PoE_off_priority” for the port increases and hence a lower priority.

Basically, 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 TLV, only if user priority is not configured (refer to [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 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 output.
Version 7.7.1.0 Introduced on S-Series
Version 4.2.1.0 Introduced on C-Series

Example

```
FTOS(conf-if-range-gi-0/1-48)#do show power detail
```

Unit	Total Power Available (Watts)	Logic Power Consumed (Watts)	Inline Power Available (Watts)	Inline Power Allocated (Watts)	Inline Power Consumed (Watts)	Inline Power Remaining (Watts)
0	470.00	150	320.00	308.00	190.00	12.00

Table 45-119. show power detail Command Output Fields

Unit	(S-Series only) The stack member unit ID.
Catalog Name	(C-Series only) Displays the component's Dell Force10 catalog number.
Slot ID	(C-Series only) Displays the slot number in which the line card or RPM is installed.
Total Power Available	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.
Logic Power Consumed	The power consumed by the system logic.
Inline Power Available	Power available for PoE (whatever was configured using power-budget command. Default: 320 watts
Inline Power Allocated	Total power allocated to the ports.
Inline Power Consumed	Total power consumed by connected devices.
Inline Power Remaining	Difference between power available and power allocated.

Related Commands

power inline	Enable power to be supplied to a device connected to a port.
power inline priority	Set the PoE 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.

Syntax

show power inline

Command Modes

EXEC
EXEC Privilege

Command History

Version 8.4.1.0	Operational Status removed from output.
Version 7.7.1.0	Introduced on S-Series
Version 7.5.1.0	Introduced on C-Series

Example

```
FTOS(conf-if-range-gi-0/1-48)#do show power inline
Interface   Admin   Inline Power   Inline Power   Class   User
           Admin   Allocated      Consumed       Class   Priority
           (Watts) (Watts)
-----
Gi 0/1      auto    0.00           0.00           NO_DEVICE Low
Gi 0/2      auto    7.00           3.20           2       Low
```



Table 45-120. show power inline Command Output Field Description

Interface	Displays the line card slot and port number.
Admin	Displays the PoE mode of the port. The mode can be either <i>auto</i> or <i>static</i> . Refer to 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.
Class	Displays the power classification of the connected device. Valid classes are 0-4.
User Priority	Displays the power configured by the user for the port (default is low). Refer to power inline priority .

Related Commands

power inline	Enable power to be supplied to a device connected to a port.
power inline priority	Set the PoE priority of the selected port

show power supply

  Display the power supply status.

Syntax `show power supply`

Command Modes EXEC
EXEC Privilege

Command History
Version 7.7.1.0 Introduced on S-Series
Version 7.5.1.0 Introduced on C-Series

C-Series Example

```
FTOS#show power supply
Power      Model
Supply    Number          Type    Status
-----
PEM0
PEM1
PEM2      CC-C-1200W-AC    AC      Active
PEM3
PEM4      CC-C-1200W-AC    AC      Powered Off
PEM5      CC-C-1200W-AC    AC      Active
FTOS#
```

[Table 45-122, "Power Supply Conditions," in Power over Ethernet \(PoE\)](#) describes the nine possible power supply conditions.

Table 45-121. Power Supply Conditions

AC Fail	The PSU is unplugged.
Active	The PSU is supplying power to the chassis.
Fail	The PSU has failed.
Not Present	The PSU is not installed in the chassis.
Over Current Shutdown	The PSU has turned off due to an high input current condition.
Over Temperature Shutdown	The PSU has turned off due to an high temperature condition.
Over Temperature Warning	The temperature of the PSU is greater than the recommended maximum operating temperature.
Over Current Warning	The current being supplied to the PSU is greater than the recommended maximum input current.
Power Off	The PSU is present but not on.

S-Series 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
2         PS0        S50-PWR-AC     AC      Active
2         PS1
FTOS
```

Table 45-122, "Power Supply Conditions," in *Power over Ethernet (PoE)* describes the nine possible power supply conditions.

Table 45-122. Power Supply Conditions

AC Fail	The PSU is unplugged.
Active	The PSU is supplying power to the chassis.
Fail	The PSU has failed.
Not Present	The PSU is not installed in the chassis.
Over Current Shutdown	The PSU has turned off due to an high input current condition.
Over Temperature Shutdown	The PSU has turned off due to an high temperature condition.
Over Temperature Warning	The temperature of the PSU is greater than the recommended maximum operating temperature.
Over Current Warning	The current being supplied to the PSU is greater than the recommended maximum input current.
Power Off	The PSU is present but not on.

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 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](#)
- [monitor session](#)
- [show config](#)
- [show monitor session](#)
- [show running-config monitor session](#)
- [source \(port monitoring\)](#)

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; VLAN and port-channel interfaces do not support port monitoring.
- A SONET port may only be a monitored port.
- FTOS 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 Monitored (source, “MD”) and Monitoring ports (destination, “MG”) must be on the same switch.
- In general, a monitoring port should have no ip address and no shutdown as the only configuration. FTOS permits a limited set of commands for monitoring ports; display them using the command ?. A monitoring port also may not be a member of a VLAN.
- There may only be one destination port in a monitoring session.
- A source port (MD) can only be monitored by one destination port (MG).
- On the E-Series TeraScale, only one MG and one MD may be in a single port-pipe.
- The C-Series and S-Series may only have four destination ports per port-pipe. There is no limitation on the total number of monitoring sessions.
- A monitoring port can monitor any physical port in the chassis.
- A monitoring port can monitor more than one port.
- More than one monitored port can have the same destination monitoring port.
- FTOS 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.

description

C **E** **S**

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

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
pre-7.7.1.0	Introduced on E-Series

Related Commands

[monitor session](#) Enable a monitoring session.

flow-based enable

E

Enable flow-based monitoring.

Syntax

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

Version 8.1.1.0	Introduced on E-Series ExaScale
Version 7.4.1.0	Introduced on E-Series

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

[monitor session](#) Create a monitoring session.

monitor session

C **E** **S** Create a session for monitoring traffic for port monitoring.

Syntax monitor session *session-ID*

To delete a session, use the `no monitor session session-ID` command.

To delete all monitor sessions, use the `no monitor session` command.

Parameters *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 8.1.1.0	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)# monitor session 60
FTOS(conf-mon-sess-60)
```

Usage Information All monitor sessions contain an implicit “mode interface,” that is, if no mode is designated, the mode is set to interface as shown in the example above.

Only one monitor session per Port-Pipe is allowed.

The `monitor` command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Related Commands

show monitor session	Display the monitor session
show running-config monitor session	Display the running configuration of a monitor session

show config

C **E** **S** 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

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

C **E** **S** Display the monitor information of a particular session or all sessions.

Syntax show monitor session {*session-ID*}

To display the monitor 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

```
FTOS#show monitor session 11
SessionID      Source      Destination  Direction  Mode
-----
      11        Gi 10/0     Gi 10/47    rx         interface
FTOS#
```

Related Commands

[monitor session](#) Create a session for monitoring.

show running-config monitor session

C **E** **S** 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)

C **E** **S** 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 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 8.1.1.0 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

```
F'TOS(conf-mon-sess-11)#source gi 10/0 destination gi 10/47 direction rx
F'TOS(conf-mon-sess-11)#
```

Usage Information



Note: A SONET port can only be configured as a monitored port.

Private VLAN (PVLAN)

Overview

Starting with FTOS 7.8.1.0, the Private VLAN (PVLAN) feature of FTOS 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](#)

Refer also to the following commands. The command output is augmented in FTOS 7.8.1.0 to provide PVLAN data:

- [show arp](#) in [Chapter 26, IPv4 Routing](#)
- [show vlan](#) in [Chapter 32, Layer 2](#)

Private VLANs extend the FTOS security suite by providing Layer 2 isolation between ports within the same private VLAN. A private VLAN partitions a traditional VLAN into subdomains identified by a *primary* and *secondary VLAN* pair.

The FTOS private VLAN implementation is based on RFC 3069.

Private VLAN Concepts

Primary VLAN:

The *primary VLAN* is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — *community VLAN* and *isolated VLAN*:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

Community VLAN:

A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all *promiscuous ports* in the primary VLAN and vice-versa.
- Devices on a community VLAN can communicate with each other via member ports, while devices in an isolated VLAN cannot.

Isolated VLAN:



An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice-versa.

Port types:

- **Community port:** A *community port* is, by definition, a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.
- **Isolated port:** An *isolated port* is, by definition, a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- **Promiscuous port:** A *promiscuous port* is, by definition, a port that is allowed to communicate with any other port type.
- **Trunk port:** A *trunk port*, by definition, carries VLAN traffic across switches:
- A trunk port in a PVLAN is always tagged.
- Primary or secondary VLAN traffic is carried by the trunk port in tagged mode. The tag on the packet helps identify the VLAN to which the packet belongs.
- A trunk port can also belong to a regular VLAN (non-private VLAN).

ip local-proxy-arp

  Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

Syntax [no] **ip local-proxy-arp**

To disable Layer 3 communication between secondary VLANs in a private VLAN, use the **no ip local-proxy-arp** command in 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

Command History Version 7.8.1.0 Introduced on C-Series and S-Series

Related Commands

private-vlan mode	Set the mode of the selected VLAN to community, isolated, or primary.
private-vlan mapping secondary-vlan	Map secondary VLANs to the selected primary VLAN.
show arp	Display the ARP table.
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.
switchport mode private-vlan	Set the PVLAN mode of the selected port.

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

Command History

Version 7.8.1.0	Introduced on C-Series and S-Series
-----------------	-------------------------------------

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.
show vlan private-vlan mapping	Display primary-secondary VLAN mapping.
switchport mode private-vlan	Set the PVLAN mode of the selected port.

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 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.

Defaults none

Command Modes EXEC

EXEC Privilege

Command History Version 7.8.1.0 Introduced on C-Series and S-Series

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

```
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 47-123. show interfaces description Command Example Fields

Field	Description
Interface	Displays type of interface and associated slot and port number
Vlan	Displays the VLAN ID of the designated interface
PVLAN-Type	Displays the type of VLAN in which the designated interface resides
Interface Type	Displays the PVLAN port type of the designated interface.
Status	States whether the interface is operationally up or down.

Related Commands

- [private-vlan mode](#) Set the mode of the selected VLAN to community, isolated, or primary.
- [show vlan private-vlan](#) Display 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 vlan private-vlan

  Display PVLANS and/or interfaces that are part of a PVLAN.

Syntax `show vlan private-vlan [community | interface | isolated | primary | primary_vlan | interface interface]`

Parameters

- community** (OPTIONAL) Enter the keyword **community** to display VLANs configured as community VLANs, along with their interfaces.
- interface** (OPTIONAL) Enter the keyword **community** to display VLANs configured as community VLANs, along with their interfaces.
- isolated** (OPTIONAL) Enter the keyword **isolated** to display VLANs configured as isolated VLANs, along with their interfaces.
- primary** (OPTIONAL) Enter the keyword **primary** to display VLANs configured as primary VLANs, along with their interfaces.
- primary_vlan** (OPTIONAL) Enter a private VLAN ID or secondary VLAN ID to display interface details about the designated PVLAN.
- interface interface** (OPTIONAL) Enter the keyword **interface** and an interface ID to display the PVLAN configuration of the designated interface.

Defaults None

Command Modes EXEC

EXEC Privilege

Command History Version 7.8.1.0 Introduced on C-Series and S-Series

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

```
FTOS# show vlan private-vlan
Primary Secondary Type      Active Ports
-----
10          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 [Example 2 \(primary\)](#). If the VLAN ID is a secondary VLAN, only its primary VLAN and its particular secondary VLAN properties will be displayed, as shown in [Example 3 \(secondary\)](#).

Example 2 (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

```

Example 3 (secondary)

```

FTOS#show vlan private-vlan 102
Primary Secondary Type      Active Ports
-----
10              Primary Yes    Po 1
              Gi 0/2
              102    Isolated Yes    Gi 0/4

```

The table, below, defines the fields in the output, above.



Table 47-124. show interfaces description Command Example Fields

Field	Description
Primary	Displays the VLAN ID of the designated or associated primary VLAN(s)
Secondary	Displays the VLAN ID of the designated or associated secondary VLAN(s)
Type	Displays the type of VLAN in which the listed interfaces reside
Active	States whether the interface is operationally up or down
Ports	Displays the interface IDs in the listed VLAN.

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

Usage Information The output of this command, shown below, displays the community and isolated VLAN IDs that are associated with each primary VLAN.

Example

```

FTOS# show vlan private-vlan mapping
Private Vlan:
  Primary   : 100
  Isolated  : 102
  Community : 101
  Unknown   : 200

```

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.

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

```
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

[private-vlan mode](#) Set the mode of the selected VLAN to either community or isolated.

[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 mapping](#) Display primary-secondary VLAN mapping.

Per-VLAN Spanning Tree plus (PVST+)

Overview

The FTOS implementation of PVST+ (Per-VLAN Spanning Tree plus) is based on the IEEE 802.1d standard Spanning Tree Protocol, but it creates a separate spanning tree for each VLAN configured.

PVST+ (Per-VLAN Spanning Tree plus) is supported by FTOS on all Dell Force10 systems, as indicated by the characters that appear below each command heading:

- C-Series: **C**
- E-Series: **E**
- S-Series: **S**

Commands

The FTOS 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

C **E** **S**

Disable PVST+ globally.

Syntax **disable**

To enable PVST+, enter **no disable**.

Defaults PVST+ is disabled

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
pre-Version 6.2.1.1	Introduced on E-Series

Related Commands

[protocol spanning-tree pvst](#) Enter PVST+ mode.

description

C **E** **S**

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

pre-7.7.1.0	Introduced
-------------	------------

Related Commands

[protocol spanning-tree pvst](#) Enter SPANNING TREE mode on the switch.

extend system-id

C **E** **S**

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

Version 8.3.1.0 Introduced

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
  Name        PortID    Prio Cost    Sts Cost        Designated
  -----
  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

C **E** **S** Enter the PVST+ mode to enable PVST+ on a device.

Syntax **protocol spanning-tree pvst**

To disable PVST+, use the [disable](#) command.

Defaults This command has no default value or behavior.

Command Modes CONFIGURATION

Command History

Version 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

Example

```
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

[disable](#)

Disable PVST+.

[show spanning-tree pvst](#)

Display the PVST+ configuration.

show spanning-tree pvst

C **E** **S**

View the Per-VLAN Spanning Tree configuration.

Syntax

show spanning-tree pvst [**vlan** *vlan-id*] [**brief**] [**guard**]

Parameters

vlan *vlan-id*

(OPTIONAL) Enter the keyword **vlan** followed by the VLAN ID.

Range: 1 to 4094

brief

(OPTIONAL) Enter the keyword **brief** to view a synopsis of the PVST+ configuration information.

Interface

(OPTIONAL) Enter one of the interface keywords along with the slot/port information:

- For a 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 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.

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 8.4.2.1	The optional guard keyword was added.
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 (pvst brief)

```
FTOS#show spanning-tree pvst vlan 3 brief
VLAN 3
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 4096, Address 0001.e801.6aa8
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	Designated Bridge ID	PortID
Gi 1/0	128.130	128	20000	FWD	20000	4096 0001.e801.6aa8	128.426
Gi 1/1	128.131	128	20000	BLK	20000	4096 0001.e801.6aa8	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

Interface Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
Gi 1/0	Root	128.130	128	20000	FWD	20000	P2P	No
Gi 1/1	Altr	128.131	128	20000	BLK	20000	P2P	No
Gi 1/16	Desg	128.146	128	20000	FWD	20000	P2P	Yes
Gi 1/17	Desg	128.147	128	20000	FWD	20000	P2P	Yes

**Example 2
(pvst vlan)**

```

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
(with EDS & 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
```

Interface Name	PortID	Prio	Cost	Sts	Cost	Designated Bridge ID	PortID
Gi 1/0	128.1223	128	20000	EDS	0	32768 0001.e800.a12b	128.1223

Example 4
(with EDS & 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
```

Interface Name	PortID	Prio	Cost	Sts	Cost	Designated Bridge ID	PortID
Gi 1/0	128.1223	128	20000	EDS	0	32768 0001.e800.a12b	128.1223

Example 5
(pvst guard)

```
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 48-125. show spanning-tree pvst guard Command Information

Field	Description
Interface Name	PVST interface
Instance	PVST instance
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut)
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard)

Related Commands

[spanning-tree pvst](#)

Configure PVST+ on an interface.

spanning-tree pvst



Configure PVST+ edge port with optional Bridge Port Data Unit (BPDU) guard, VLAN, port priority, and port cost on an interface.

Syntax `spanning-tree pvst [edge-port [bpduguard [shutdown-on-violation]] | vlan vlan-range {cost number | priority value}]`

Parameters

- edge-port** (OPTIONAL) Enter the keyword **edge-port** to configure the interface as a PVST+ 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.
- vlan *vlan-range*** (OPTIONAL) Enter the keyword **vlan** followed by the VLAN number(s).
Range: 1 to 4094
- cost *number*** (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 *value*** (OPTIONAL) Enter the keyword **priority** followed the Port priority value in increments of 16.
Range: 0 to 240
Default: 128

Defaults Not Configured

Command Modes INTERFACE

Command History

- Version 8.2.1.0 Introduced hardware shutdown-on-violation option
- 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

Usage Information

The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an error disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.



Note: A port configured as an edge port, on a PVST switch, will immediately transition to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

If **shutdown-on-violation** is not enabled, BPDUs will still be sent to the RPM CPU.

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 Force10 systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU.

Dell Force10 systems do not expect PVST+ BPDU on an untagged port. If this happens, FTOS places the port in error-disable state. This behavior might result in the network not converging. To prevent FTOS from executing this action, use the command `no spanning-tree pvst err-disable cause invalid-pvst-bpdu`.

**Related
Commands**

[show spanning-tree pvst](#)

[View the PVST+ configuration.](#)

tc-flush-standard

C **E** **S** 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 FTOS implements an optimized flush mechanism for PVST+. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this *knob* command can be turned on to enable flushing MAC addresses upon receiving every topology change notification.

vlan bridge-priority

C **E** **S** 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 <i>vlan-range</i>	Enter the keyword vlan followed by the VLAN number(s). Range: 1 to 4094
bridge-priority <i>value</i>	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 FTOS transitions to the forwarding state
vlan hello-time	Change the time interval between BPDUs
vlan max-age	Change the time interval before PVST+ refreshes
show spanning-tree pvst	Display the PVST+ configuration

vlan forward-delay

C **E** **S**

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

C **E** **S**

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 FTOS 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 <i>vlan-range</i>	Enter the keyword vlan followed by the VLAN number(s). Range: 1 to 4094
	max-age <i>seconds</i>	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 FTOS transitions to the forwarding state
	vlan hello-time	Change the time interval between BPDUs
	show spanning-tree pvst	Display the PVST+ configuration

Quality of Service (QoS)

Overview

FTOS commands for Quality of Service (QoS) include traffic conditioning and congestion control. QoS commands are not universally supported on all Dell Force10 platforms. Support is indicated by the **C**, **E** and **S** 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

C **E** **S**

By default, while rate limiting, policing, and shaping, FTOS does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC Destination Address to the CRC are used for forwarding and are included in these rate metering calculations. You can optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

Syntax `qos-rate-adjustment overhead-bytes`

Parameters

<code>overhead-bytes</code>	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

Version 8.3.1.0	Introduced
-----------------	------------

Per-Port QoS Commands

Per-port QoS (“port-based QoS”) allows users to defined QoS configuration on a per-physical-port basis. The commands include:

- [dot1p-priority](#)
- [rate 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

<i>priority-value</i>	Enter a value from 0 to 7.
dot1p	Queue Number
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

For the **C-Series** and **S-Series**, enter a value 0, 2, 4, or 6

dot1p	Queue Number
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Defaults No default behavior or values

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced on C-Series
pre-Version 6.1.1.1	Introduced on E-Series

Usage Information

The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.

When you set the priority for a Port Channel, the physical interfaces assigned to the Port Channel are configured with the same value. You cannot assign `dot1p-priority` command to individual interfaces in a Port Channel.

rate limit

E 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 Force10 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: 0-10000000
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 Force10 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: 0-10000000
<i>committed-rate</i>	Enter a number as the bandwidth in Mbps. Range: 0 to 10000
<i>burst-KB</i>	(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

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

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

C **E** **S**

Shape the traffic output on the selected interface.

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

Granularity for *rate* is Mbps unless the **kbps** option is used.

Command Modes

INTERFACE

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 and on C-Series
pre-Version 6.1.1.1 Introduced on E-Series

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.

Related Commands

[rate-shape](#) Shape traffic output as part of the designated policy.

service-class dynamic dot1p



Honor all 802.1p markings on incoming switched traffic on an interface (from INTERFACE mode) or on all interfaces (from CONFIGURATION mode). A CONFIGURATION mode entry supercedes 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. The default mapping is as follows:

Table 49-126. Default dot1p to Queue Mapping

dot1p	E-Series Queue ID	C-Series Queue ID	S-Series Queue ID
0	2	1	1
1	0	0	0
2	1	0	0
3	3	1	1
4	4	2	2
5	5	2	2
6	6	3	3
7	7	3	3

Command Modes INTERFACE

CONFIGURATION (C-Series and S-Series only)

Command History

Version 8.2.1.0	Available globally on the C-Series and S-Series so that the configuration applies to all ports.
Version 7.6.1.0	Introduced on S-Series
Version 7.5.1.0	Introduced on C-Series
Version 6.5.1.0	Expanded command to permit configuration on port channels
pre-Version 6.1.1.1	Introduced on E-Series

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 queueing 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

C **S** 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. Range 1-1024.

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 supercedes the `service-class bandwidth-weight` command.

show interfaces rate

E 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 1 (rate limit)

```
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 49-127. show interfaces Command Example Fields

Field	Description
Rate limit	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Traffic monitor 0	Traffic coming to class 0
Normal	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Out of profile Yellow	Number of packets that have exceeded the configured committed rate
Out of profile Red	Number of packets that have exceeded the configured peak rate
Traffic monitor 1	Traffic coming to class 1
Traffic monitor 2	Traffic coming to class 2
Traffic monitor 3	Traffic coming to class 3
Traffic monitor 4	Traffic coming to class 4
Traffic monitor 5	Traffic coming to class 5
Traffic monitor 6	Traffic coming to class 6
Traffic monitor 7	Traffic coming to class 7
Total: yellow	Total number of packets that have exceeded the configured committed rate
Total: red	Total number of packets that have exceeded the configured peak rate

**Example 2
(rate police)**

```

FTOS#show interfaces gigabitEthernet 1/2 rate police
Rate police 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 49-128. show interfaces police Command Example Fields

Field	Description
Rate police	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Traffic monitor 0	Traffic coming to class 0
Normal	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Out of profile Yellow	Number of packets that have exceeded the configured committed rate
Out of profile Red	Number of packets that have exceeded the configured peak rate
Traffic monitor 1	Traffic coming to class 1
Traffic monitor 2	Traffic coming to class 2
Traffic monitor 3	Traffic coming to class 3
Traffic monitor 4	Traffic coming to class 4
Traffic monitor 5	Traffic coming to class 5
Traffic monitor 6	Traffic coming to class 6
Traffic monitor 7	Traffic coming to class 7
Total: yellow	Total number of packets that have exceeded the configured committed rate
Total: red	Total number of packets that have exceeded the configured peak rate

strict-priority queue

C **E** **S**

Configure a unicast queue as a strict-priority (SP) queue.

Syntax

strict-priority queue unicast *number*

Parameters

unicast *number* Enter the keyword **unicast** followed by the queue number.
C-Series and **S-Series** Range: 1 to 3
E-Series Range: 1 to 7

Defaults

No default behavior or value

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 6.1.1.1 Introduced on E-Series

Usage Information

Once a unicast queue is configured as strict-priority, that particular queue, on the entire chassis, is treated as strict-priority queue. Traffic for a strict priority is scheduled before any other queues are serviced. For example, if you send 100% line rate traffic over the SP queue, it will *starve* all other queues on the ports on which this traffic is flowing.

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. FTOS enables you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANs, or loopbacks. The commands are:

- [bandwidth-percentage](#)
- [bandwidth-weight](#)
- [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](#)
- [show cam layer2-qos](#)
- [show cam layer3-qos](#)
- [show qos class-map](#)
- [show qos policy-map](#)
- [show qos policy-map-input](#)
- [show qos policy-map-output](#)
- [show qos qos-policy-input](#)
- [show qos qos-policy-output](#)
- [show qos statistics](#)
- [show qos wred-profile](#)
- [test cam-usage](#)
- [threshold](#)
- [trust](#)
- [wred](#)
- [wred-profile](#)

bandwidth-percentage

E 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

C **S** 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)

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.
<i>class-map-name</i>	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

ip access-list extended	Configure an extended IP ACL.
ip access-list standard	Configure a standard IP ACL.
match ip access-group	Configure the match criteria based on the access control list (ACL)
match ip precedence	Identify IP precedence values as match criteria
match ip dscp	Configure the match criteria based on the DSCP value
match mac access-group	Configure a match criterion for a class map, based on the contents of the designated MAC ACL.
match mac dot1p	Configure a match criterion for a class map, based on a dot1p value.
match mac vlan	Configure a match criterion for a class map based on VLAN ID.
service-queue	Assign a class map and QoS policy to different queues.
show qos class-map	View the current class map information.

clear qos statistics

C **E** **S**

Clears Matched Packets, Matched Bytes, and Dropped Packets. For TeraScale, clears Matched Packets, Matched Bytes, Queued Packets, Queued Bytes, and Dropped Packets.

Syntax `clear qos statistics interface-name`.

Parameters

interface-name

Enter one of the following keywords:

- 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.

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

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

C **E** **S**

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



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



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)

Command History

- Version 7.7.1.0 Added keyword **multicast**.
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
Added support for DSCP Marking option
- Version 6.2.1.1 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.

The **match ip dscp** and **match ip precedence** commands are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DCSP values 0 1 2 3 4 5 6 7, enter either the command **match ip dscp 0,1,2,3,4,5,6,7** or **match ip dscp 0-7**.



Note: Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values need to match.

Related Commands

- [class-map](#) Identify the class map.

match ip precedence

C **E** **S** 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)

Command History

Version 7.7.1.0	Added keyword multicast . Added DSCP marking option support for S-Series
Version 7.6.1.0	Introduced on S-Series
Version 7.5.1.0	Introduced on C-Series Added support for DSCP Marking option
Version 6.2.1.1	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.

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

C **E** **S** 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

C **E** **S** 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

C **E** **S**

Configure a match criterion for a class map based on VLAN ID.

Syntax `match mac vlan number`

Parameters *number* Enter the VLAN ID.
Range: 1–4094

Defaults None

Command Modes CLASS-MAP

Command History Version 8.2.0.1 Introduced

Usage Information You must first enter the **class-map** command in order to access this command. You can match against only one VLAN ID.

Related Commands [class-map](#) Create/access a class map.

policy-aggregate

C **E** **S**

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 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
pre-Version 6.1.1.1 Introduced on E-Series

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

policy-map-input	Create an input policy map
policy-map-output	Create an output policy map (E-Series Only)

policy-map-input

C **E** **S** 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

- [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 input](#) Apply an input policy map to the selected interface.

policy-map-output

C E S Create an output policy map.

Syntax **policy-map-output** *policy-map-name*
To remove a policy map, use the **no policy-map-output** *policy-map-name* command.

Parameters *policy-map-name* Enter the name for the policy map in character format (16 characters maximum).

Defaults 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 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, FTOS 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

[rate-police](#) Incoming traffic policing function

qos-policy-output

C **E** **S**

Create a QoS output policy.

Syntax `qos-policy-output qos-policy-name`

To remove an existing output QoS policy, use **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

rate-limit	Outgoing traffic rate-limit functionality
bandwidth-percentage	Assign weight to class/queue percentage
bandwidth-weight	Assign a priority weight to a queue.
wred	Assign yellow or green drop precedence

queue backplane ignore-backpressure

E

Reduce egress pressure by ignoring the ingress backpressure

Syntax `queue backplane ignore-backpressure`

To return to the default, use the **no queue backplane ignore-backpressure** command.

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 7.7.1.0	Introduced on E-Series
-----------------	------------------------

queue egress

E 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 7.5.1.0 Added support for multicast-bandwidth
Version 7.4.1.0 and 6.5.3.0 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

[show queue statistics egress](#) Display the egress queue statistics

queue ingress

E 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

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

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 7.4.1.0 and 6.5.3.0 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 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

Related Commands

[show queue statistics ingress](#) Display the ingress queue statistics

rate-limit

E Specify the rate-limit functionality on outgoing traffic as part of the selected policy.

Syntax `rate-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 Force10 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: 0-10000000

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

C **E** **S**

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 Force10 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: 0-10000000

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

C **E** **S**

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 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

<i>policy-map-name</i>	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

Usage Information A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.






Note: The **service-policy** commands are not allowed on a port channel.

The **service-policy input *policy-map-name*** command and the **service-class dynamic dot1p** command are not allowed simultaneously on an interface. 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

<i>policy-map-name</i>	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	Version 7.6.1.0 Introduced on C-Series and S-Series pre-Version 6.1.1.1 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

C **E** **S** Assign a class map and QoS policy to different queues.

Syntax `service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]`

To remove the queue assignment, use the **no service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]** command.

Parameters	<i>queue-id</i> Enter the value used to identify a queue. Range: 0 to 7 on E-Series (eight queues per interface), 0-3 on C-Series and S-Series (four queues per interface; four queues are reserved for control traffic.)
	class-map <i>class-map-name</i> (OPTIONAL) Enter the keyword class-map followed by the class map name assigned to the queue in character format (16 character maximum). Note: This option is available under policy-map-input only.
	qos-policy <i>qos-policy-name</i> (OPTIONAL) Enter the keyword qos-policy followed by the QoS policy name assigned to the queue in text format (16 characters maximum). This specifies the input QoS policy assigned to the queue under policy-map-input and output QoS policy under policy-map-output context.

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

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 There are eight (8) queues per interface on the E-Series and four (4) queues per interface on the C-Series and S-Series. This command assigns a class map or QoS policy to different queues.

Related Commands	class-map Identify the class map.
	service-policy input Apply an input policy map to the selected interface.
	service-policy output Apply an output policy map to the selected interface.

set

C **E** **S**

Mark outgoing traffic with a Differentiated Service Code Point (DSCP) or dot1p value.

Syntax `set {ip-dscp value | mac-dot1p value}`

Parameters

ip-dscp *value* (OPTIONAL) Enter the keyword **ip-dscp** followed by the IP DSCP value.
Range: 0 to 63

mac-dot1p *value* Enter the keyword **mac-dot1p** followed by the dot1p value.
Range: 0 to 7
On the C-Series and S-Series allowed values are:0,2,4,6

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
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

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

E

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 Introduced on E-Series

Example 1 (interface) FTOS#show cam layer2-qos interface gigabitethernet 2/0

Cam Index	Port	Dot1p	Proto	SrcMac	SrcMask	DstMac	DstMask	Dot1p	DSCP	Queue
								Marking	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:c0	00:00:00:00:00:f0	00:00:00:00:00:d0	00:00:00:00:00:f0	-	45	5
01819	0	4	0	00:00:00:a0:00:00	00:00:00:ff:00:00	00:00:00:b0:00:00	00:00:00:ff:00:00	4	-	4
01820	0	-	0x2000	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:b0	ff:ff:ff:ff:ff:ff	-	-	1
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

Example 2 (linecard) FTOS#show cam layer2-qos linecard 2 port-set 0

Cam Index	Port	Dot1p	Proto	SrcMac	SrcMask	DstMac	DstMask	Dot1p	DSCP	Queue
								Marking	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:c0	00:00:00:00:00:f0	00:00:00:00:00:d0	00:00:00:00:00:f0	-	45	5
01819	0	4	0	00:00:00:a0:00:00	00:00:00:ff:00:00	00:00:00:b0:00:00	00:00:00:ff:00:00	4	-	4
01820	0	-	0x2000	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:b0	ff:ff:ff:ff:ff:ff	-	-	1
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

show cam layer3-qos

E Display the Layer 3 QoS CAM entries.

Syntax **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 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 6.5.1.0 Introduced on E-Series

Example 1
(show cam layer3-qos linecard interface)

```
FTOS#sh cam layer3-qos interface gigabitethernet 2/1
```

Cam Index	Port	Dscp	Proto	Tcp Flag	Src Port	Dst Port	SrcIp	DstIp	DSCP Marking	Queue
23488	1	0	0	0x0	0	0	0.0.0.0/0	0.0.0.0/0	-	TRUST-DSCP

FTOS#

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 2
(show cam layer3-qos linecard port-set)

```
FTOS#show cam layer3-qos linecard 13 port-set 0
```

Cam Index	Port	Dscp	Proto	Tcp Flag	Src Port	Dst Port	SrcIp	DstIp	DSCP Marking	Queue
24511	1	0	TCP	0x5	2	5	1.0.0.1/24	2.0.0.2/24	-	TRUST-DSCP
24512	1	0	UDP	0x2	2	5	8.0.0.8/24	8.0.0.8/24	23	3

FTOS#

Example 3
(show cam layer3-qos linecard interface)

```
FTOS#sh cam layer3-qos interface gigabitethernet 2/1
```

Cam Index	Port	Dscp	Proto	Tcp Flag	Src Port	Dst Port	SrcIp	DstIp	DSCP Marking	Queue
23488	1	56	0	0x0	0	0	0.0.0.0/0	0.0.0.0/0	-	7
23489	1	48	0	0x0	0	0	0.0.0.0/0	0.0.0.0/0	-	6
23490	1	40	0	0x0	0	0	0.0.0.0/0	0.0.0.0/0	-	5
23491	1	0	IP	0x0	0	0	10.1.1.1/32	20.1.1.1/32	-	0
23492	1	0	IP	0x0	0	0	10.1.1.1/32	20.1.1.2/32	-	0

```
24511 1 0 0 0x0 0 0 0.0.0.0/0 0.0.0.0/0 - 0
FTOS#
```

**Example 4
(show cam
layer3-qos
summary)**

```
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

C **E** **S**

View the current class map information.

Syntax `show qos class-map [class-name]`

Parameters *class-name* (Optional) Enter the name of a configured class map.

Defaults 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

```
FTOS#show qos class-map

Class-map match-any CM
  Match ip access-group ACL
```

Related Commands [class-map](#) Identify the class map

show qos policy-map

C **E** **S** View the QoS policy map information.

Syntax `show qos policy-map {summary [interface] | detail [interface]}`

Parameters

- summary interface** To view a policy map interface summary, enter the keyword **summary** and optionally one of the following keywords and slot/port or number information:
- For a 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.
- 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.

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
Version 7.4.1.0	E-Series only: Added Trust IPv6 diffserv
Version 6.2.1.1	Introduced on E-Series

Example 1 (IPv4) FTOS#show qos policy-map detail gigabitethernet 0/0

```
Interface GigabitEthernet 4/1

Policy-map-input policy
Trust diffserv
Queue#    Class-map-name          Qos-policy-name
  0        -                  q0
  1        CM1                 q1
  2        CM2                 q2
  3        CM3                 q3
  4        CM4                 q4
  5        CM5                 q5
  6        CM6                 q6
  7        CM7                 q7
FTOS#
```

Example 2
(E-Series, IPv6)

```

FTOS# show qos policy-map detail gigabitethernet 0/0

Interface GigabitEthernet 8/29

Policy-map-input pmap1
Trust ipv6-diffserv
Queue#   Class-map-name           Qos-policy-name
0        c0                            q0
1        c1                            q1
2        c2                            q2
3        c3                            q3
4        c4                            q4
5        c5                            -
6        c6                            q6
7        c7                            q7
FTOS#

```

Example 3
(IPv4)

```

FTOS#sho qos policy-map summary

Interface           policy-map-input      policy-map-output
Gi 4/1              PM1                   -
Gi 4/2              PM2                   PMOut
FTOS#

```

show qos policy-map-input



View the input QoS policy map details.

Syntax

show qos policy-map-input [*policy-map-name*] [*class class-map-name*] [*qos-policy-input qos-policy-name*]

Parameters

policy-map-name Enter the policy map name.

class *class-map-name* Enter the keyword class followed by the class map name.

qos-policy-input Enter the keyword **qos-policy-input** followed by the QoS policy name.

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

Version 7.4.1.0 E-Series Only: Added Trust IPv6 diffserv

Version 6.2.1.1 Introduced on E-Series

Example 1
(IPv4)

```

FTOS#show qos policy-map-input

Policy-map-input PolicyMapInput
Aggregate Qos-policy-name AggPolicyIn
Queue#   Class-map-name           Qos-policy-name

```

```

0      ClassMap1      qosPolicyInput
FTOS#

```

**Example 2
(IPv6)**

```

FTOS# show qos policy-map-input

Policy-map-input pmap1
Trust ipv6-diffserv
Queue#   Class-map-name   Qos-policy-name
0        c0                q0
1        c1                q1
2        c2                q2
3        c3                q3
4        c4                q4
5        c5                -
6        c6                q6
7        c7                q7
FTOS#

```

show qos policy-map-output

C **E** **S** View the output QoS policy map details.

Syntax **show qos policy-map-output** [*policy-map-name*] [**qos-policy-output** *qos-policy-name*]

Parameters

<i>policy-map-name</i>	Enter the policy map name.
qos-policy-output <i>qos-policy-name</i>	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

Example

```

FTOS#show qos policy-map-output

Policy-map-output PolicyMapOutput
Aggregate Qos-policy-name AggPolicyOut
Queue#       Qos-policy-name
0            qosPolicyOutput
FTOS#

```

show qos qos-policy-input

C **E** **S** 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

```
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

C **E** **S** 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

```
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.

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.

Defaults No default behavior or values

Command Modes EXEC
EXEC Privilege

Command History

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

Usage Information 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, refer to 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 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 49-129. show qos statistics Command Example Fields (ED and EE Series)

Field	Description
Queue #	Queue Number
Queued Bytes	Snapshot of the byte count in that queue.
Matched Pkts	The number of packets that matched the class-map criteria. Note: When trust is configured, matched packet counters are not incremented in this field.
Matched Bytes	The number of bytes that matched the class-map criteria. Note: When trust is configured, matched byte counters are not incremented in this field.

Example 2 FTOS#show qos statistics gig 0/1

```

Queue#  Queued          Queued          Matched          Matched          Dropped
        Bytes          Pkts            Pkts            Bytes            Pkts
        (Cumulative)  (Cumulative)
  0      0                0                1883725         1883725000       0
  1      0                0                1883725         1883725000       0
  2      0                0                1883725         1883725000       0
  3      0                0                1883725         1883725000       0
  4      0                0                1883725         1883725000       0
  5      0                0                1883724         1883724000       0
  6      0                0                1883720         1883720000       0
  7      0                0                1883720         1883720000       0
FTOS#

```

Table 49-130. show qos statistics Command Example Fields (EF Series)

Field	Description
Queue #	Queue number
Queued Bytes	Cumulative byte count in that queue
Queued Pkts	Cumulative packet count in that queue.

Table 49-130. show qos statistics Command Example Fields (EF Series) (Continued)

Field	Description
Matched Pkts	The number of packets that matched the class-map criteria. Note: When trust is configured, matched packet counters are not incremented in this field.
Matched Bytes	The number of bytes that matched the class-map criteria. Note: When trust is configured, matched byte counters are not incremented in this field.
Dropped Pkts	The total of the number of packets dropped for green, yellow and out-of-profile.

**Example 3
(show qos
statistics
wred-profile)**

```

FTOS#show qos statistics wred-profile
Interface Gi 5/11
Queue# Drop-statistic WRED-name Dropped Pkts
  0     Green          WRED1          51623
      Yellow          WRED2          51300
      Out of Profile
  1     Green          WRED1          52082
      Yellow          WRED2          51004
      Out of Profile
  2     Green          WRED1          50567
      Yellow          WRED2          49965
      Out of Profile
  3     Green          WRED1          50477
      Yellow          WRED2          49815
      Out of Profile
  4     Green          WRED1          50695
      Yellow          WRED2          49476
      Out of Profile
  5     Green          WRED1          50245
      Yellow          WRED2          49535
      Out of Profile
  6     Green          WRED1          50033
      Yellow          WRED2          49595
      Out of Profile
  7     Green          WRED1          50474
      Yellow          WRED2          49522
      Out of Profile
FTOS#

```

Table 49-131. show qos statistics wred-profile Command Example Fields (ED, EE, and EF Series)

Field	Description
Queue #	Queue Number
Drop-statistic	Drop statistics for green, yellow and out-of-profile packets
WRED-name	WRED profile name
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

**Related
Commands**

[clear qos statistics](#)

Clears counters as shown in [show qos statistics](#)

show qos wred-profile

E 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

C E S 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 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,

Linecard	Portpipe	CAM Partition	Available CAM	Estimated CAM per Port	Status (Allowed ports)
0	0	L2ACL	500	200	Allowed (2)
0	1	L2ACL	100	200	Exception
1	0	L2ACL	1000	200	Allowed (5)
1	1	L2ACL	0	200	Exception
		...			
		...			
		...			
13	1	L2ACL	400	200	Allowed (2)

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 49-132. test cam-usage Command Example Fields

Field	Description
Linecard	Indicates the line card slot number.
Portpipe	Indicates the portpipe number.
CAM Partition	The CAM space where the rules are added.
Available CAM	Indicates the free CAM space, in the partition, for the classification rules. Note: The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, can not be used as a policy map for the classification rules.
Estimated CAM per Port	Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface. Note: The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.
Status (Allowed ports)	Indicates if the input policy map configuration on an interface belonging to a linecard/port-pipe is successful—Allowed (<i>n</i>)—or not successful—Exception. The allowed number (<i>n</i>) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.

Usage Information

This features 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

E 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

min number Enter the keyword **min** followed by the minimum threshold number for the WRED profile.
Range: 1024 to 77824 KB

max number Enter the keyword **max** followed by the maximum threshold number for the WRED profile.
Range: 1024 to 77824 KB

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 49-133. Pre-defined WRED Profile Threshold Values

Pre-defined WRED Profile Name	Minimum Threshold	Maximum 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

Related Commands

[wred-profile](#) Create a WRED profile.

trust

C **E** **S** 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.

Table 49-134. Standard Default DSCP Mapping Table

DSCP/CP hex range (XXX)	DSCP Definition	Traditional IP Precedence	E-Series Internal Queue ID	C-Series and S-Series Internal Queue ID	DSCP/CP decimal
111XXX		Network Control	7	3	48–63
110XXX		Internetwork Control	6	3	
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	5	2	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	4	2	
011XXX	AF3	Flash	3	1	16–31
010XXX	AF2	Immediate	2	1	
001XXX	AF1	Priority	1	0	0–15
000XXX	BE (Best Effort)	Best Effort	0	0	

wred

E 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

Version 8.2.1.0 Profile name character limit increased from 16 to 32.
pre-Version 6.1.1.1 Introduced on E-Series

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

wred-profile

E 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 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

E 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

E Clear ingress queue statistics.

Syntax `clear queue statistics ingress [unicast [src-card ID [dst-card ID]] | [multicast] [src-card ID]]`

Parameters

unicast [src-card ID [dst-card ID]] (OPTIONAL) Enter the keyword **unicast** to clear Unicast queue statistics. Optionally, enter the source card identification (**src-card ID**) and the destination card identification (**dst-card ID**) to clear the unicast statistics from the source card to the destination card.

multicast [src-card ID] (OPTIONAL) Enter the keyword **multicast** to clear only Multicast queue statistics. Optionally, enter the source card identification (**src-card ID**) to clear the multicast statistics from the source card. Default: Both Unicast and Multicast queue statistics are cleared.

Defaults No default behavior or values

Command Modes EXEC

EXEC Privilege

Command History Version 6.2.1.1 Introduced

Related Commands

clear queue statistics egress	Clear egress queue statistics
show queue statistics egress	Display egress queue statistics
show queue statistics ingress	Display ingress queue statistics

show queue statistics egress

E Display the egress queue statistics.

Syntax `show queue statistics egress [unicast | multicast] [Interface] [brief]`

Parameters

unicast | multicast (OPTIONAL) Enter the keyword **multicast** to display only Multicast queue statistics. Enter the keyword **unicast** to display only Unicast queue statistics. Default: Both Unicast and Multicast queue statistics are displayed.

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.

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 for E-Series

Usage Information 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 49-135. Numbering Conventions for show queue egress statistics Output

Value	Divide the number by	Quotient Display	Examples
(10 ¹¹) - (10 ¹⁴)	1024	K	12345678901K
(10 ¹⁴) - (10 ¹⁷)	1024*1024	M	12345678901M
> (10 ¹⁷)	1024*1024*1024	T	12345678901T



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 (TeraScale)

```
FTOS#show queue statistics egress unicast gigabitethernet 9/1
```

```
Interface Gi 9/1
```

Egress Port Queue#	Queued bytes	Queued packets	Packet Type	Min KB	Max KB	Dropped packets
0	281513847K	31959000	Green	2048	4096	0
			Yellow	1024	2048	0
			Out of Profile			30385770
1	99281660K	11271000	Green	2048	4096	0
			Yellow	1024	2048	0
			Out of Profile			9886100
2	99281660K	11271000	Green	2048	4096	0
			Yellow	1024	2048	0
			Out of Profile			9784600
3	38984440000	4322000	Green	2048	4096	0
			Yellow	1024	2048	0
			Out of Profile			3053753
4	99281660K	11271000	Green	2048	4096	0
			Yellow	1024	2048	0
			Out of Profile			9581600
5	39760160000	4408000	Green	2048	4096	0
			Yellow	1024	2048	0
			Out of Profile			3070671
6	39642900000	4395000	Green	2048	4096	0

```

          Yellow          1024      2048      0
          Out of Profile
7      99274410K      11270177      Green          2048      4096      0
          Yellow          1024      2048      0
          Out of Profile
FTOS#

```

Table 49-136. show queue statistics egress Command Fields

Field	Description
Egress Port Queue#	Egress Port Queue Number
Queued bytes	Cumulative byte count in that queue
Queued packets	Cumulative packet count in that queue.
Packet type	Green, yellow, and out-of-profile packets
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Example 2
(show queue
statistics egress)

```

FTOS#sho queue statistics egress multicast
Linecard 3 port pipe 0, multicast

Packet Type      Min      Max      Dropped
                  KB       KB       packets
Green            8192    16384    0
Yellow           4096    8192     0
Out of Profile
Linecard 3 port pipe 1, multicast

Packet Type      Min      Max      Dropped
                  KB       KB       packets
Green            8192    16384    0
Yellow           4096    8192     0
Out of Profile
Linecard 7 port pipe 0, multicast

Packet Type      Min      Max      Dropped
                  KB       KB       packets
Green            2048    4096     0
Yellow           1024    2048     0
Out of Profile
Linecard 7 port pipe 1, multicast

Packet Type      Min      Max      Dropped
                  KB       KB       packets
Green            2048    4096     0
Yellow           1024    2048     0
Out of Profile
FTOS#

```


Table 49-137. show queue statistics egress multicast Command Fields

Field	Description
Packet type	Green, yellow, and out-of-profile packets
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

**Example 3
(show queue
statistics egress
brief)**

```

FTOS#show queue statistics egress brief
LC      Portpipe      Port      Dropped
        PortPipe      packets
0       0              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              8         0
0       0              9         0
0       0              10        0
0       0              11        0
0       0              M         0
0       1              0         0
0       1              1         0
0       1              2         0
0       1              3         0
0       1              4         0
0       1              5         0
0       1              6         0
0       1              7         0
0       1              8         0
0       1              9         0
0       1              10        0
0       1              11        0
0       1              M         0
1       0              0         0
FTOS#

```

Table 49-138. show queue statistics egress brief Command Fields

Field	Description
LC	Line Card
Portpipe	Portpipe number
Port	Port Queue. Where M is Multicast queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

**Related
Commands**

[clear queue statistics egress](#)
[clear queue statistics ingress](#)
[show queue statistics ingress](#)

Clear egress queue statistics.
Clear ingress queue statistics.
Display ingress queue statistics

show queue statistics ingress

E 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 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 49-139. Numbering Conventions for show queue statistics ingress Output

Value	Divide the number by	Quotient Display	Examples
(10 ¹¹) - (10 ¹⁴)	1024	K	12345678901K
(10 ¹⁴) - (10 ¹⁷)	1024*1024	M	12345678901M
> (10 ¹⁷)	1024*1024*1024	T	12345678901T

 **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.

Example 1
(show queue
statistics ingress
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

SF	Packet Type	Min	Max	Dropped
Ingress		KB	KB	packets
Queue#				
0	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
1	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
2	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
3	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
4	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
5	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
6	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
7	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0

Linecard 7 port pipe 0, to linecard 3 port pipe 1, unicast

SF	Packet Type	Min	Max	Dropped
Ingress		KB	KB	packets
Queue#				
0	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
1	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
2	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
3	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
4	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
5	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
6	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
7	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0

4	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
5	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
6	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
7	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0

Table 49-140. show queue statistics Command Fields

Field	Description
SF Ingress Queue #	Switch Fabric Queue Number
Packet type	Green, yellow, and out-of-profile packets
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Example 2
(show queue
statistics ingress
multicast)

```
FTOS#show queue statistics ingress multicast src-card 7
```

```
Linecard 7 port pipe 0, multicast
```

SF Ingress Queue#	Packet Type	Min KB	Max KB	Dropped packets
0	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
1	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
2	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
3	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
4	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
5	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
6	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
7	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0

```
Linecard 7 port pipe 1, multicast
```

SF Ingress Queue#	Packet Type	Min KB	Max KB	Dropped packets
0	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
1	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
2	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
3	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
4	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
5	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
6	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0
7	Green	4096	4096	0
	Yellow	3276	3276	0
	Out of Profile			0

FTOS#

Table 49-141. show queue statistics ingress Multicast Command Fields

Field	Description
SF Ingress Queue #	Switch Fabric Queue Number
Packet type	Green, yellow, and out-of-profile packets
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

**Example 3
(show queue statistics ingress brief)**

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
0	1	1	100
1	0	0	0
1	0	1	100
1	1	0	0
1	1	1	100
2	0	0	0
2	0	1	100
2	1	0	0
2	1	1	100
3	0	0	0

3	0	1	100
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 49-142. show queue statistics ingress brief Command Fields

Field	Description
Dest LC	Destination Line Card
Src Port Set	Source PortPipe Number
Dest Port Set	Destination PortPipe Number
Dropped Pkts	The number of packets dropped

**Related
Commands**

clear queue statistics egress	Clear egress queue statistics.
clear queue statistics ingress	Clear ingress queue statistics.
show queue statistics ingress	Display egress queue statistics

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 FTOS version 7.6.1.0 and later. The S-Series platform supports RIP with FTOS 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

C **E** **S**

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

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

clear ip rip

C **E** **S**

Update all the RIP routes in the FTOS routing table.

Syntax **clear ip rip**

Command Modes EXEC Privilege

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

This command triggers updates of the main RIP routing tables.

debug ip rip

C E S

Examine RIP routing information for troubleshooting.

Syntax `debug ip rip [interface | database | events [interface] | packet [interface] | trigger]`

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 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.
- 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 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

C E S

Generate a default route for the RIP traffic.

Syntax `default-information originate [always] [metric metric-value] [route-map map-name]`

To return to the default values, enter **no default-information originate**.

Parameters

- always** (OPTIONAL) Enter the keyword **always** to enable the switch software to always advertise the default route.
- metric metric-value** (OPTIONAL) Enter the keyword **metric** followed by a number as the metric value.
Range: 1 to 16
Default: 1
- route-map map-name** (OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route-map.

Defaults Disabled.
metric: 1

Command Modes ROUTER RIP

Command History

Version 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 The default route must be present in the switch routing table for the [default-information originate](#) command to take effect.

default-metric

C **E** **S** 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

<i>number</i>	Specify a number. Range: 1 to 16. The default is 1.
---------------	---

Default 1

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

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

C **E** **S**

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

C **E** **S**

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

<i>weight</i>	Enter a number from 1 to 255 for the weight (for prioritization). The default is 120.
<i>ip-address</i>	(OPTIONAL) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric.
<i>mask</i>	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)
<i>prefix-name</i>	(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

C **E** **S** Configure a filter for incoming routing updates.

Syntax **distribute-list** *prefix-list-name* **in** [*interface*]

To delete the filter, use the **no distribute-list** *prefix-list-name in* command.

Parameters

prefix-list-name Enter the name of a configured prefix list.

interface (OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a 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 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

C **E** **S** 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	<i>prefix-list-name</i>	Enter the name of a configured prefix list.
	<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> C-Series and S-Series Range: 1-128 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 VLAN, enter the keyword vlan followed by a number from 1 to 4094.
	connected	(OPTIONAL) Enter the keyword connected to filter only directly connected routes.
	isis	(OPTIONAL) Enter the keyword isis to filter only IS-IS routes. Note: This option is only available on E-Series.
	ospf	(OPTIONAL) Enter the keyword ospf to filter all OSPF routes.
	static	(OPTIONAL) Enter the keyword static to filter manually configured routes.
Defaults	Not configured.	
Command Modes	ROUTER RIP	
Command History	Version 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.

ip poison-reverse

C **E** **S** 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 IPv4 and IPv6.

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 IPv4.
2	(OPTIONAL) Enter the number 2 for RIP version 2.

Defaults IPv4.

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 To enable the interface to send both version of RIP packets, enter **ip rip send version 1 2**.

Related Commands

ip rip receive version	Sets the RIP version for the interface to receive traffic.
version	Sets the RIP version to be used for the switch software.

ip split-horizon

C **E** **S**

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

Syntax **ip split-horizon**

To disable split-horizon, enter **no ip split-horizon**.

Defaults Enabled

Command Modes INTERFACE

Command History

Version 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 poison-reverse](#) Set the prefix for RIP routing updates.

maximum-paths

C **E** **S**

Set RIP to forward packets over multiple paths.

Syntax **maximum-paths** *number*

To return to the default values, enter **no maximum-paths**.

Parameters

number Enter the number of paths.
Range: 1 to 16.
The default is 4 paths.

Defaults 4

Command Modes ROUTER RIP

Command History

Version 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

RIP supports a maximum of 16 ECMP paths.

neighbor

C **E** **S**

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

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 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

C **E** **S**

Enable RIP for a specified network. Use this command to enable RIP on all networks connected to the switch.

Syntax **network** *ip-address*

To disable RIP for a network, use the **no network** *ip-address* command.

Parameter *ip-address* Specify an IP network address in dotted decimal format. You cannot specify a subnet.

Defaults No RIP network is configured.

Command Modes ROUTER RIP

Command History

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 You can enable an unlimited number of RIP networks.
RIP operates over interfaces configured with any address specified by the [network](#) command.

offset-list

C **E** **S**

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 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

Usage Information When the offset metric is applied to an interface, that value takes precedence over an offset value that is not extended to an interface.

Related Commands

[ip prefix-list](#) Enter the PREFIX-LIST mode and configure a prefix list.

output-delay

C **E** **S**

Set the interpacket delay of successive packets to the same neighbor.

Syntax `output-delay delay`

To return to the switch software defaults for interpacket delay, 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	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	This command is intended for low-speed interfaces.	

passive-interface

C **E** **S** Suppress routing updates on a specified interface.

Syntax `passive-interface interface`

To delete a passive interface, use the **no passive-interface *interface*** command.

Parameters	<i>interface</i>	Enter the following information:
		<ul style="list-style-type: none"> 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 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

Usage Information 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

C **E** **S**

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

Usage Information 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

E

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.

Parameters

<i>tag</i>	(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.
level-1-2	(OPTIONAL) Enter the keyword level-1-2 to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keyword level-2 to redistribute only IS-IS Level-2 routes.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword metric followed by a number as the metric value. Range: 0 to 16
route-map <i>map-name</i>	(OPTIONAL) Enter the keyword route-map followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER RIP

Command History

pre-Version 6.2.1.1	Introduced on E-Series
---------------------	------------------------

Usage Information IS-IS is not supported on S-Series systems.

redistribute ospf

C **E** **S**

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

<i>process-id</i>	Enter a number that corresponds to the OSPF process ID to be redistributed. Range: 1 to 65355.
match external {1 2}	(OPTIONAL) Enter the keywords match external followed by the numbers 1 or 2 to indicated that external 1 routes or external 2 routes should be redistributed.
match internal	(OPTIONAL) Enter the keywords match internal to indicate that internal routes should be redistributed.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword metric followed by a number as the metric value. Range: 0 to16
route-map <i>map-name</i>	(OPTIONAL) Enter the keyword route-map followed by the name of a configured route map.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

Version 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

router rip

C **E** **S**

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

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

To enable RIP, you must assign a network address using the [network](#) command.

Example

```
FTOS(conf)#router rip
FTOS(conf-router_rip)#
```

Related Commands

network	Enable RIP.
exit	Return to the CONFIGURATION mode.

show config

C **E** **S**

Display the changes you made to the RIP configuration. Default values are not shown.

Syntax **show config**

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

Example

```
FTOS(conf-router_rip)#show config
!
router rip
 network 172.31.0.0
 passive-interface GigabitEthernet 0/1
FTOS(conf-router_rip)#
```

show ip rip database

C **E** **S**

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

<i>ip-address</i>	(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.
<i>mask</i>	(OPTIONAL) Specify a mask, in /network format, for the IP address.

Command Modes EXEC Privilege

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

Example

```
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
204.250.54.0/24      auto-summary
203.250.49.0/24
    [50/1] via 192.13.1.3, 00:00:12, GigabitEthernet 9/14
203.250.49.0/24      auto-summary
210.250.40.0/24
    [50/2] via 1.1.18.2, 00:00:14, Vlan 18
    [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
210.250.40.0/24      auto-summary
207.250.53.0/24
    [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
    [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          auto-summary
208.250.42.0/24
    [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
    [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
    [50/2] via 1.1.10.2, 00:00:18, Vlan 10
208.250.42.0/24          auto-summary

```

Table 50-143. Fields in show ip rip database Command Output

Field	Description
Total number of routes in RIP database	Displays the number of RIP routes stored in the RIP database.
100.10.10.0/24 directly connected	Lists the route(s) directly connected.
150.100.0.0 redistributed	Lists the routes learned through redistribution.
209.9.16.0/24...	Lists the routes and the sources advertising those routes.

show running-config rip

C **E** **S** 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

```

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

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

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**.

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

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 the timers on one router are changed, the timers on all routers in the RIP domain must also be synchronized.

version

C **E** **S**

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

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 rip receive version](#) Set the RIP version to be received on the interface.

[ip rip send version](#) Set the RIP version to be sent out the interface.

Remote Monitoring (RMON)

Overview

FTOS RMON is implemented on all Dell Force10 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**

FTOS RMON is based on IEEE standards, providing both 32-bit and 64-bit monitoring, and long-term statistics collection. FTOS RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, and RFC-3434:

- | | |
|---|------------------|
| • Ethernet Statistics Table | RFC-2819 |
| • Ethernet Statistics High-Capacity Table | RFC-3273, 64bits |
| • Ethernet History Control Table | RFC-2819 |
| • Ethernet History Table | RFC-2819 |
| • Ethernet History High-Capacity Table | RFC-3273, 64bits |
| • Alarm Table | RFC-2819 |
| • High-Capacity Alarm Table (64bits) | RFC-3434, 64bits |
| • Event Table | RFC-2819 |
| • Log Table | RFC-2819 |

FTOS RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization



Note: Only SNMP GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

Commands

The FTOS Remote Network Monitoring RMON commands are:

- [rmon alarm](#)
- [rmon collection history](#)
- [rmon collection statistics](#)
- [rmon event](#)
- [rmon hc-alarm](#)
- [show rmon](#)
- [show rmon alarms](#)
- [show rmon events](#)
- [show rmon hc-alarm](#)
- [show rmon history](#)
- [show rmon log](#)
- [show rmon statistics](#)

rmon alarm



Set an alarm on any MIB object.

Syntax `rmon alarm number variable interval {delta | absolute} rising-threshold value event-number falling-threshold value event-number [owner string]`

To disable the alarm, use the **no rmon alarm number** command.

Parameters

<i>number</i>	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.
<i>variable</i>	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.
<i>interval</i>	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds
delta	Enter the keyword delta to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.
absolute	Enter the keyword absolute to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.
rising-threshold value event-number	Enter the keyword rising-threshold followed by the value (32bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold value event-number	Enter the keyword falling-threshold followed by the value (32bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner string	(OPTIONAL) Enter the keyword owner followed by the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Default owner

Command Modes CONFIGURATION

Command History

Version 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 collection history

C **E** **S**

Enable the RMON MIB history group of statistics collection on an interface.

Syntax **rmon collection history** { **controlEntry** *integer* } [**owner** *name*] [**buckets** *number*] [**interval** *seconds*]

To remove a specified RMON history group of statistics collection, use the **no rmon collection history** { **controlEntry** *integer* } command.

Parameters

controlEntry *integer* Enter the keyword **controlEntry** to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON History Table.

owner *name* (OPTIONAL) Enter the keyword **owner** followed by the owner name to record the owner of the RMON group of statistics.

buckets *number* (OPTIONAL) Enter the keyword **buckets** followed the number of buckets for the RMON collection history group of statistics.
Bucket Range: 1 to 1000
Default: 50

interval *seconds* (OPTIONAL) Enter the keyword **interval** followed the number of seconds in each polling cycle.
Range: 5 to 3600 seconds
Default: 1800 seconds

Defaults No default behavior

Command Modes CONFIGURATION INTERFACE (config-if)

Command History

Version 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 collection statistics

C **E** **S**

Enable RMON MIB statistics collection on an interface.

Syntax **rmon collection statistics** { **controlEntry** *integer* } [**owner** *name*]

To remove RMON MIB statistics collection on an interface, use the **no rmon collection statistics** { **controlEntry** *integer* } command.

Parameters

controlEntry *integer* Enter the keyword **controlEntry** to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON Statistic Table.

owner *name* (OPTIONAL) Enter the keyword **owner** followed by the owner name to record the owner of the RMON group of statistics.

Defaults No default behavior

Command Modes CONFIGURATION INTERFACE (config-if)

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 event

C **E** **S**

Add an event in the RMON event table.

Syntax **rmon event** *number* [**log**] [**trap community**] [**description string**] [**ownername**]

To disable RMON on an interface, use the **no rmon event** *number* [**log**] [**trap community**] [**description string**] command.

Parameters

<i>number</i>	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

C **E** **S**

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

<i>number</i>	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.
<i>variable</i>	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.
<i>interval</i>	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds
delta	Enter the keyword delta to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.

absolute Enter the keyword **absolute** to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.

rising-threshold value event-number Enter the keyword **rising-threshold** followed by the value (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.

falling-threshold value event-number 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.

owner string (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.

Defaults owner

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

show rmon

C **E** **S**

Display the RMON running status including the memory usage.

Syntax **show rmon**

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

```

FTOS# show rmon
RMON status
  total memory used 218840 bytes.
  ether statistics table: 8 entries, 4608 bytes
  ether history table: 8 entries, 6000 bytes
  alarm table: 390 entries, 102960 bytes
  high-capacity alarm table: 5 entries, 1680 bytes
  event table: 500 entries, 206000 bytes
  log table: 2 entries, 552 bytes
FTOS#

```

show rmon alarms

C **E** **S** 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
(show rmon
alarms index)

```
FTOS#show rmon alarm 1
RMON alarm entry 1
  sample Interval: 5
  object: 1.3.6.1.2.1.1.3
  sample type: absolute value.
  value: 255161
  alarm type: rising or falling alarm.
  rising threshold: 1, RMON event index: 1
  falling threshold: 501, RMON event index: 501
  alarm owner: 1
  alarm status: OK
FTOS#
```

Example 2
(show rmon
alarms brief)

```
FTOS#show rmon alarm br
index          SNMP OID
-----
1              1.3.6.1.2.1.1.3
2              1.3.6.1.2.1.1.3
3              1.3.6.1.2.1.1.3
4              1.3.6.1.2.1.1.3
5              1.3.6.1.2.1.1.3
6              1.3.6.1.2.1.1.3
7              1.3.6.1.2.1.1.3
8              1.3.6.1.2.1.1.3
9              1.3.6.1.2.1.1.3
10             1.3.6.1.2.1.1.3
11             1.3.6.1.2.1.1.3
12             1.3.6.1.2.1.1.3
13             1.3.6.1.2.1.1.3
14             1.3.6.1.2.1.1.3
15             1.3.6.1.2.1.1.3
16             1.3.6.1.2.1.1.3
17             1.3.6.1.2.1.1.3
18             1.3.6.1.2.1.1.3
19             1.3.6.1.2.1.1.3
20             1.3.6.1.2.1.1.3
21             1.3.6.1.2.1.1.3
22             1.3.6.1.2.1.1.3
FTOS#
```

show rmon events

C **E** **S** 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

- 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
(show rmon event index)

```
FTOS#show rmon event 1
RMON event entry 1
  description: 1
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner: 1
  event status: OK
FTOS#
```

Example 2
(show rmon event brief)

```
FTOS#show rmon event br
index      description
-----
1          1
2          2
3          3
4          4
5          5
6          6
7          7
8          8
9          9
10         10
11         11
12         12
13         13
14         14
15         15
16         16
17         17
18         18
19         19
20         20
21         21
22         22
FTOS#
```

show rmon hc-alarm

C **E** **S** 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

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
(show rmon hc-alarm brief)

```
FTOS#show rmon hc-alarm brief
index          SNMP OID
-----
1              1.3.6.1.2.1.1.3
2              1.3.6.1.2.1.1.3
3              1.3.6.1.2.1.1.3
4              1.3.6.1.2.1.1.3
5              1.3.6.1.2.1.1.3
FTOS#
```

Example 2
(show rmon hc-alarm index)

```
FTOS#show rmon hc-alarm 1
RMON high-capacity alarm entry 1
  object: 1.3.6.1.2.1.1.3
  sample interval: 5
  sample type: absolute value.
  value: 185638
  alarm type: rising or falling alarm.
  alarm rising threshold value: positive.
  rising threshold: 1001, RMON event index: 1
  alarm falling threshold value: positive.
  falling threshold: 999, RMON event index: 6
  alarm sampling failed 0 times.
  alarm owner: 1
  alarm storage type: non-volatile.
  alarm status: OK
FTOS#
```


show rmon history

C **E** **S** 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

- Version 7.6.1.0 Support added for S-Series
- Version 6.1.1.0 Introduced for E-Series

Example 1
(show rmon history index)

```
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#
```

Example 2
(show rmon history brief)

```
FTOS#show rmon history brief
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#
```

show rmon log

C **E** **S** Display the contents of RMON Log Table.

Syntax `show rmon log [index] [brief]`

Parameters

index (OPTIONAL) Enter the log index number to display just that entry.

brief (OPTIONAL) Enter the keyword **brief** to display the RMON Log Table in an easy-to-read format.

Defaults 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
(show rmon log index)

```
FTOS#show rmon log 2
RMON log entry, alarm table index 2, log index 1
    log time: 14638 (THU AUG 12 22:10:40 2004)
    description: 2
FTOS#
```

Example 2
(show rmon log brief)

```
FTOS#show rmon log br
eventIndex      description
-----
2                2
4                4
FTOS#
```

Usage Information The log table has a maximum of 500 entries. If the log exceeds that maximum, the oldest log entry is purged to allow room for the new entry.

show rmon statistics

C **E** **S** Display the contents of RMON Ethernet Statistics table.

Syntax `show rmon statistics [index] [brief]`

Parameters

index (OPTIONAL) Enter the index number to display just that entry.

brief (OPTIONAL) Enter the keyword **brief** to display the RMON Ethernet Statistics table in an easy-to-read format.

Defaults 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
(show mon
statistics index)**

```

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
(show rmon
statistics brief)**

```

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 FTOS 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 FTOS on all Dell Force10 systems, as indicated by the characters that appear below each command heading:

- C-Series: **C**
- E-Series: **E**
- S-Series: **S**

Commands

The FTOS 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

C **E** **S** Set the bridge priority for RSTP.

Syntax **bridge-priority** *priority-value*

To return to the default value, enter **no bridge-priority**.

Parameters *priority-value* Enter a number as the bridge priority value in increments of 4096.
Range: 0 to 61440.
Default: 32768

Defaults 32768

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 [protocol spanning-tree rstp](#) Enter the Rapid Spanning Tree mode

debug spanning-tree rstp

C **E** **S** Enable debugging of RSTP and view information on the protocol.

Syntax **debug spanning-tree rstp** [**all** | **bpdu** *interface* {**in** | **out**} | **events**]

To disable debugging, enter **no debug spanning-tree rstp**.

Parameters

all (OPTIONAL) Enter the keyword **all** to debug all spanning tree operations.

bpdu *interface* (OPTIONAL) Enter the keyword **bpdu** to debug Bridge Protocol Data Units.

{**in** | **out**} (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 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
	Version 7.5.1.0	Support added for C-Series
	Version 6.2.1.1	Introduced for E-Series
Example	<pre>FTOS#debug spanning-tree rstp bpdu gigabitethernet 2/0 ? in Receive (in) out Transmit (out)</pre>	

description

C **E** **S**

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

C **E** **S**

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 7.6.1.0 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

C **E** **S**

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 FTOS waits before transitioning RSTP to the forwarding state.
Range: 4 to 30
Default: 15 seconds

Defaults 15 seconds

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 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

C **E** **S**

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

Usage Information

The hello time is encoded in BPDUs in increments of 1/256ths of a second. The standard minimum hello time in seconds is 1 second, which is encoded as 256. Millisecond hello times are encoded using values less than 256; the millisecond hello time equals (x/1000)*256.

When millisecond hellos are configured, the default hello interval of 2 seconds is still used for edge ports; the millisecond hello interval is not used.

Related Commands

- [forward-delay](#) 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

C **E** **S**

Set the time interval for the RSTP bridge to maintain configuration information before refreshing that information.

Syntax

max-age *seconds*

To return to the default values, enter **no max-age**.

Parameters

max-age Enter a number of seconds the FTOS waits before refreshing configuration information.
Range: 6 to 40 seconds
Default: 20 seconds

Defaults

20 seconds

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

C **E** **S**

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	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
Example	<pre>FTOS(conf)#protocol spanning-tree rstp FTOS(config-rstp)##no disable</pre>	
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

C **E** **S**

View the current configuration for the mode. Only non-default values are displayed.

Syntax **show config**

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History	Version 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

Example

```
FTOS(conf-rstp)#show config
!
protocol spanning-tree rstp
no disable
bridge-priority 16384
```

show spanning-tree rstp

C **E** **S**

Display the RSTP configuration.

Syntax **show spanning-tree rstp [brief] [guard]**

Parameters	brief	(OPTIONAL) Enter the keyword brief to view a synopsis of the RSTP configuration information.
	guard	(OPTIONAL) Enter the keyword guard to display the type of guard enabled on an RSTP interface and the current port state.

Command Modes EXEC
EXEC Privilege

Command History

Version 8.4.2.1 The optional **guard** keyword was added.
 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 (show spanning-tree rstp brief)

```
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	Designated Bridge ID	PortID
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#
```

Example 2 (show spanning-tree rstp with EDS and LBK)

```
FTOS#show spanning-tree rstp br
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root
Configured hello time 2, max age 20, forward delay 15
```

Interface Name	PortID	Prio	Cost	Sts	Cost	Designated Bridge ID	PortID
Gi 0/0	128.257	128	20000	EDS	0	32768 0001.e801.6aa8	128.257

```
Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge
-----
Gi 0/0 ErrDis 128.257 128 20000 EDS 0 P2P No
```

```
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
Port path cost 20000, Port priority 128, Port Identifier 128.257
```

```

Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU : sent 27, received 9
The port is not in the Edge port mode

```

Example 3
(show
spanning-tree
rstp guard)

```

FTOS#show spanning-tree rstp guard
Interface
Name          Instance    Sts          Guard type
-----
Gi 0/1        0          INCON(Root)  Rootguard
Gi 0/2        0          FWD          Loopguard
Gi 0/3        0          BLK          Bpduguard

```

Table 52-144. show spanning-tree rstp guard Command Information

Field	Description
Interface Name	RSTP interface
Instance	RSTP instance
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut)
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard)

spanning-tree rstp



Configure Port cost, Edge port with optional Bridge Port Data Unit (BPDU) guard, or Port priority on the RSTP.

Syntax

spanning-tree rstp { *cost Port cost* | **edge-port** [**bpduguard** [**shutdown-on-violation**]] | **priority** *priority* }

Parameters

cost *Port 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

edge-port

Enter the keyword **edge-port** to configure the interface as a Rapid 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.

priority (OPTIONAL) Enter keyword **priority** followed by a value in increments of 16 as the priority.
priority Range: 0 to 240.
 Default: 128

Defaults Not configured

Command Modes INTERFACE

Command History

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

Usage Information The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an error disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.



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.

Example

```
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




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 for E-Series

Usage Information

By default FTOS implements an optimized flush mechanism for RSTP. This helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, 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 Force10 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 FTOS, 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, refer to the Security chapter in the *FTOS Configuration Guide*.



Note: Starting with FTOS 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 suppress](#)
- [accounting](#)
- [show accounting](#)

aaa accounting



Enable AAA Accounting and create a record for monitoring the accounting function.

Syntax

`aaa accounting {system | exec | commands level} {name | default} {start-stop | wait-start | stop-only} {tacacs+}`

To disable AAA Accounting, use the `no aaa accounting {system | exec | command level} {name | default} {start-stop | wait-start | stop-only} {tacacs+}` command.

Parameters

<code>system</code>	Enter the keyword <code>system</code> to send accounting information of any other AAA configuration.
<code>exec</code>	Enter the keyword <code>EXEC</code> to send accounting information when a user has logged in to the EXEC mode.
<code>commands <i>level</i></code>	Enter the keyword <code>command</code> followed by a privilege level for accounting of commands executed at that privilege level.
<code><i>name</i> default</code>	Enter one of the following: <ul style="list-style-type: none"> For <i>name</i>, a user-defined name of a list of accounting methods <code>default</code> for the default accounting methods
<code>start-stop</code>	Enter the keyword <code>start-stop</code> to send a “start accounting” notice at the beginning of the requested event and a “stop accounting” notice at the end of the event.
<code>wait-start</code>	Enter the keyword <code>wait-start</code> to ensure that the TACACS+ security server acknowledges the start notice before granting the user’s process request.
<code>stop-only</code>	Enter the keyword <code>stop-only</code> to instruct the TACACS+ security server to send a “stop record accounting” notice at the end of the requested user process.
<code>tacacs+</code>	Enter the keyword <code>tacacs+</code> to use TACACS+ data for accounting. FTOS 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+
FTOS (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

enable password	Change the password for the enable command.
login authentication	Enable AAA login authentication on terminal lines.
password	Create a password.
tacacs-server host	Specify a TACACS+ server host.

aaa accounting suppress

C **E** **S**

Prevent the generation of accounting records of users with user name value of NULL.

Syntax `aaa accounting suppress null-username`

To permit accounting records to users with user name value of NULL, use the `no aaa accounting suppress null-username` command

Defaults Accounting records are recorded for all users.

Command Modes CONFIGURATION

Command History

Version 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

FTOS issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the `aaa authentication login method-list none` command is applied. Use `aaa accounting suppress` command to prevent accounting records from being generated for sessions that do not have user names associated to them.

accounting

C **E** **S**

Apply an accounting method list to terminal lines.

Syntax `accounting { exec | commands level } method-list`

Parameters

<i>exec</i>	Enter this keyword to apply an EXEC level accounting method list.
<i>commands level</i>	Enter this keyword to apply an EXEC and CONFIGURATION level accounting method list.
<i>method-list</i>	Enter a method list that you defined using the command <code>aaa accounting exec</code> or <code>aaa accounting commands</code> .

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 accounting](#) Enable AAA Accounting and create a record for monitoring the accounting function.

show accounting

C **E** **S** Display the active accounting sessions for each online user.

Syntax show accounting

Defaults No default configuration or behavior

Command Modes EXEC

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

Example

```
FTOS#show accounting
Active accounted actions on tty2, User admin Priv 1
  Task ID 1, EXEC Accounting record, 00:00:39 Elapsed, service=shell
Active accounted actions on tty3, User admin Priv 1
  Task ID 2, EXEC Accounting record, 00:00:26 Elapsed, service=shell
FTOS#
```

Usage Information This command steps through all active sessions and then displays the accounting records for the active account functions.

Authorization and Privilege Commands

Set command line authorization and privilege levels with the following commands:

- [authorization](#)
- [aaa authorization commands](#)
- [aaa authorization config-commands](#)
- [aaa authorization exec](#)
- [privilege level \(CONFIGURATION mode\)](#)
- [privilege level \(LINE mode\)](#)

authorization

C **E** **S** Apply an authorization method list to terminal lines.

Syntax authorization { *exec* | *commands level* } *method-list*

Parameters

<i>exec</i>	Enter this keyword to apply an EXEC level authorization method list.
<i>commands level</i>	Enter this keyword to apply an EXEC and CONFIGURATION level authorization method list.
<i>method-list</i>	Enter a method list that you defined using the command <code>aaa authorization exec</code> or <code>aaa authorization commands</code> .

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 commands

C **E** **S** 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 }`

Undo a configuration with the **no** `aaa authorization commands level { name | default } { local || tacacs+ || none }` command syntax.

Parameters	<code>commands <i>level</i></code>	Enter the keyword commands followed by the command privilege level for command level authorization.
	<code><i>name</i></code>	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

aaa authorization config-commands

E 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

C **E** **S** 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

<i>name</i>	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

privilege level (CONFIGURATION mode)

C **E** **S** Change the access or privilege level of one or more commands.

Syntax `privilege mode {level level command | reset command}`

To delete access to a level and command, use the `no privilege mode level level command` command.

Parameters

mode Enter one of the following keywords as the mode for which you are controlling access:

- **configure** for the CONFIGURATION mode
- **exec** for the EXEC mode
- **interface** for the INTERFACE modes
- **line** for the LINE mode
- **route-map** for the ROUTE-MAP
- **router** for the ROUTER OSPF, ROUTER RIP, 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

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 the [enable password](#) command to define a password for the level to which you are assigning privilege or access.

privilege level (LINE mode)

C **E** **S** Change the access level for users on the terminal lines.

Syntax `privilege level level`

To delete access to a terminal line, use the `no privilege level level` command.

Parameters

level level Enter the keyword **level** followed by a number for the access level.
Range: 0 to 15.
Level 1 is the EXEC mode and Level 15 allows access to all CLI modes.

Defaults `level = 15`

Command Modes LINE

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

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
<i>method-list-name</i>	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at log in.
<i>method</i>	Enter one of the following methods: <ul style="list-style-type: none">• enable - use the password defined by the enable password command in the CONFIGURATION mode.• line - use the password defined by the password command in the LINE mode.• none - no authentication.• radius - use the RADIUS server(s) configured with the radius-server host command.• tacacs+ - use the TACACS+ server(s) configured with the tacacs-server host command.
... <i>method2</i>	(OPTIONAL) In the event of a “no response” from the first method, FTOS applies the next configured method.

Defaults	Use the enable password.										
Command Modes	CONFIGURATION										
Command History	<table border="0"> <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>Version 6.2.1.1</td> <td>Introduced</td> </tr> </table>	Version 7.6.1.0	Introduced for S-Series	Version 7.5.1.0	Introduced for C-Series	Version 6.2.1.1	Introduced				
Version 7.6.1.0	Introduced for S-Series										
Version 7.5.1.0	Introduced for C-Series										
Version 6.2.1.1	Introduced										
Usage Information	<p>By default, the Enable password is used. If aaa authentication enable default is configured, FTOS will use the methods defined for Enable access instead.</p> <p>Methods configured with the aaa authentication enable command are evaluated in the order they are configured. If authentication fails using the primary method, FTOS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, FTOS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.</p>										
Related Commands	<table border="0"> <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> </table>	enable password	Change the password for the enable command.	login authentication	Enable AAA login authentication on terminal lines.	password	Create a password.	radius-server host	Specify a RADIUS server host.	tacacs-server host	Specify a TACACS+ server host.
enable password	Change the password for the enable command.										
login authentication	Enable AAA login authentication on terminal lines.										
password	Create a password.										
radius-server host	Specify a RADIUS server host.										
tacacs-server host	Specify a TACACS+ server host.										


aaa authentication login

C **E** **S** 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	<p><i>method-list-name</i> 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.</p> <p>default Enter the keyword default to specify that the method list specified is the default method for all terminal lines.</p> <p><i>method</i> Enter one of the following methods:</p> <ul style="list-style-type: none"> • 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. <p><i>... method4</i> (OPTIONAL) Enter up to four additional methods. In the event of a “no response” from the first method, FTOS applies the next configured method (up to four configured methods).</p>
-------------------	---

Default	Not configured (that is, no authentication is performed)	
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 6.2.1.0	Introduced on E-Series
Usage Information	<p>By default, the locally configured <code>username password</code> will be used. If aaa authentication login default is configured, FTOS will use the methods defined by this command for login instead.</p> <p>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 <code>local</code> 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.</p> <hr/> <p> Note: If authentication fails using the primary method, FTOS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, FTOS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.</p> <hr/> <p>After configuring the aaa authentication login command, configure the login authentication command to enable the authentication scheme on terminal lines.</p> <p>Connections to the SSH server will work with the following login mechanisms: local, radius and tacacs.</p>	
Related Commands	login authentication	Apply an authentication method list to designated terminal lines.
	password	Create a password.
	radius-server host	Specify a RADIUS server host.
	tacacs-server host	Specify a TACACS+ server host.

access-class

C **E** **S** 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

C **E** **S** 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	<code>level <i>level</i></code>	(OPTIONAL) Enter the keyword <code>level</code> followed by a number as the level of access. Range: 1 to 15
	<code><i>encryption-type</i></code>	(OPTIONAL) Enter the number <code>7</code> or <code>0</code> as the encryption type. Enter a <code>7</code> 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 <code>SHOW running-config</code> file of another Dell Force10 router.
	<code><i>password</i></code>	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 CTRL + v prior to entering regular expression. For example, to create the password `abcd|e`, you type “`abcd CTRL v |e`”. When the password is created, you do not use the CTRL + v key combination and enter “`abcd|e`”.



Note: The question mark (?) and the tilde (~) are not supported characters.

Related Commands	show running-config	View the current configuration.
	privilege level (CONFIGURATION mode)	Control access to command modes within the switch.

enable restricted

C **E** **S** Allows Dell Force10 technical support to access restricted commands.

Syntax enable restricted [*encryption-type*] *password*

To disallow access to restricted commands, enter no enable restricted.

Parameters

<i>encryption-type</i>	(OPTIONAL) Enter the number 7 as the encryption type. Enter 7 followed a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Force10 router. Use this parameter only with a password that you copied from the show running-config file of another Dell Force10 router.
<i>password</i>	Enter a text string, up to 32 characters long, as the clear text password.

Command Modes Not configured.

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 Only Dell Force10 Technical Support staff use this command.

enable secret

C **E** **S** Change the password for the [enable](#) command.

Syntax enable secret [*level level*] [*encryption-type*] *password*

To delete a password, use the no enable secret [*encryption-type*] *password* [*level level*] command.

Parameters

<i>level level</i>	(OPTIONAL) Enter the keyword level followed by a number as the level of access. Range: 1 to 15
<i>encryption-type</i>	(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 show running-config file of another Dell Force10 router.
<i>password</i>	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 CTRL + v prior to entering regular expression. For example, to create the password **abcd]e**, you type **abcd** CTRL v **]e**. When the password is created, you do not use the CTRL + v key combination and enter **abcd]e**.



Note: The question mark (?) and the tilde (~) are not supported characters.

Related Commands

[show running-config](#)

View the current configuration.

[privilege level \(CONFIGURATION mode\)](#)

Control access to command modes within the E-Series.

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

method-list-name

Enter the *method-list-name* to specify that method list, created in the [aaa authentication login](#) command, to be applied to the designated terminal line.

default

Enter the keyword **default** to specify that the default method list, created in the [aaa authentication login](#) command, is applied to the terminal line.

Defaults

No authentication is performed on the console lines, and local authentication is performed on the virtual terminal and auxiliary lines.

Command Modes

LINE

Command History

Version 7.6.1.0 Introduced for S-Series

Version 7.5.1.0 Introduced for C-Series

pre-Version 6.2.1.0 Introduced on E-Series

Usage Information

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

C **E** **S**

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

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

FTOS 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 FTOS.

[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

C **E** **S**

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 <i>number</i>	(OPTIONAL) Enter the keyword min-length followed by the number of characters. Range: 0 - 32 characters
	max-retry <i>number</i>	(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 <i>number</i>	(OPTIONAL) Enter the keyword upper followed the upper number. Range: 0 - 31
	lower <i>number</i>	(OPTIONAL) Enter the keyword lower followed the lower number. Range: 0 - 31
	numeric <i>number</i>	(OPTIONAL) Enter the keyword numeric followed the numeric number. Range: 0 - 31
	special-char <i>number</i>	(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

C **E** **S** Encrypt all passwords configured in FTOS.

Syntax `service password-encryption`
To store new passwords as clear text, enter `no service password-encryption`.

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



Caution: Encrypting passwords with this command does not provide a high level of security. When the passwords are encrypted, you cannot return them to plain text unless you re-configure them. To remove an encrypted password, use the `no password password` command.

Usage Information

To keep unauthorized people from viewing passwords in the switch configuration file, use the [service password-encryption](#) command. This command encrypts the clear-text passwords created for user name passwords, authentication key passwords, the privileged command password, and console and virtual terminal line access passwords.

To view passwords, use the [show running-config](#) command.

show privilege

C **E** **S** View your access level.

Syntax show privilege

Command Modes

EXEC
EXEC Privilege

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

```
FTOS#show privilege
Current privilege level is 15
FTOS#
```

Related Commands

[privilege level \(CONFIGURATION mode\)](#) Assign access control to different command modes.

show users

C **E** **S** View information on all users logged into the switch.

Syntax show users [all]

Parameters

all (OPTIONAL) Enter the keyword **all** to view all terminal lines in the switch.

Command Modes

EXEC Privilege

Command History

Version 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

```
FTOS#show user
  Line           User           Host(s)      Location
  0 console 0     admin         idle
*  3 vty 1       admin         idle         172.31.1.4
FTOS#
```

Table 1, "show users Command Example Fields," in [Security](#) describes the information in the show users command example.

Table 1 show users Command Example Fields

Field	Description
(untitled)	Indicates with a * which terminal line you are using.
Line	Displays the terminal lines currently in use.
User	Displays the user name of all users logged in.
Host(s)	Displays the terminal line status.
Location	Displays the IP address of the user.

Related Commands

[username](#) Enable a user.

timeout login response

C **E** **S**

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

Refer to parameters above.

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 6.1.1.0	Introduced for E-Series

Usage Information

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

C E S

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

<i>name</i>	Enter a text string for the name of the user up to 63 characters.
<i>access-class</i>	Enter the keyword <code>access-class</code> followed by the name of a configured access control list (either a IP access control list or MAC access control list).
<i>access-list-name</i>	
<code>nopassword</code>	Enter the keyword <code>nopassword</code> to specify that the user should not enter a password.
<code>password</code>	Enter the keyword <code>password</code> followed by the <i>encryption-type</i> or the password.
<code>secret</code>	Enter the keyword <code>secret</code> followed by the <i>encryption-type</i> or the password.
<i>encryption-type</i>	Enter an encryption type for the <i>password</i> that you will enter. <ul style="list-style-type: none">• 0 directs FTOS to store the password as clear text. It is the default encryption type when using the <code>password</code> option.• 7 to indicate that a password encrypted using a DES hashing algorithm will follow. This encryption type is available with the <code>password</code> option only.• 5 to indicate that a password encrypted using an MD5 hashing algorithm will follow. This encryption type is available with the <code>secret</code> option only, and is the default encryption type for this option.
<i>password</i>	Enter a string up to 32 characters long.
<i>privilege level</i>	Enter the keyword <code>privilege</code> followed by a number from zero (0) to 15.
<code>secret</code>	Enter the keyword <code>secret</code> followed by the encryption type.

Defaults

The default encryption type for the `password` option is 0. The default encryption type for the `secret` option is 0.

Command Modes

CONFIGURATION

Command History

Version 7.7.1.0	Added support for <code>secret</code> option and MD5 password encryption. Extended <i>name</i> from 25 characters to 63.
Version 7.6.1.0	Introduced for S-Series
Version 7.5.1.0	Introduced for C-Series
E-Series original Command	

Usage Information

To view the defined user names, use the [show running-config](#) user command.

Related Commands

password	Specify a password for users on terminal lines.
show running-config	View the current configuration.

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

C **E** **S**

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

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

ip radius source-interface

C **E** **S**

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`.

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 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 VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults	Not configured.	
Command Mode	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

radius-server deadline

C **E** **S** Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

Syntax radius-server deadline *seconds*

To disable this function or return to the default value, enter `no radius-server deadline`.

Parameters

seconds Enter a number of seconds during which non-responsive RADIUS servers are skipped.
Range: 0 to 2147483647 seconds.
Default: 0 seconds.

Defaults 0 seconds

Command Modes CONFIGURATION

Command History

Version 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

radius-server host

C **E** **S** 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

login authentication	Set the database to be checked when a user logs in.
radius-server key	Set a authentication key for RADIUS communications.
radius-server retransmit	Set the number of times the RADIUS server will attempt to send information.
radius-server timeout	Set the time interval before the RADIUS server times out.

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

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

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 FTOS tries to locate a RADIUS server.
Range: zero (0) to 100.
Default: 3 retries.

Defaults 3 retries

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

Related Commands	radius-server host	Configure a RADIUS host.
-------------------------	------------------------------------	--------------------------

radius-server timeout

C **E** **S**

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	<i>seconds</i>	Enter the number of seconds between an unsuccessful attempt and the FTOS times out. Range: zero (0) to 1000 seconds. Default: 5 seconds.
-------------------	----------------	--

Defaults 5 seconds

Command Modes CONFIGURATION

Command History	Version 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

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+

C **E** **S** View TACACS+ transactions to assist with troubleshooting.

Syntax debug tacacs+

To disable debugging of TACACS+, enter `no debug tacacs+`.

Defaults Disabled.

Command Modes EXEC Privilege

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

ip tacacs source-interface

C **E** **S** 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`.

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 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 VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Mode CONFIGURATION

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

tacacs-server host

C **E** **S** Specify a TACACS+ host.

Syntax tacacs-server host { *hostname* | *ipv4-address* | *ipv6-address* } [*port number*] [*timeout seconds*] [*key key*]

Parameters

<i>hostname</i>	Enter the name of the TACACS+ server host.
<i>ipv4-address</i> <i>ipv6-address</i>	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X), of the TACACS+ server host.
<i>port number</i>	(OPTIONAL) Enter the keyword <i>port</i> followed by a number as the port to be used by the TACACS+ server. Range: zero (0) to 65535 Default: 49
<i>timeout seconds</i>	(OPTIONAL) Enter the keyword <i>timeout</i> followed by the number of seconds the switch waits for a reply from the TACACS+ server. Range: 0 to 1000 Default: 10 seconds
<i>key key</i>	(OPTIONAL) Enter the keyword <i>key</i> followed by a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the tacacs-server key for the TACACS+ daemon. Configure this parameter last because leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 8.4.1.0	Added support for IPv6
Version 7.7.1.0	Authentication key length increased to 42 characters
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

Usage Information To list multiple TACACS+ servers to be used by the [aaa authentication login](#) command, configure this command multiple times.

If you are not configuring the switch as a TACACS+ server, you do not need to configure the port, timeout and key optional parameters. If you do not configure a key, the key assigned in the [tacacs-server key](#) command is used.

Related Commands

aaa authentication login	Specify the login authentication method.
tacacs-server key	Configure a TACACS+ key for the TACACS server.

tacacs-server key



Configure a key for communication between a TACACS+ server and client.

Syntax tacacs-server key [*encryption-type*] *key*

To delete a key, use the no tacacs-server key *key*

Parameters

encryption-type (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the *key* entered. The options are:

- 0 is the default and means the key is not encrypted and stored as clear text.
- 7 means that the key is encrypted and hidden.

key Enter a text string, up to 42 characters long, as the clear text password. Leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 7.7.1.0	Authentication key length increased to 42 characters
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

Usage Information

The key configured with this command must match the key configured on the TACACS+ daemon.

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.

FTOS supports RADIUS and Active Directory environments using 802.1X Port Authentication.

Important Points to Remember

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

- 802.1X is supported on C-Series, E-Series, 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)

C **E** **S** 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)

C **E** **S** 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

C **E** **S** 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

C **E** **S** 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

C **E** **S** 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

<i>vlan-id</i>	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

C **E** **S** 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

<i>number</i>	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

Related Commands [interface range](#) Configure a range of interfaces

dot1x port-control

C **E** **S** 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

C **E** **S**

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

<i>seconds</i>	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

C **E** **S**

Enable periodic re-authentication of the client.

Syntax dot1x reauthentication [*interval seconds*]
To disable periodic re-authentication, use the `no dot1x reauthentication` command.

Parameters

<i>interval seconds</i>	(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
Version 7.6.1.0 Introduced on C-Series and S-Series
Version 7.4.1.0 Introduced on E-Series

dot1x supplicant-timeout

C **E** **S** 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

C **E** **S** 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 interface

C **E** **S** Display the 802.1X information on an interface.

Syntax 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.

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

```
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

<code>rsa</code>	Enter the keyword <code>rsa</code> followed by the key size to generate a SSHv2 RSA host keys. Range: 1024 to 2048 Default: 1024
<code>rsa1</code>	Enter the keyword <code>rsa1</code> followed by the key size to generate a SSHv1 RSA host keys. Range: 1024 to 2048 Default: 1024

Defaults Key size 1024

Command Modes CONFIGURATION

Command History

Version 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

```

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

ip ssh server	Enable the SSH server.
show crypto	Display SSH host public keys

debug ip ssh

C **E** **S** Enables collecting SSH debug information.

Syntax debug ip ssh {client | server}
 To disable debugging, use the no debug ip ssh {client | server} command.

Parameters

client	Enter the keyword client to enable collecting debug information on the client.
server	Enter the keyword server to enable collecting debug information on the server.

Defaults Disabled on both client and server

Command Modes EXEC

Command History

Version 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 Debug information includes details for key-exchange, authentication, and established session for each connection.

ip scp topdir

C **E** **S**

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

C **E** **S**

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 a 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

C **E** **S** Configure the maximum number of incoming SSH connections per minute.

Syntax ip ssh connection-rate-limit *1-10*

Parameters *1-10* Enter the number of maximum number of incoming SSH connections allowed per minute.
Range: 1 to 10 per minute
Default: 10 per minute

Defaults 10 per minute

Command Modes CONFIGURATION

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

ip ssh hostbased-authentication

C **E** **S** Enable hostbased-authentication for the SSHv2 server.

Syntax ip ssh hostbased-authentication enable

To disable hostbased-authentication for SSHv2 server, use the `no ip ssh hostbased-authentication enable` command.

Parameters *enable* Enter the keyword **enable** to enable hostbased-authentication for SSHv2 server.

Defaults Disable by default

Command Modes CONFIGURATION

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 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

[ip ssh pub-key-file](#)
[ip ssh rhostsfile](#)

Public keys of trusted hosts from a file.

Trusted hosts and users for rhost authentication.

ip ssh key-size

C **E** **S** 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

C **E** **S** 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 *WORD* Enter the file name for the host-based authentication.

Defaults No default behavior or values

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

Example

```
FTOS#conf
FTOS(conf)# ip ssh pub-key-file flash://knownhosts
FTOS(conf)#
```

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/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tKBU3t
ReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqeNxPDpEn
WIMPJi0ds= ashwani@poclab4
```



Note: For rhostfile and pub-key-file, the administrator must FTP the file to the chassis.

Related Commands [show ip ssh client-pub-keys](#) Display the client-public keys used for the host-based authentication.

ip ssh rhostfile

   Specify the rhost file to be used for host-based authorization.

Syntax ip ssh rhostfile { *WORD* }

Parameters *WORD* Enter the rhost file name for the host-based authentication.

Defaults No default behavior or values

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
Example	<pre>FTOS#conf FTOS(conf)# ip ssh rhostsfile flash://shosts FTOS(conf)#</pre>	
Usage Information	<p>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.</p> <p>This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.</p>	



Note: For rhostfile and pub-key-file, the administrator must FTP the file to the switch.

ip ssh rsa-authentication (Config)



Enable RSA authentication for the SSHv2 server.

Syntax ip ssh rsa-authentication enable

To disable RSA authentication, use the no ip ssh rsa-authentication enable command.

Parameters enable Enter the keyword **enable** to enable RSA authentication for the SSHv2 server.

Defaults RSA authentication is disabled by default




Command Modes CONFIGURATION

Command History	Version 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 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

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 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 <i>port-number</i>	(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

Command Modes CONFIGURATION

Command History	Version 7.6.1.0	Introduced for S-Series
	Version 7.5.1.0	Expanded to include specifying SSHv1 or SSHv2; Introduced for C-Series
	pre-Version 6.1.1.0	Introduced for E-Series
Usage Information	This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.	
Example	<pre>FTOS# conf FTOS(conf)# ip ssh server port 45 FTOS(conf)# ip ssh server enable FTOS#</pre>	
Related Commands	show ip ssh	Display the ssh information

show crypto

C **E** **S**

Display the public part of the SSH host-keys.

Syntax show crypto key mypubkey {rsa | rsa1}

Parameters	Key	Enter the keyword key to display the host public key.
	mypubkey	Enter the keyword mypubkey to display the host public key.
	rsa	Enter the keyword rsa to display the host SSHv2 RSA public key.
	rsa1	Enter the keyword rsa1 to display the host SSHv1 RSA public key.

Defaults 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

```
FTOS#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtzkZME/
e8V8smnXR22EJGQhCMkEOkuisa+OILVoMYU1ZKGfj0W5BPCSvF/
x5ifqYFFwUzJNOcsJK7vjSsnmMhChF2YSvXlvTJ6h971FJAQlOsgd0ycpocsF+DNLKfJnx7SAjha
kFQMwGg/g78ZkDT3Ydr8KKjfsI4Bg/WS8B740=
```

```
FTOS#show crypto key mypubkey rsa1
1024 35
1310600154808733989532575153972496578500722064442949636740809356830889610203
1722667988956754966765265006379622189779927609278523638839223055081819166009
9281326164086643457746022192295189039929663345791173742247431553750501676929
6602737906014944340500000151798644256296133857749192360817713410595337600639
13083
FTOS#
```

Usage Information This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

Related Commands [crypto key generate](#) Generate SSH keys.

show ip ssh

C **E** **S** Display information about established SSH sessions.

Syntax show ip ssh

Command Modes EXEC
EXEC Privilege

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
FTOS
```

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

C **E** **S** 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

```
FTOS#show ip ssh client-pub-keys

poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoiethO9G4sNV+ui+DWEc3cgYAcU5LailMU2ODrzhCwyDNp05tKB
U3tReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc+Rs4p2urzV0F4pRKnaXdhf3Lk4D460HZRhVrxqe
NxPDpEnWIMPJi0ds= ashwani@poclab4

FTOS#
```

Usage Information This command displays the contents of the file flash://ADMIN_DIRssh/knownhosts

Related Commands

ip ssh pub-key-file	Configure the file name for the host-based authentication
-------------------------------------	---

show ip ssh rsa-authentication

C **E** **S**

Display the authorized-keys for the RSA authentication.

Syntax show ip ssh rsa-authentication {my-authorized-keys}

Parameters my-authorized-keys Display the RSA authorized keys.

Defaults 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

```
FTOS#show ip ssh rsa-authentication my-authorized-keys
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB1714gFp4r2DRHIvMc1VZd0Sg5GQxRV1y1X1JOMeO6Nd0Wu
YyZrQMM4qJAoBwtneOXfLBcHF3V2hcMIqaZN+CRcnw/
zCmlnCf0+qVTd1oofsea5r09kS0xTp0CNfHXZ3NuGCq9Ov33m9+U9tMwhS8vy8AVxdH4x4km3c3t
5Jvc= freedom@poclalab4
```

FTOS#

Usage Information This command displays the contents of the file flash:/ADMIN_DIR/ssh/authorized-keys.*username*.

Related Commands [ip ssh rsa-authentication \(Config\)](#) Configure the RSA authorized keys.

ssh

C **E** **S**

Open an SSH connection specifying the hostname, username, port number and version of the SSH client.

FTOS supports both inbound and outbound SSH sessions using IPv4 or IPv6 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

Syntax ssh {hostname | ipv4 address | ipv6 address} [-l username | -p port-number | -v {1 | 2}]

Parameters

<i>hostname</i>	(OPTIONAL) Enter the IP address or the hostname of the remote device.
<i>vrf instance</i>	(OPTIONAL) E-Series Only: Enter the keyword vrf following by the VRF Instance name to open a SSH connection to that instance.
<i>ipv4 address</i>	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
<i>ipv6-address prefix-length</i>	(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

Version 7.9.1.0	Introduced VRF
Version 7.6.1.0	Introduced for S-Series
Version 7.5.1.0	Added IPv6 support; Introduced for C-Series
pre-Version 6.1.1.0	Introduced for E-Series

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, refer to the chapters [the ACL VLAN Group chapter](#) and [the Access Control Lists \(ACL\) chapter](#).

- [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

E 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

E 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

<code>ip</code>	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.
<code><i>ip-protocol-number</i></code>	Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
<code><i>source</i></code>	Enter the IP address of the network or host from which the packets were sent.
<code><i>mask</i></code>	(OPTIONAL) Enter a network mask in /prefix format (/x).
<code>any</code>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<code>host <i>ip-address</i></code>	Enter the keyword <code>host</code> followed by the IP address to specify a host IP address.
<code><i>destination</i></code>	Enter the IP address of the network or host to which the packets are sent.
<code>count</code>	(OPTIONAL) Enter the keyword <code>COUNT</code> to count packets processed by the filter.
<code>bytes</code>	(OPTIONAL) Enter the keyword <code>bytes</code> to count only bytes processed by the filter.
<code>log</code>	(OPTIONAL) Enter the keyword <code>log</code> to have the information kept in a Trace-list log file.
<code>order <i>number</i></code>	(OPTIONAL) Enter the keyword <code>order</code> followed by a number from 0 to 7 as the order number.

Defaults Not configured.

Command Modes TRACE LIST

Related Commands

deny tcp	Assign a trace list filter to deny TCP packets.
deny udp	Assign a trace list filter to deny UDP packets.
ip trace-group	Create a trace list.

deny tcp

E 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	<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
	<i>mask</i>	(OPTIONAL) Enter a network mask in /prefix format (/x).
	<i>any</i>	Enter the keyword any to specify that all routes are subject to the filter.
	<i>host ip-address</i>	Enter the keyword host followed by the IP address to specify a host IP address.
	<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"> • 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 <i>port</i> command parameter.)
	<i>port port</i>	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: <ul style="list-style-type: none"> • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
	<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
	<i>count</i>	(OPTIONAL) Enter the keyword count to count packets processed by the filter.
	<i>byte</i>	(OPTIONAL) Enter the keyword byte to count only bytes processed by the filter.
	<i>log</i>	(OPTIONAL) Enter the keyword log to have the information kept in a Trace-list log file.
<i>order number</i>	(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 udp	Assign a trace list filter to deny UDP traffic.

deny udp



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

Syntax `deny udp { source mask | any | host ip-address } [operator port [port]] { destination mask | any | host ip-address } [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	<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
	<i>mask</i>	(OPTIONAL) Enter a network mask in /prefix format (/x).
	<i>any</i>	Enter the keyword any to specify that all routes are subject to the filter.
	<i>host ip-address</i>	Enter the keyword host followed by the IP address to specify a host IP address.
	<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"> • eq = equal to • neq = not equal to • gt = greater than • lt = less than • range = inclusive range of ports
	<i>port port</i>	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535
	<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
	<i>mask</i>	(OPTIONAL) Enter a network mask in /prefix format (/x).
	<i>count</i>	(OPTIONAL) Enter the keyword COUNT to count packets processed by the filter.
	<i>byte</i>	(OPTIONAL) Enter the keyword byte to count only bytes
<i>log</i>	(OPTIONAL) Enter the keyword log to have the information kept in a Trace-list log file.	
<i>order number</i>	(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

E 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

E 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 *trace-list-name* Enter a string up to 16 characters long as the access list name.

Defaults Not configured

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

E 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

<code>ip</code>	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.
<code><i>ip-protocol-number</i></code>	Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header.
<code><i>source</i></code>	Enter the IP address of the network or host from which the packets were sent.
<code><i>mask</i></code>	(OPTIONAL) Enter a network mask in /prefix format (/x).
<code>any</code>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<code>host <i>ip-address</i></code>	Enter the keyword <code>host</code> followed by the IP address to specify a host IP address.
<code><i>destination</i></code>	Enter the IP address of the network or host to which the packets are sent.
<code>count</code>	(OPTIONAL) Enter the keyword <code>COUNT</code> to count packets processed by the filter.
<code>byte</code>	(OPTIONAL) Enter the keyword <code>byte</code> to count only bytes processed by the filter.
<code>log</code>	(OPTIONAL) Enter the keyword <code>log</code> to have the information kept in a Trace-list log file.

Defaults Not configured.

Command Modes TRACE LIST

Related Commands [ip trace-list](#) Create a trace list.
[permit tcp](#) Assign a trace list filter to forward TCP packets.
[permit udp](#) Assign a trace list filter to forward UDP packets.

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

<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	(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 <i>ip-address</i>	Enter the keyword host followed by the IP address to specify a host IP address.
<i>operator</i>	(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 <i>port</i> parameter.)
<i>port port</i>	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
<i>destination</i>	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.
<i>order number</i>	(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

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

<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	(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 <i>ip-address</i>	Enter the keyword host followed by the IP address to specify a host IP address.
<i>operator</i>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none">• 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 <i>port</i> parameter.)
<i>port port</i>	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535
<i>destination</i>	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 <i>number</i>	(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

ip trace-list	Configure a trace list.
permit	Assign a trace list filter to forward IP packets.
permit tcp	Assign a trace list filter to forward TCP packets.

seq

- E** 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

<i>sequence-number</i>	Enter a number from 0 to 65535.
<i>deny</i>	Enter the keyword deny to configure a filter to drop packets meeting this condition.
<i>permit</i>	Enter the keyword permit to configure a filter to forward packets meeting this criteria.
<i>ip-protocol-number</i>	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
<i>ip</i>	Enter the keyword ip to configure a generic IP access list. The keyword ip specifies that the access list will permit all IP protocols.
<i>tcp</i>	Enter the keyword tcp to configure a TCP access list filter.
<i>udp</i>	Enter the keyword udp to configure a UDP access list filter.
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	(OPTIONAL) Enter a network mask in /prefix format (/x).
<i>any</i>	Enter the keyword any to specify that all routes are subject to the filter.
<i>host ip-address</i>	Enter the keyword host followed by the IP address to specify a host IP address.
<i>operator</i>	(OPTIONAL) Enter one of the following logical operands: <ul style="list-style-type: none"> • 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 <i>port</i> parameter.)
<i>port port</i>	(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: <ul style="list-style-type: none"> • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>precedence</i> <i>precedence</i>	Enter the keyword precedence followed by a number from 0 to 7 as the precedence value.
<i>tos tos-value</i>	Enter the keyword tos followed by a number from 0 to 15 as the TOS value.
<i>count</i>	(OPTIONAL) Enter the keyword count to count packets processed by the filter.
<i>byte</i>	(OPTIONAL) Enter the keyword byte to count only bytes processed by the filter.
<i>log</i>	(OPTIONAL) Enter the keyword log to have the information kept in a Trace-list log file.

Defaults Not configured.

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.

show config

E View the current IP trace list configuration.

Syntax show config

Command Modes TRACE LIST

Example

```
FTOS(config-trace-acl)#show config
!
ip trace-list suzanne
 seq 5 deny tcp any any
FTOS(config-trace-acl)#
```

show ip accounting trace-lists

E 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

<i>trace-list-name</i>	(OPTIONAL) Enter the name of the trace list to be displayed.
<i>linecard number</i>	(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 C300 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



```
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 binding](#)
- [ip dhcp snooping database renew](#)
- [ip dhcp snooping trust](#)
- [ip dhcp source-address-validation](#)
- [ip dhcp snooping vlan](#)
- [show ip dhcp snooping](#)

clear ip dhcp snooping

  Clear the DHCP binding table.

Syntax clear ip dhcp snooping binding



Command Modes EXEC Privilege

Default None

Command History Version 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

  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 7.8.1.0 Introduced on C-Series and S-Series

ip dhcp snooping

C **S** Enable DHCP Snooping globally.

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

C **S** 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 7.8.1.0 Introduced on C-Series and S-Series

ip dhcp snooping binding

C **S** 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.

<i>interface type</i>	Enter the keyword interface followed by the type of interface to which the host is connected. <ul style="list-style-type: none"> For an 10/100 Ethernet interface, enter the keyword fastethernet. For a Gigabit Ethernet interface, enter the keyword gigabitethernet. For a SONET interface, enter the keyword sonet. For a Ten Gigabit Ethernet interface, enter the keyword tengigabitethernet.
<i>slot/port</i>	Enter the slot and port number of the interface.
<i>lease time</i>	Enter the keyword lease followed by the amount of time the IP address will be leased. Range: 1-4294967295

Command Modes

EXEC

EXEC Privilege

Default

None

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 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

Default Disabled

Command History Version 7.8.1.0 Introduced on C-Series and S-Series

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 FTOS Configuration Guide Service Provider Bridging chapter.

This chapter includes CLI information for FTOS Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel. L2PT is available in FTOS for the C-Series [\[C\]](#), E-Series [\[E\]](#), and S-Series [\[S\]](#).

L2PT is supported on E-Series ExaScale [\[E\]](#)_X with FTOS 8.2.1.0. and later.

Refer to [Chapter 62, VLAN Stacking](#) or [Chapter 60, Spanning Tree Protocol \(STP\)](#) and [Chapter 22, 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, refer to [Chapter 62, 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

C **E** **S** 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 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.
- 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 8.2.1.0	Introduced on the C-Series, E-Series and E-Series ExaScale.
Version 7.4.1.0	Introduced

protocol-tunnel

C **E** **S** 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

Version 8.2.1.0	Introduced on the C-Series, E-Series and E-Series ExaScale.
Version 7.4.1.0	Introduced




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)#
```

Usage Information  **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

   Overwrite the BPDU destination MAC address with a specific value.

Syntax **protocol-tunnel destination-mac xstp 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

Version 8.2.1.0	Introduced on the C-Series and S-Series.
Version 7.4.1.0	Introduced

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

   Enable protocol tunneling globally on the system.

Syntax **protocol-tunnel enable**

To disable protocol tunneling, use the **no protocol-tunnel enable** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced
-----------------	------------

Usage Information FTOS 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

<i>rate</i>	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

```
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 VLAN.
Range: 1 to 4094

Defaults No default values or behavior

Command Modes EXEC

Command History
Version 8.2.1.0 Introduced on the C-Series, E-Series and E-Series ExaScale.
Version 7.4.1.0 Introduced

Example 1

```
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#
```

Example 2 (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 [show running-config](#) Display the current configuration.

sFlow

Overview

sFlow commands are supported on these platforms: [C](#) [E](#) [S](#).

FTOS sFlow monitoring system includes an sFlow Agent and an sFlow Collector. The sFlow Agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector. The sFlow Collector analyses the sFlow Datagrams received from the different devices and produces a network-wide view of traffic flows.

Important Points to Remember

- Dell Force10 recommends that the sFlow Collector be connected to the Dell Force10 chassis through a line card port rather than the RPM Management Ethernet port.
- FTOS exports all sFlow packets to the sFlow Collector. A small sampling rate can equate to a large number of exported packets. A backoff mechanism 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 (refer to [sflow extended-switch enable](#))
 - 1600 packets when extended-router and/or extended-gateway information packing is enabled (refer to [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*]

Parameters

sflow collector *ipv4-address* | *ipv6-address* Enter the IPv4 (A.B.C.D) or IPv6 address (X: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::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

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

Version 8.4.1.1	On E-series ExaScale, support for IPv6 sFlow collectors and agents was added.
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 6.5.1.0	Expanded the no form of the command to mirror the syntax used to configure
Version 6.2.1.1	Introduced on E-Series

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 only on E-Series ExaScale 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, FTOS will return the corresponding configured agent IP in MIB requests. FTOS checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, FTOS generates the following error:

%Error: Different agent-addr attempted for an existing collector

sflow enable (Global)

C **E** **S** Enable sFlow globally.

Syntax **sflow enable**

To disable sFlow, use the **no sflow enable** command.

Defaults sFlow is disabled by default

Command Modes CONFIGURATION

Command History

Version 8.2.1.0	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

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

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

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.

Related Commands

[sflow enable \(Global\)](#)

Turn sFlow on globally

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.

FTOS 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

```

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

E 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 FTOS 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

C **E** **S** 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	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 7.4.1.0	Introduced on E-Series

Usage Information FTOS 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-router enable	Enable packing information on a router.
show sflow	Display the sFlow configuration

sflow polling-interval (Global)

C **E** **S** Set the sFlow polling interval at a global level.

Syntax **sflow polling-interval *interval value***

To return to the default, use the **no sflow polling-interval *interval*** command.

Parameters ***interval value*** Enter the interval value in seconds.
Range: 15 to 86400 seconds
Default: 20 seconds

Defaults 20 seconds

Command Modes CONFIGURATION

Command History

Version 8.2.1.0	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 [sflow polling-interval \(Interface\)](#) Set the polling interval for an interface

sflow polling-interval (Interface)

C **E** **S** Set the sFlow polling interval at an interface (overrides the global-level setting.)

Syntax **sflow polling-interval** *interval value*

To return to the default, use the **no sflow polling-interval** *interval* command.

Parameters *interval value* Enter the interval value in seconds.
Range: 15 to 86400 seconds
Default: The global counter polling interval

Defaults The same value as the current global default counter polling interval

Command Modes INTERFACE

Command History

Version 8.2.1.0	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 This command sets the counter polling interval for an interface.

Related Commands [sflow polling-interval \(Global\)](#) Globally set the polling interval

sflow sample-rate (Global)

C **E** **S** 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	<p>Version 8.2.1.0 Introduces on S-Series Stacking</p> <p>Version 8.1.1.0 Introduced on E-Series ExaScale</p> <p>Version 7.7.1.0 Introduced on S-Series</p> <p>Version 7.6.1.0 Introduced on C-Series</p> <p>Version 6.2.1.1 Introduced on E-Series</p>
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)

C **E** **S** 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

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

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.

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

```
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

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 example above will always display a value of zero.

show sflow linecard

C **E** **S** 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

```
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 FTOS are:

- [show snmp](#)
- [show snmp engineID](#)
- [show snmp group](#)
- [show snmp user](#)
- [snmp context](#)
- [snmp ifmib ifalias long](#)
- [snmp mib community-map context](#)
- [snmp-server community](#)
- [snmp-server contact](#)
- [snmp-server context](#)
- [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. FTOS supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. FTOS can be configured to send SNMP traps, informing a management system about significant device/network-related events. FTOS supports up to 16 SNMP trap receivers.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both LAN and WAN applications. If you experience a timeout with these values, the recommended best practice on Dell Force10 switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
 - SNMP Timeout—greater than 3 seconds
 - SNMP Retry count—greater than 2 seconds
- If you 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 SNMP statistics.

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

```
FTOS#show snmp
 32685 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
 96988 Number of requested variables
    0 Number of altered variables
 31681 Get-request PDUs
    968 Get-next PDUs
    0 Set-request PDUs
 61727 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    9 No such name errors
    0 Bad values errors
    0 General errors
 32649 Response PDUs
 29078 Trap PDUs
FTOS#
```

Related Commands

[snmp-server community](#)

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

```
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

```
FTOS#show snmp group
groupname: ngroup          security model: v3 auth
  readview : nview        writeview: no write view specified
  notifyview: nview
  row status: active
FTOS#
```

Related Commands [snmp-server group](#) Configure an SNMP server group

show snmp user

C **E** **S** Display the information on each configured SNMP user .

Syntax `show snmp user`

Command Modes EXEC
EXEC Privilege

Example

```
FTOS#show snmp user
  User name: v1v2creadu
  Engine ID: 0000178B02000001E80214A8
  storage-type: nonvolatile          active
  Authentication Protocol: None
  Privacy Protocol: None

FTOS#
```

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

snmp context

E Specify the context name that should be mapped to the OSPF instance.

Syntax `snmp context context-name`

Defaults None

Parameters

context-name Specify the SNMP server context name to be associated with the selected OSPF instance.
Note: There is a 32-character limit for this parameter.

Command Modes CONFIGURATION (ROUTER OSPF)

Example

```
FTOS(conf)#router ospf 248
FTOS(conf-router_ospf-248)# snmp context test
FTOS(conf-router_ospf-248)#
```

Command History

Version 8.4.1.5	Introduced on the ExaScale series.
-----------------	------------------------------------

snmp ifmib ifalias long

C **E** **S**

Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

Syntax `snmp ifmib ifalias long`

Defaults Interface description truncated beyond 63 characters

Command Modes CONFIGURATION

Command History

Version 7.6.1.0	Introduced for S-Series
Version 7.5.1.0	Introduced for C-Series
unknown	Introduced for E-Series

Example

```
!-----command run on host connected to switch: -----!  
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more  
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This  
is a port connected to  
IF-MIB::ifAlias.134792448 = STRING:  
  
!-----command run on Force10 switch: -----!  
FTOS(conf)#snmp ifmib ifalias long  
  
!-----command run on server connected to switch: -----!  
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more  
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This  
is a port connected to Router2. This is a port connected to Router2. This is  
a port connected to Router2. This is a port connected to Router2.  
IF-MIB::ifAlias.134792448 = STRING:
```

snmp mib community-map context

E

Map an SNMP community name with the SNMP context.

Syntax `snmp mib community-map community-name context context-name`

Parameters

<i>community-name</i>	Specify the SNMP community name to be mapped against a context. Note: There is a 20-character limit for this parameter.
<i>context-name</i>	Specify the SNMP context to be mapped with the community. Note: There is a 32-character limit for this parameter.

Defaults None

Command Modes CONFIGURATION

Command History

Version 8.4.1.5	Introduced on the ExaScale series.
-----------------	------------------------------------

snmp-server community



Configure a new community string access for SNMPv1, v2, and v3.

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

<i>community-name</i>	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 an 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.
<i>access-list-name</i>	(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 1

```
FTOS#config
FTOS(conf)# snmp-server community public ro
FTOS(conf)# snmp-server community guest ro security-name guestuser
FTOS(conf)#
```

The **security-name** parameter maps the community string to an SNMPv3 user/security name as defined by the community MIB.

If a community string is configured without a **security-name** (for example, `snmp-server community public ro`), the community is mapped to a default security-name/group:

- `v1v2creadu / v1v2creadg` — maps to a community with **ro** permissions
- `v1v2cwriteu / v1v2cwriteg` — maps to a community with **rw** permissions

This command is indexed by the *community-name* parameter.

If the `snmp-server community` is not configured, you cannot interact with the switch through SNMP. 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 2

```
FTOS(conf)# ip access-list standard snmp-ro-acl
FTOS(config-std-nacl)#seq 5 permit host 10.10.10.224
FTOS(config-std-nacl)#seq 10 deny any count
!
```

```
FTOS(conf)#snmp-server community guest ro snmp-ro-acl
FTOS(conf)#
```



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.

**Related
Commands**

- [ip access-list standard](#) Name (or select) a standard access list to filter based on IP address.
- [ipv6 access-list](#) Configure an access list based on IPv6 addresses or protocols.
- [show running-config snmp](#) Display the current SNMP configuration and defaults.

snmp-server contact



Configure system contact information for this SNMP node.

Syntax `snmp-server contact text`

To delete the SNMP server contact information, use the **no snmp-server contact** command.

Parameters `text` Enter an alphanumeric text string, up to 55 characters long.

Defaults No default values or behavior

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

snmp-server context

E Define a new SNMP context.

Syntax `snmp-server context context-name`

Parameters *context-name* Specify the SNMP server context name.
Note: There is a 32-character limit for this parameter.

Defaults None

Command Modes CONFIGURATION

Command History Version 8.4.1.5 Introduced on the ExaScale series.

snmp-server enable traps

C **E** **S** 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 Enter the type of notification from the list below:

- **bgp**—Notification of changes in BGP process
- **envmon**—For Dell Force10 Networks, device notifications when an environmental threshold is exceeded
- **ldp**—Notification of MPLS LDP traps.
- **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+

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 Version 8.4.1.0 Support was added for VRRP traps.
 Version 7.6.1.0 Support added for S-Series; Added support for STP and xSTP traps.

Version 7.5.1.0 Support added for C-Series
E-Series legacy command

Usage Information

FTOS 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

C **E** **S**

Configure name for both the local and remote SNMP engines on the router.

Syntax

snmp-server engineID [**local engineID**] [**remote ip-address udp-port port-number engineID**]

To return to the default, use the **no snmp-server engineID** [**local engineID**] [**remote ip-address udp-port port-number engineID**] command

Parameters

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.

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 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}}] [context context-name] [read name] [write name] [notify name] [access 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}}][context context-name] [read name] [write name] [notify name] [access access-list-name | ipv6 access-list-name]` command.

Parameters

<i>group_name</i>	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. <ul style="list-style-type: none"> <code>v1v2creadg</code> — maps to a community/security-name with ro permissions <code>1v2cwriteg</code> — maps to a community/security-name rw permissions
1 2c 3	(OPTIONAL) Enter the security model version number (1 , 2c , or 3). <ul style="list-style-type: none"> 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.
context context-name	Enter the keyword context followed by the SNMP context name to specify the context name that should be mapped to the OSPF instance.
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 access-list-name	(Optional) Enter the standard IPv4 access list name (a string up to 140 characters long).
ipv6 access-list-name	(Optional) Enter the keyword ipv6 followed by the IPv6 access list name (a string up to 140 characters long)

Defaults As defined above

Command Modes CONFIGURATION

Command History

Version 8.4.1.5 Support added for **context** *context-name* parameter
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 specifies the group named **harig** as a version **3** user requiring both authentication and encryption and read access limited to the read named **rview**.



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

```
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* | **host** *host 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* [**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 are 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

host Enter the keyword **host** followed by the name of the host for destination lookup.

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.
<i>community-string</i>	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 <i>port-number</i>	(OPTIONAL) Enter the keywords udp-port followed by the port number of the remote host to use. Range: 0 to 65535. Default: 162
<i>notification-type</i>	(OPTIONAL) Enter one of the following keywords for the type of trap to be sent to the host: <ul style="list-style-type: none"> • bgp - BGP state change • envmon - Environment monitor trap • ldp - MPLS LDP traps • 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

Version 8.4.1.0	Support was added for VRRP traps.
Version 7.6.1.0	Support added for S-Series; Added support for STP and xSTP notification types.
Version 7.5.1.0	Support added for C-Series E-Series legacy command

Usage Information

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

[snmp-server enable traps](#)
[snmp-server community](#)

Enable SNMP traps.
Configure a new community SNMPv1 or SNMPv2c

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

text Enter an alpha-numeric text string, up to 55 characters long.

Defaults

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
E-Series legacy command

snmp-server packetsize

C **E** **S**

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, 24000 bytes, and 32000 bytes.

Defaults 8

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

snmp-server trap-source

C **E** **S**

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 VLAN interface, enter the keyword **vlan** followed by the VLAN interface number.

Defaults The IP address assigned to the management interface is the default.

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 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 udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access 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 udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv password] [access access-list-name | ipv6 access-list-name]` command.

Parameters

<i>name</i>	Enter the name of the user (not to exceed 20 characters), on the host, that connects to the agent.
<i>group_name</i>	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. <ul style="list-style-type: none">• <code>v1v2creadu</code> — maps to a community with ro permissions• <code>v1v2cwriteu</code> — maps to a community rw permissions
<i>remote ip-address</i>	Enter the keyword remote followed by the IP address that identifies the copy of the SNMP on the <i>remote</i> device.
<i>udp-port port-number</i>	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	Enter the security model version number (1 , 2c , or 3). <ul style="list-style-type: none">• 1 is the least secure version• 3 is the most secure of the security modes.• 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. Default: 1
encrypted	(OPTIONAL) Enter the keyword encrypted to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
auth	(OPTIONAL) Enter the keyword auth to specify authentication of a packet without encryption.
md5 sha	(OPTIONAL) Enter the keyword md5 or sha to designate the authentication level. md5 — Message Digest Algorithm sha — Secure Hash Algorithm
<i>auth-password</i>	(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).
<i>priv password</i>	(OPTIONAL) Enter a text string (up to 20 characters long) password that will enables the host to encrypt the contents of the message it sends to the agent. Minimum: 8 characters long
access access-list-name	(Optional) Enter the standard IPv4 access list name (a string up to 140 characters long).
ipv6 access-list-name	(Optional) Enter the keyword ipv6 followed by the IPv6 access list name (a string up to 140 characters long)

Defaults	As above
Command Modes	CONFIGURATION
Command History	<p>Version 7.6.1.0 Support added for S-Series</p> <p>Version 7.5.1.0 Support added for C-Series</p> <p>E-Series legacy command</p>
Usage Information	<p> 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.</p> <p>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.</p> <p>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:</p>
Examples	<pre>FTOS# snmp-server user privuser v3group 3 encrypted auth md5 9fc53d9d908118b2804fe80e3ba8763d priv des56 d0452401a8c3ce42804fe80e3ba8763d</pre> <p>The following command is an example of how to enter a plain-text password as the string authpasswd for user authuser of group v3group.</p> <pre>FTOS#conf FTOS(conf)# snmp-server user authuser v3group 3 auth md5 authpasswd</pre> <p>The following command configures a remote user named n3user with a v3 security model and a security level of authNOPriv.</p> <pre>FTOS#conf FTOS(conf)# snmp-server user n3user ngroup remote 172.31.1.3 udp-port 5009 3 auth md5 authpasswd</pre> <p> Note: The number of configurable users is limited to 16.</p>
Related Commands	<p>show snmp user Display the information configured on each SNMP user name.</p>

snmp-server view

C **E** **S**

Configure an SNMPv3 view.

Syntax `snmp-server view view-name oid-tree { included | excluded }`

To remove an SNMPv3 view, use the **no snmp-server view *view-name oid-tree* { **included** | **excluded** }** command.

Parameters

view-name Enter the name of the view (not to exceed 20 characters).
oid-tree Enter the OID sub tree for the view (not to exceed 20 characters).
included (OPTIONAL) Enter the keyword **included** to include the MIB family in the view.
excluded (OPTIONAL) Enter the keyword **excluded** to exclude the MIB family in the view.

Defaults 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

Usage Information

The *oid-tree* variable is a full sub-tree starting from 1.3.6 and can not specify the name of a sub-tree or a MIB. The following example configures a view named **rview** that allows access to all objects under 1.3.6.1:

Example

```
FTOS# conf
FTOS#(conf) snmp-server view rview 1.3.6.1 included
```

Related Commands

[show running-config snmp](#) Display the SNMP running configuration

snmp trap link-status

C **E** **S**

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 **no snmp trap link-status**.

Defaults Enabled.

Command Modes INTERFACE

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

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 Force10 switches:

- [clear logging](#)
- [default logging buffered](#)
- [default logging console](#)
- [default logging monitor](#)
- [default logging trap](#)
- [logging](#)
- [logging buffered](#)
- [logging console](#)
- [logging facility](#)
- [logging history](#)
- [logging history size](#)
- [logging monitor](#)
- [logging on](#)
- [logging source-interface](#)
- [logging synchronous](#)
- [logging trap](#)
- [show logging](#)
- [terminal monitor](#)

clear logging

C **E** **S**

Clear the messages in the logging buffer.

Syntax `clear logging`

Defaults None.

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
E-Series legacy command	

Related Commands [show logging](#) Display logging settings and system messages in the internal buffer.

default logging buffered

C **E** **S** Return to the default setting for messages logged to the internal buffer.

Syntax **default logging buffered**

Defaults size = 40960; level = 7 or debugging

Command Modes CONFIGURATION

Command History
Version 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 [logging buffered](#) Set the logging buffered parameters.

default logging console

C **E** **S** Return the default settings for messages logged to the console.

Syntax **default logging console**

Defaults level = 7 or debugging

Command Modes CONFIGURATION

Command History
Version 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 [logging console](#) Set the logging console parameters.

default logging monitor

C **E** **S** Return to the default settings for messages logged to the terminal.

Syntax **default logging monitor**

Defaults level = 7 or debugging

Command Modes CONFIGURATION

Command History
Version 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 [logging monitor](#) Set the logging monitor parameters.
[terminal monitor](#) Send system messages to the terminal/monitor.

default logging trap

C **E** **S**

Return to the default settings for logging messages to the Syslog servers.

Syntax **default logging trap**

Defaults level = 6 or informational

Command Modes CONFIGURATION

Command History

Version 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

logging trap	Limit messages logged to the Syslog servers based on severity.
------------------------------	--

logging

C **E** **S**

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* }

To disable logging, enter **no logging**.

Parameters

<i>ipv4-address</i> <i>ipv6-address</i>	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) address.
<i>hostname</i>	Enter the name of a host already configured and recognized by the switch.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 8.4.1.0	Added support for IPv6.
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

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

C **E** **S**

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

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 decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.

Related Commands

[clear logging](#) Clear the logging buffer.

[default logging buffered](#) Returns the logging buffered parameters to the default setting.

[show logging](#) Display the logging setting and system messages in the internal buffer.

logging console

C **E** **S**

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

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

[clear logging](#) Clear logging buffer.
[default logging console](#) Returns the logging console parameters to the default setting.
[show logging](#) Display logging settings and system messages in the internal buffer.

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)
- daemon (system daemons)
- 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	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	logging	Enable logging to a Syslog server.
	logging on	Enables logging.

logging history

C **E** **S** 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**.

Parameters	<i>level</i>	Indicate a value from 0 to 7 or enter one of the following equivalent words: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 4.
-------------------	--------------	--

Defaults 4 or warnings

Command Modes CONFIGURATION

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 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

C **E** **S** 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	<i>size</i>	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	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 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

C **E** **S** Specify which messages are logged to Telnet applications.

Syntax **logging monitor** [*level*]

To disable logging to terminal connections, enter **no logging monitor**.

Parameters *level* Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
The default is 7 or debugging.

Defaults 7 or debugging

Command Modes CONFIGURATION

Command History	Version 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

C **E** **S** 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

C **E** **S** 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 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 VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults 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

E-Series legacy command

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

C **E** **S**

Synchronize unsolicited messages and FTOS output.

Syntax **logging synchronous** [**level** *level* | **all**] [**limit** *number-of-buffers*]

To disable message synchronization, use the **no logging synchronous** [**level** *level* | **all**] [**limit** *number-of-buffers*] command.

Parameters

all Enter the keyword **all** to ensure that all levels are printed asynchronously.

level *level* Enter the keyword **level** followed by a number as the severity level. A high number indicates a low severity level and visa versa.
Range: 0 to 7.
Default: 2

all Enter the keyword **all** to turn off all

limit *number-of-buffers* Enter the keyword **limit** followed by the number of buffers to be queued for the terminal after which new messages are dropped
Range: 20 to 300
Default: 20

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

C **E** **S**

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

level Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
The default is 6.

Defaults	6 or informational
Command Modes	CONFIGURATION
Command History	Version 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	logging Enable the logging to another device. logging on Enables logging.

show logging

C **E** **S** 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	<p>number (OPTIONAL) Enter the number of message to be displayed on the output. Range: 1 to 65535</p> <p>history (OPTIONAL) Enter the keyword history to view only information in the Syslog history table.</p> <p>reverse (OPTIONAL) Enter the keyword reverse to view the Syslog messages in FIFO (first in, first out) order.</p> <p>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.</p>
-------------------	---

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 1 (show logging)

```

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 192.200.13.2 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 1.1.14.2 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 1.1.11.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.5 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 192.1.1.4 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: Neighbor 1.1.10.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Session closed by neighbor 1.1.10.2 (Hold time
expired)
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.14.7 Up
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor 1.1.11.2 closed. Neighbor
recycled
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor 1.1.14.2 closed. Neighbor
recycled
--More--

```

Example 2 (show logging history)

```

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#

```

terminal monitor

C **E** **S** Configure the FTOS to display messages on the monitor/terminal.

Syntax **terminal monitor**

To return to default settings, enter **terminal no monitor**.

Defaults Disabled.

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

Related Commands [logging monitor](#) Set the logging parameters on the monitor/terminal.

SONET

Overview

FTOS 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](#)
- [encap](#)
- [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

E 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

E Specify which POS/SDH alarms to report to the remote SNMP server.

Syntax **alarm-report** { **lais** | **lrldi** | **pais** | **plop** | **prdi** | **sd-ber** | **sf-ber** | **slof** | **slos** }

To disable an alarm, use the **no alarm-report** { **lais** | **lrldi** | **pais** | **plop** | **prdi** | **sd-ber** | **sf-ber** | **slof** | **slos** } command.

Parameters

lais	Enter the keyword lais to report line alarm indication signal.
lrldi	Enter the keyword lrldi to report line remote defect indicator.
pais	Enter the keyword pais to report path alarm indication signal.
plop	Enter the keyword plop to report path loss of pointer.
prdi	Enter the keyword prdi to report the path remote defect indication.
sd-ber	Enter the keyword sd-ber to report signal degradation BER errors.
sf-ber	Enter the keyword sf-ber to report signal failure BER errors.
slof	Enter the keyword slof to report section loss of frame.
slos	Enter the keyword slos to report section loss of signal.

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 57-145. Alarm Definitions

Alarm	Description
lais	Line Alarm Indication Signal
lrldi	Line Remote Defect Indication
pais	Path Alarm Indication Signal

Table 57-145. Alarm Definitions

Alarm	Description
plop	Path loss of Pointer
prdi	Path Remote Defect Indication
sd-ber	LBIP BER in excess of Signal Degradation threshold. The default SD alarm value is 10 ⁻⁶ , this value can not be changed.
sf-ber	LBIP BER in excess of Signal Failure threshold. The default SF alarm value is 10 ⁻³ , this value can not be changed.
slof	Section Loss of Frame
slos	Section Loss of Signal

Related Commands

[show controllers](#)

Display alarms and defects

clock source

(E) 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

internal Enter the keyword **internal** to use the internal clock from the interface.
line Enter the keyword **line** to use the recovered clock from the interface. This is the default.

Defaults `line`

Command Modes INTERFACE

debug ppp

(E) Display traffic and information in a Point-to-Point Protocol (PPP) network.

Syntax `debug ppp [authentication | error | negotiation | packet] interface sonet slot/port`

To disable debugging, enter **no debug ppp**.

Parameters	authentication	(OPTIONAL) Enter the keyword authentication to display PPP authentication exchanges (Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges) and traffic.
	error	(OPTIONAL) Enter the keyword error to display PPP error statistics and protocol errors.
	negotiation	(OPTIONAL) Enter the keyword negotiation to display PPP settings negotiated at startup.
	packet	(OPTIONAL) Enter the keyword packet to display low-level packet dumps.
	interface sonet slot/ port	Enter the keywords interface sonet followed by the slot and port information.
	Command Modes	EXEC Privilege
Usage Information	If you enter debug ppp without parameters, all parameters are enabled.	

delay triggers

E 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	line	Enter the keyword line to delay the specified line alarm.
	lrdi	(OPTIONAL) Enter the keyword lrdi to specify line remote defect indicator.
	sd-ber	(OPTIONAL) Enter the keyword sd-ber to specify signal degradation BER errors.
	sf-ber	(OPTIONAL) Enter the keyword sf-ber to specify signal failure BER errors.
	path	Enter the keyword path to delay the specified path alarm.
	pais	(OPTIONAL) Enter the keyword pais to specify path alarm indication signal.
	prdi	(OPTIONAL) Enter the keyword prdi to specify the path remote defect indication.

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

E 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

E Configure encapsulation for a PPP interface.

Syntax **encap ppp**

To remove encapsulation, enter **no encap**.

Parameters **ppp** Enter the keyword **ppp** for Point-to-Point Protocol encapsulation.

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

E 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.

Parameters

c2 value Enter the keyword **c2** followed by value to set the path signal byte.
Range: 0x00 to 0xFF hexadecimal (0-255 decimal)
Default: 0xCF in hexadecimal (207 in decimal)

j0 value Enter the keyword **j0** to set the section trace byte.
Range: 0x00 to 0xFF hexadecimal (0-255 decimal)
Default: 0xCC (204 in decimal)

Defaults as above

Command Modes INTERFACE

Usage Information You enter the flag C2 and J0 values in decimal, but the FTOS displays the values in hexadecimal in the **show controllers sonet** command output.

framing

E Set the type of framing used on a POS/SDH interface.

Syntax **framing {sdh | sonet}**

To return to the default, enter **no framing**.

Parameters

sdh Enter the keyword **sdh** to specify Synchronous Digital Hierarchy (SDH) framing.
Default: Sonet

sonet Enter the keyword **sonet** to specify SONET framing.
Default: Sonet

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

E 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

E 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	<pre>FTOS(conf)#interface sonet 8/2 FTOS(conf-if-so-8/2)#</pre>
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

E Send SONET 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 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

E Troubleshoot a POS/SDH interface by looping back traffic through the interface or the line.

Syntax **loopback** {**internal** | **line**}

To delete a loopback setting, use the **no loopback** {**internal** | **line**} command.

Parameters

internal Enter the keyword **internal** to test the physical interface by sending incoming traffic back through the interface.

line Enter the keyword **line** to test connectivity to the network by sending incoming traffic back to the network.

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

E 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**.

Parameters	chap	Enter the keyword chap to enable CHAP authentication only.
	chap pap	Enter the keywords chap pap to enable CHAP on one side and PAP on the other.
	pap	Enter the keyword pap to enable PAP authentication only.
	pap chap	Enter the keywords pap chap to enable PAP on one side and CHAP on the other side.

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: <ul style="list-style-type: none"> • 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	ppp chap hostname	Configure a hostname for CHAP authentication.
	ppp chap password	Configure a password for CHAP authentication.
	ppp chap rem-hostname	Configure a remote hostname for CHAP authentication.
	ppp chap rem-password	Configure a remote password for CHAP authentication.
	ppp pap hostname	Configure a hostname for PAP authentication.
	ppp pap password	Configure a password 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 chap hostname

E 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

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap password	Configure a password for CHAP authentication.
ppp chap rem-hostname	Configure a remote hostname for CHAP authentication.
ppp chap rem-password	Configure a remote password for CHAP authentication.

ppp chap password

E 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

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

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap hostname	Configure a hostname for CHAP authentication.
ppp chap rem-hostname	Configure a remote hostname for CHAP authentication.
ppp chap rem-password	Configure a remote password for CHAP authentication.

ppp chap rem-hostname

E 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 *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

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap rem-password	Configure a remote password for CHAP authentication.
ppp chap hostname	Configure a hostname for CHAP authentication.
ppp chap password	Configure a password for CHAP authentication.

ppp chap rem-password

E Configure a remote password for CHAP authentication.

Syntax `ppp chap rem-password password`

To remove a password, enter **no ppp chap rem-password**.

Parameters *password* Enter a character string up to 32 characters long.

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

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap rem-hostname	Configure a remote host name for CHAP authentication.
ppp chap hostname	Configure a hostname for CHAP authentication.
ppp chap password	Configure a password for CHAP authentication.

ppp next-hop

E 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 *ip-address* Enter an IP address in dotted decimal format (A.B.C.D).

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

E Configure a host name for PAP authentication.

Syntax `ppp pap hostname name`

To delete a host name, enter **no ppp pap 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, 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 password	Configure a password 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 password

E 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 host name 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

E 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

E Configure a remote PAP password.

Syntax `ppp pap rem-password password`

To delete a remote PAP password, enter **no ppp pap rem-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 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

E Enable POS/SDH payload scrambling on the interface.

Syntax **scramble-atm**

To disable scrambling, enter **no scramble-atm**.

Defaults Disabled

Command Modes INTERFACE

Usage Information You must either enable payload scrambling or disable scrambling on both ends of the link.

show controllers

E Display troubleshooting information, such as the clock source, SONET alarms and error rates, and registers values.

Syntax **show controllers** *interface*

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

Command History Version 7.4.2.0 Added support for Ten Gigabit Ethernet

Example 1 (show controllers sonet)

```
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

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#
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#

```

Example 2
(show controllers
tengigabitethernet)

Table 57-146. Lines in show controllers *interface* Command Example

Line	Description
interface is...	Displays the interface type and the slot and port number information.
SECTION	Displays the section loss of frame (LOF) error.
LOF	This error is detected when a severely error framing (SEF) defect on the incoming interface signal persist for 3 milliseconds
LOS	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.
BIP(B1)	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.

Table 57-146. Lines in show controllers *interface* Command Example (Continued)

Line	Description
LINE	Displays the alarm indication signal.
AIS	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.
RDI	Displays remote defect indication. This indication is reported by the downstream LTE when it detects LOF, LOS, or AIS conditions.
BIP(B2)	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.
PATH	Displays the alarm indication signal.
AIS	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.
RDI	Displays remote defect indication. This indication is reported by the downstream LTE when it detects LOF, LOS, or AIS conditions.
BIP(B3)	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.
Active Defects:	Lists the current interface defects.
Active Alarms	List the current interface alarms as enforced the interface Alarm Hierarchy.
Alarm reporting enabled for:	List the alarms enabled. Enabled alarms generate trap reports.

show interfaces

E Display detailed information on the Sonet or 10-Gigabit Ethernet interfaces.

Syntax `show interfaces interface`

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

```

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 Oc48
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 57-147. Fields in the show interfaces sonet with PPP Encapsulation

Field	Description
Sonet 2/0...	Displays the interface's type, slot/port and physical and line protocol status.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Encapsulation is...	Displays the encapsulation method, the framing, and if the ais-shut command is enabled.
Scramble-ATM is enabled	States whether the scramble-atm and the down-when-looped commands are enabled.
Loopback is...	States whether the loopback , clock source , and speed , and flag commands are configured. This information is displayed over 2 lines.
Keepalive Set	Displays the number of seconds between keepalive messages.
LCP State:	States if LCP was successfully negotiated.
IPCP State:	States if IPCP was successfully negotiated.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
Peer address	Displays the PPP peer's IP address.
MTU 1554...	Displays link and IP MTU.
LineSpeed	Displays interface's line speed.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the show interfaces counters were cleared.
Queueing strategy.	States the packet queuing strategy. FIFO means first in first out.
0 packets...	Displays the number of packets and bytes into the interface.

Table 57-147. Fields in the show interfaces sonet with PPP Encapsulation

Field	Description
Input 0 IP packets...	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.
0 64-byte...	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.
Received 0...	Displays the type and number of error or other specific packets received. This information is displayed over 3 lines.
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over 2 lines.
Time since...	Displays the time since the last change in the configuration of this interface.

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

- E** Recovery interval to automatically clear a condition that could cause a SONET port to hang, and stop sending and receiving data.

Syntax `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

Command History
Version 7.7.1.0 Introduced

Usage Information When enabled, FTOS 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

E Set the speed of the SONET interface.

Syntax `speed { 155 | 622 | 2488 }`

To return to the default value, enter **no speed**.

Parameters

155 Enter **155** to set the interface as OC3.

622 Enter **622** to set the interface as OC12.

2488 Enter **2488** to set the interface as OC48.

Defaults

2488

Command Modes

INTERFACE

Command History

Version 7.4.1.0 Added support for 2488 (OC48)

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, refer to the chapter “Stacking S-Series Switches” in the *FTOS Configuration Guide*.



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](#)
- [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



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 CONFIGURATION

Command History

Version 8.3.1.0	Added the all option
Version 7.7.1.0	Introduced on S-Series

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.

reset stack-unit

S Reset any designated stack member except the management unit (master unit).

Syntax `reset stack-unit 0-7 hard`

Parameters

<code>0-7</code>	Enter the stack member unit identifier of the stack member to reset.
<code>hard</code>	Reset the stack unit if the unit is in a problem state.

Default none

Command Modes CONFIGURATION

Command History

Version 8.3.1.0	Added hard reset option.
Version 7.8.1.0	Augmented to run on the standby unit in order to reset the standby unit directly.
Version 7.7.1.0	Introduced on S-Series

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 FTOS 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

```
FTOS#show system brief

Stack MAC : 00:01:e8:51:4e:f8
```

```
-- Stack Info --
Unit  UnitType   Status      ReqTyp      CurTyp      Version     Ports
-----
  0   Member      online      S50N        S50N        4.7.7.117   52
  1   Member      online      S50N        S50N        4.7.7.117   52
  2   Member      online      S50N        S50N        4.7.7.117   52
  3   Member      online      S50N        S50N        4.7.7.117   52
  4   Standby     online      S50N        S50N        4.7.7.117   52
  5   Member      online      S50N        S50N        4.7.7.117   52
  6   Mgmt       online      S50N        S50N        4.7.7.117   52
  7   Member      online      S50N        S50N        4.7.7.117   52
```

```
FTOS(standby)#reset ? <<Standby management unit
stack-unit           Unit number
FTOS(standby)#reset stack-unit ?
<0-7>                Unit number id
FTOS(standby)#reset stack-unit 6
% Error: Reset of master unit is not allowed.
FTOS(standby)#reset stack-unit 0
```

```

% Error: Reset of stack units from standby is not allowed.<<no reset of other mem-
ber
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**

reload	Reboot FTOS.
upgrade (S-Series management unit)	Reset the designated S-Series stack member.

show redundancy

S 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

```

FTOS#show redundancy

FTOS#show redundancy

-- SSeries 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

[redundancy disable-auto-reboot](#)

Prevent the system from auto-rebooting if it fails.

show system stack-ports

S Display information about the stacking ports on all switches in the S-Series stack.

Syntax `show system stack-ports [status | topology]`

Parameters

status (OPTIONAL) Enter the keyword **status** to display the command output without the Connection field.

topology (OPTIONAL) Enter the keyword **topology** to limit the table to just the Interface and Connection fields.

Defaults

No default behavior

Command Modes

EXEC

EXEC Privilege

Command History

Version 7.7.1.0 Introduced on S-Series

Example 1 (show system stack-ports)

```
FTOS# show system stack-ports
```

```
Topology: Ring
```

Interface	Connection	Link Speed (Gb/s)	Admin Status	Link Status
0/49	1/49	12	up	up
0/50		12	up	down
0/51	2/49	24	up	up
1/49	0/49	12	up	up
1/50	2/51	12	up	up
2/49	0/51	24	up	up
2/51	1/50	12	up	up
2/52		12	up	down

```
FTOS#
```

Example 2
(show system stack-ports status)

```
FTOS# show system stack-ports status
Topology: Ring

Interface    Link Speed      Admin    Link
              (Gb/s)         Status   Status
-----
0/49         12              up       up
0/50         12              up       down
0/51         24              up       up
1/49         12              up       up
1/50         12              up       up
2/49         24              up       up
2/51         12              up       up
2/52         12              up       down
FTOS#
```

Example 3
(show system stack-ports topology)

```
FTOS# show system stack-ports topology
Topology: Ring

Interface    Connection
-----
0/49         1/49
0/50
0/51         2/49
1/49         0/49
1/50         2/51
2/49         0/51
2/51         1/50
2/52
FTOS#
```

Table 58-148. show interfaces description Command Example Fields

Field	Description
Topology	Lists the topology of stack ports connected: Ring, Daisy chain, or Standalone
Interface	The unit/port ID of the connected stack port on this unit
Link Speed	Link Speed of the stack port (12 or 24) in Gb/s
Admin Status	The only currently listed status is Up.
Connection	The stack port ID to which this unit's stack port is connected

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.

stack-unit priority

S 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

<code>0-7</code>	Enter the stack member unit identifier, from 0 to 7, of the switch on which you want to set the management priority.
<code>1-14</code>	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

reload	Reboot FTOS.
show system (S-Series)	Display the current status of all stack members or a specific member.

stack-unit provision

S 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

<code>0-7</code>	Enter a stack member identifier, from 0 to 7, of the switch that you want to add to the stack.
<code>S25N S25P S25V S50N S50V</code>	Enter the S-Series model identifier of the switch to be added as a stack member. This identifier is also referred to as the <i>provision type</i> .

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 FTOS.
show system (S-Series)	Display the current status of all stack members or a specific member.

stack-unit renumber

S 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 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.

Example `S50V_7.7#stack-unit 0 renumber 2`

Renumbering master unit will reload the stack. Proceed to renumber [confirm yes/no]:

Related Commands

reload	Reboot FTOS.
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.

upgrade system stack-unit (S-Series stack member)

S Copy the boot image or FTOS 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 FTOS 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 FTOS after using the **upgrade** command.

Related Commands

- [reload](#) Reboot FTOS.
- [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 FTOS 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 FTOS 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 Force10 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

C **E** **S** 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 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 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 1 (E-Series)

```
FTOS#show storm-control broadcast gigabitethernet 11/11
Broadcast storm control configuration
Interface          Direction          Percentage          Wred Profile
-----
Gi 11/11           Ingress            5.6
Gi 11/11           Egress             5.6                 -
FTOS#
```

Example 2 (C-Series)

```
FTOS#show storm-control broadcast gigabitethernet 3/24
Broadcast storm control configuration
Interface          Direction          Packets/Second
-----
Gi 3/24           Ingress            1000
FTOS#
```

show storm-control multicast

C **S** 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.

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

Example FTOS#show storm-control multicast gigabitethernet 1/0

```
Multicast storm control configuration

Interface          Direction          Packets/Second
-----
Gi 1/0             Ingress            5

FTOS#
```

show storm-control unknown-unicast

C **E** **S** 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 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 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			
	Interface	Direction	Percentage	Wred Profile
	-----	-----	-----	-----
Gi 11/1	Ingress	5.9	-	
Gi 11/1	Egress	5.7	w8	
	FTOS#			
Example C-Series	FTOS#show storm-control unknown-unicast gigabitethernet 3/0			
	Unknown-unicast storm control configuration			
	Interface	Direction	Packets/Second	
	-----	-----	-----	
Gi 3/0	Ingress	1000		
	FTOS#			

storm-control broadcast (Configuration)

C **E** **S** 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	<i>percentage decimal_value</i> 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: .1 to .9
	wred-profile name	E-Series Only: (Optionally) Enter the keyword wred-profile followed by the profile name to designate a wred-profile.
	<i>packets_per_second</i> 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)

C **E** **S**

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.

Parameters

percentage decimal_value in

E-Series Only: Enter the percentage of broadcast traffic allowed in to 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: .1 to .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

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)

C E S

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

<i>percentage decimal_value [in out]</i>	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: .1 to .9
wred-profile name	E-Series Only: (Optionally) Enter the keyword wred-profile followed by the profile name to designate a wred-profile.
<i>packets_per_second in</i>	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
Version 7.4.1.0	E-Series Only: Added percentage decimal value option
Version 6.5.1.0	Introduced on E-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 in to 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: .1 to .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 Force10 switch/routing platforms, as indicated by the **C**, **E**, and **S** characters under the command headings:

Commands

- [bridge-priority](#)
- [bpdu-destination-mac-address](#)
- [debug spanning-tree](#)
- [description](#)
- [disable](#)
- [forward-delay](#)
- [hello-time](#)
- [max-age](#)
- [protocol spanning-tree](#)
- [show config](#)
- [show spanning-tree 0](#)
- [spanning-tree](#)

bridge-priority

C **E** **S** 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

bpdu-destination-mac-address

C **S** Use the Provider Bridge Group address in Spanning Tree or GVRP PDUs.

Syntax **bpdu-destination-mac-address** [**stp** | **gvrp**] **provider-bridge-group**

Parameters

xstp 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.
-----------------	--------------------------------------

debug spanning-tree

C **E** **S** Enable debugging of Spanning Tree Protocol and view information on the protocol.

Syntax **debug spanning-tree** { *stp-id* [**all** | **bpdu** | **config** | **events** | **exceptions** | **general** | **root**] | *protocol* }

To disable debugging, enter **no debug spanning-tree**.

Parameters

stp-id Enter zero (0). The switch supports one Spanning Tree group with a group ID of 0.

protocol Enter the keyword for the type of STP to debug, either **mstp**, **pvst**, or **rstp**.

all (OPTIONAL) Enter the keyword **all** to debug all spanning tree operations.

bpdu (OPTIONAL) Enter the keyword **bpdu** to debug Bridge Protocol Data Units.

config (OPTIONAL) Enter the keyword **config** to debug configuration information.

events (OPTIONAL) Enter the keyword **events** to debug STP events.

general (OPTIONAL) Enter the keyword **general** to debug general STP operations.

root (OPTIONAL) Enter the keyword **root** to debug STP root transactions.

Command Modes EXEC Privilege

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

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

C **E** **S**

Enter a description of the Spanning Tree

Syntax **description** { *description* }

To remove the description from the Spanning Tree, 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 (The prompt is “config-stp”.)

Command History

pre-7.7.1.0	Introduced
-------------	------------

Related Commands [protocol spanning-tree](#) Enter SPANNING TREE mode on the switch.

disable

C **E** **S**

Disable Spanning Tree Protocol globally on the switch.

Syntax **disable**

To enable Spanning Tree Protocol, enter **no disable**.

Defaults Enabled (that is, Spanning Tree Protocol is disabled.)

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](#) Enter SPANNING TREE mode.

forward-delay

C **E** **S**

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 the FTOS waits before transitioning STP to the forwarding state.
Range: 4 to 30
Default: 15 seconds.

Defaults	15 seconds	
Command Modes	SPANNING TREE	
Command History	Version 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	max-age	Change the wait time before STP refreshes protocol configuration information.
	hello-time	Change the time interval between BPDUs.

hello-time

C **E** **S**

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	<i>seconds</i>	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

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	forward-delay	Change the wait time before STP transitions to the Forwarding state.
	max-age	Change the wait time before STP refreshes protocol configuration information.

max-age

C **E** **S**

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	<i>seconds</i>	Enter a number of seconds the FTOS waits before refreshing configuration information. Range: 6 to 40 Default: 20 seconds.
-------------------	----------------	---

Defaults	20 seconds						
Command Modes	SPANNING TREE						
Command History	<table> <tr> <td>Version 7.7.1.0</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 6.2.1.1</td> <td>Introduced on E-Series</td> </tr> </table>	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
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	<table> <tr> <td>forward-delay</td> <td>Change the wait time before STP transitions to the Forwarding state.</td> </tr> <tr> <td>hello-time</td> <td>Change the time interval between BPDUs.</td> </tr> </table>	forward-delay	Change the wait time before STP transitions to the Forwarding state.	hello-time	Change the time interval between BPDUs.		
forward-delay	Change the wait time before STP transitions to the Forwarding state.						
hello-time	Change the time interval between BPDUs.						

protocol spanning-tree

C **E** **S** 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

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

```
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

C **E** **S** Display the current configuration for the mode. Only non-default values are displayed.

Syntax **show config**

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

Example

```
FTOS(config-stp)#show config
protocol spanning-tree 0
  no disable
FTOS(config-stp)#
```

show spanning-tree 0

C **E** **S** Display the Spanning Tree group configuration and status of interfaces in the Spanning Tree group.

Syntax **show spanning-tree 0** [**active** | **brief** | **interface** *interface* | **root** | **summary**] [**guard**]

Parameters

0 Enter **0** (zero) to display information about that specific Spanning Tree group.

active (OPTIONAL) Enter the keyword **active** to display only active interfaces in Spanning Tree group 0.

brief (OPTIONAL) Enter the keyword **brief** to display a synopsis of the Spanning Tree group configuration information.

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 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.

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.

guard (OPTIONAL) Enter the keyword **guard** to display the type of guard enabled on an STP interface and the current port state.

Command Modes EXEC Privilege

Usage Information You must enable Spanning Tree group 0 prior to using this command.

Command History

Version 8.4.2.1 The optional **guard** keyword was added.
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 1
(show spanning-tree 0)

```
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
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 27 (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
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 28 (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
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:31, received 0
The port is not in the portfast mode

```

FTOS#

Table 60-149. show spanning-tree 0 Command Information

Field	Description
"Bridge Identifier..."	Lists the bridge priority and the MAC address for this STP bridge.
"Configured hello..."	Displays the settings for hello time, max age, and forward delay.
"We are..."	States whether this bridge is the root bridge for the STG.
"Current root..."	Lists the bridge priority and MAC address for the root bridge.
"Topology flag..."	States whether the topology flag and the detected flag were set.
"Number of..."	Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.
"Timers"	Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.

Table 60-149. show spanning-tree 0 Command Information

Field	Description
“Times”	List the number of seconds since the last: <ul style="list-style-type: none"> • hello time • topology change • notification • aging
“Port 1...”	Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).
“Port path...”	Displays the path cost, priority, and identifier for the interface.
“Designated root...”	Displays the priority and MAC address of the root bridge of the STG that the interface belongs.
“Designated port...”	Displays the designated port ID

Example 2
(show
spanning-tree 0
brief)

```

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
Name          PortID Prio Cost Sts Cost      Designated
-----
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#

```

Example 3
(show
spanning-tree 0
guard)

```

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          BLK          Bpduguard

```

Table 60-150. show spanning-tree 0 guard Command Example Information

Field	Description
Interface Name	STP interface
Instance	STP 0 instance
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut)
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard)

spanning-tree



Configure Spanning Tree group id, cost, loop guard, priority, Portfast, and root guard for an interface.

Syntax `spanning-tree stp-id [cost cost] [loopguard | rootguard] [portfast [bpduguard [shutdown-on-violation]]] [priority priority]`

Parameters

- stp-id*** Enter the Spanning Tree Protocol group ID.
Range: 0
- cost cost*** (OPTIONAL) 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
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
- [loopguard]** (OPTIONAL) Enter the keyword **loopguard** to enable STP loop guard on a port or port-channel interface.
- priority priority*** (OPTIONAL) Enter keyword **priority** followed by a number as the priority.
Range: zero (0) to 15. Default: 8
- portfast** (OPTIONAL) Enter the keyword **portfast** to enable Portfast to move the interface into forwarding mode immediately after the root fails.
- [bpduguard**
shutdown-on-violation]] Enter the keyword **bpduguard** to disable the port when it receives a BPDU.
Enter the keyword **shutdown-on-violation** to hardware disable an interface when a BPDU is received and the port is disabled.
- [rootguard]** (OPTIONAL) Enter the keyword **rootguard** to enable STP root guard on a port or port-channel interface.

Defaults *cost* = depends on the interface type; *priority* = 8

Command Modes INTERFACE

Command History

- Version 8.4.2.0 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

Usage Information

If you enable **portfast bpduguard** on an interface and the interface receives a BPDU, the software disables the interface and sends a message stating that fact. The port is in ERR_DISABLE mode, yet appears in the **show interface** commands as enabled. If **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. When you configure loop guard on a port, an existing root guard configuration is disabled. When you configure root guard on a port, an existing loop guard configuration is disabled.

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 FTOS, 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, refer to the “Network Time Protocol” section of the Management chapter in the *FTOS 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 master](#)
- [ntp multicast client](#)
- [ntp server](#)
- [ntp source](#)
- [ntp trusted-key](#)
- [ntp update-calendar](#)
- [show calendar](#)
- [show clock](#)
- [show ntp associations](#)
- [show ntp status](#)

calendar set



Set the time and date for the switch hardware clock.

Syntax `calendar set time month day year`

Parameters

time Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, for example, 17:15:00 is 5:15 pm.

month Enter the name of one of the 12 months in English.
You can enter the name of a day to change the order of the display to *time day month year*.

day Enter the number of the day.
Range: 1 to 31.
You can enter the name of a month to change the order of the display to *time day month year*.

year Enter a four-digit number as the year.
Range: 1993 to 2035.

Command Modes EXEC Privilege

Command History

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#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`

Defaults Not configured.

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

Usage Information 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	<i>time</i>	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.
	<i>month</i>	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 <i>time day month year</i> .
	<i>day</i>	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 <i>time month day year</i> .
	<i>year</i>	Enter a four-digit number as the year. Range: 1993 to 2035.

Defaults Not configured

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

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 [ntp update-calendar](#) Set the switch using the NTP settings.

clock summer-time date



Set a date (and time zone) on which to convert the switch to daylight savings time on a one-time basis.

Syntax

clock summer-time *time-zone date start-month start-day start-year start-time end-month end-day end-year end-time [offset]*

To delete a daylight savings time zone configuration, enter no clock summer-time.

Parameters

<i>time-zone</i>	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
<i>start-month</i>	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 <i>time day month year</i> .
<i>start-day</i>	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 <i>time day month year</i> .
<i>start-year</i>	Enter a four-digit number as the year. Range: 1993 to 2035.
<i>start-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format, example, 17:15 is 5:15 pm.
<i>end-day</i>	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 <i>time day month year</i> .
<i>end-month</i>	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 <i>time day month year</i> .
<i>end-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format, example, 17:15 is 5:15 pm.
<i>end-year</i>	Enter a four-digit number as the year. Range: 1993 to 2035.
<i>offset</i>	(OPTIONAL) Enter the number of minutes to add during the summer-time period. Range: 1 to 1440. Default: 60 minutes

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

Version 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

calendar set	Set the hardware clock.
clock summer-time recurring	Set a date (and time zone) on which to convert the switch to daylight savings time each year.
show clock	Display the current clock settings.

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.
- end-time*** Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.
- offset*** (OPTIONAL) Enter the number of minutes to add during the summer-time period.
Range: 1 to 1440.
Default: 60 minutes.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

- | | |
|---------------------|---|
| Version 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 <i>start-day</i> and <i>end-day</i> options to allow for using the three-letter abbreviation of the weekday name. |
| pre-Version 6.1.1.0 | Introduced for E-Series |

Related Commands	calendar set	Set the hardware clock.
	clock summer-time date	Set a date (and time zone) on which to convert the switch to daylight savings time on a one-time basis.
	show clock	Display the current clock settings.

clock timezone

C **E** **S** Configure a timezone for the switch.

Syntax `clock timezone timezone-name offset`
To delete a timezone configuration, enter `no clock timezone`.

Parameters

<i>timezone-name</i>	Enter the name of the timezone. You cannot use spaces.
<i>offset</i>	Enter one of the following: <ul style="list-style-type: none"> 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
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

C **E** **S** Set the switch hardware clock based on the software clock.

Syntax `clock update-calendar`

Defaults Not configured.

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

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

C **E** **S**

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

C **E** **S**

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

Syntax

`ntp authenticate`

To disable NTP authentication, enter `no ntp authenticate`.

Defaults

Not 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
pre-Version 6.1.1.0	Introduced for E-Series

Usage Information

You also must configure an authentication key for NTP traffic using the [ntp authentication-key](#) command.

Related Commands

[ntp authentication-key](#)
[ntp trusted-key](#)

Configure authentication key for NTP traffic.
Configure a key to authenticate

ntp authentication-key

C **E** **S** Specify a key for authenticating the NTP server.

Syntax ntp authentication-key *number* md5 [0 | 7] *key*

Parameters

number Specify a number for the authentication key.
Range: 1 to 4294967295.
This number must be the same as the number parameter configured in the [ntp trusted-key](#) command.

md5 Specify that the authentication key will be encrypted using MD5 encryption algorithm.

0 Specify that authentication key will be entered in an unencrypted format (default).

7 Specify that the authentication key will be entered in DES encrypted format.

key Enter the authentication key in the previously specified format.

Defaults NTP authentication is not configured by default. If you do not specify the option [0 | 7], 0 is selected by default.

Command Modes CONFIGURATION

Command History

Version 8.2.1.0	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

Usage Information After configuring the [ntp authentication-key](#) command, configure the [ntp trusted-key](#) command to complete NTP authentication.

FTOS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous FTOS versions; beginning in version 8.2.1.0, FTOS uses DES encryption to store the key in the startup-config when you enter the command `ntp authentication-key`. Therefore, if your system boots with a startup-configuration from an FTOS versions prior to 8.2.1.0 in which you have configured `ntp authentication-key`, the system cannot correctly decrypt the key, and cannot authenticate NTP packets. In this case you must re-enter this command and save the running-config to the startup-config.

Related Commands

ntp authenticate	Enables NTP authentication.
ntp trusted-key	Configure a trusted key.

ntp broadcast client

C **E** **S** 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	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 master



Enable the system to act as an NTP (network time protocol) server.

Syntax ntp master {*stratum*}

Parameters

<i>stratum</i>	Define the distance from the reference clock. Range: 2 to 15 Default: 8
----------------	---

Default 8

Command Modes CONFIGURATION

Command History	Version 8.4.1.4	Introduced for E-Series
------------------------	-----------------	-------------------------

Usage Information Use this command to enable the system to act as an authoritative time server to downstream clients. The commands ntp server and ntp master can be enabled simultaneously to allow the system to act as a bridge to downstream clients if the local clock fails.

ntp disable



Prevent an interface from receiving NTP packets.

Syntax ntp disable

To re-enable NTP on an interface, enter no ntp disable.

Default Disabled (that is, if an NTP host is configured, all interfaces receive NTP packets)

Command Modes INTERFACE

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 multicast client

E 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::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

Version 8.4.1.0	Added support for IPv6 multicast addresses.
pre-Version 6.1.1.0	Introduced for E-Series

ntp server

C E S Configure an NTP time-serving host.

Syntax ntp server {*hostname* | *ipv4-address* | *ipv6-address*} [*key keyid*] [prefer] [*version number*]

Parameters

<i>ipv4-address</i> <i>ipv6-address</i>	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).
<i>hostname</i>	Enter the hostname of the server.
<i>key keyid</i>	(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.
<i>version number</i>	(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

Version 8.4.1.0	Added IPv6 support.
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 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.

**Related
Commands**

[show ntp associations](#)

Displays NTP servers configured and their status.

ntp source

C **E** **S**

Specify an interface's IP address to be included in the NTP packets.

Syntax

ntp 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 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 VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults

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
pre-Version 6.1.1.0	Introduced for E-Series

ntp trusted-key

C **E** **S**

Set a key to authenticate the system to which NTP will synchronize.

Syntax

ntp trusted-key *number*

To delete the key, use the `no ntp trusted-key number` command.

Parameters

number Enter a number as the trusted key ID.
Range: 1 to 4294967295.

Defaults

Not configured.

Command Modes	CONFIGURATION	
Command History	Version 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 <i>number</i> parameter in the ntp trusted-key command must be the same number as the <i>number</i> 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

C **E** **S** 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 *minutes* (OPTIONAL) Enter the number of minutes between updates from NTP to the hardware clock.
Range: 1 to 1440.
Default: 60 minutes.

Defaults Not enabled.

Command Modes CONFIGURATION

Command History

Version 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

show calendar

C **E** **S** 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
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

C **E** **S** 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 1 (show clock)
FTOS#show clock
11:05:56.949 UTC Thu Oct 25 2001
FTOS#

Example 2 (show clock detail)
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](#) Set the software clock to convert to daylight savings time on a specific day each year.
[show calendar](#) Display the time and date from the switch hardware clock.

show ntp associations

C **E** **S** 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

```

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 (syncd), # master (unsyncd), + selected, - candidate
FTOS#

```

Table 61-151. show ntp associations Command Fields

Field	Description
(none)	One or more of the following symbols could be displayed: <ul style="list-style-type: none"> * means synchronized to this peer # means almost synchronized to this peer + means the peer was selected for possible synchronization - means the peer is a candidate for selection ~ means the peer is statically configured
remote	Displays the remote IP address of the NTP peer.
ref clock	Displays the IP address of the remote peer's reference clock.
st	Displays the peer's stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source.
when	Displays the last time the switch received an NTP packet.
poll	Displays the polling interval (in seconds).
reach	Displays the reachability to the peer (in octal bitstream).
delay	Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
offset	Displays the relative time of the NTP peer's clock to the switch clock (in milliseconds).
disp	Displays the dispersion.

Related Commands

[show ntp status](#) Display current NTP status.

show ntp status

C **E** **S** Display the current NTP status.

Syntax show ntp status

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

```
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 61-152. show ntp status Command Example Information

Field	Description
“Clock is...”	States whether or not the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.
“frequency is...”	Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
“reference time is...”	Displays the reference time stamp.
“clock offset is...”	Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.
“root dispersion is...”	Displays the root and path dispersion.
“peer mode is...”	State what NTP mode the switch is. This should be client mode.

Related Commands [show ntp associations](#) Display information on NTP master and peer configurations.

VLAN Stacking

Overview

With the VLAN-Stacking feature (also called Stackable VLANs and *QinQ*), available on all Dell Force10 platforms (C-Series [C](#), E-Series [E](#), and S-Series [S](#)) that are supported by this version of FTOS, you can “stack” VLANs into one tunnel and switch them through the network transparently.

VLAN Stacking is supported on E-Series ExaScale [E](#)[X](#) with FTOS 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, refer to [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, refer to [Chapter 54, 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 FTOS 7.8.1 for C-Series and S-Series (FTOS 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. Refer to [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 FTOS 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.

Usage Information You must first enable DEI for this configuration to take effect.

Related Commands [dei enable](#) Make packets eligible for dropping based on their DEI value.

dei mark



Set the DEI value on egress according to the color currently assigned to the packet.

Syntax `dei mark {green | yellow} {0 | 1}`

Parameters

`0 | 1` Enter the bit value you want to map to a color.
`green | 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.

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.

Related Commands [dei enable](#) Make packets eligible for dropping based on their DEI value.

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 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 Not configured.

Command Mode CONF-IF-VLAN

Command History Version 8.2.1.0 Introduced on the E-Series ExaScale
Version 7.6.1.0 Support added for C-Series and S-Series
E-Series original Command

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

C **S** Display the dei honor configuration.

Syntax show interface dei-honor [*interface slot/port* | *linecard number port-set number*]

Parameters

<i>interface slot/port</i>	Enter the interface type followed by the line card slot and port number.
<i>linecard number port-set number</i>	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 8.3.1.0 Introduced on C-Series and S-Series.

Example FTOS#show interface dei-honor

```
Default Drop precedence: Green
Interface          CFI/DEI          Drop precedence
-----
Gi 0/1             0                 Green
Gi 0/1             1                 Yellow
Gi 8/9             1                 Red
Gi 8/40            0                 Yellow
```

Related Commands [dei honor](#) Honor the incoming DEI value by mapping it to an FTOS drop precedence.

show interface dei-mark

C **S** Display the dei mark configuration.

Syntax show interface dei-mark [*interface slot/port* | *linecard number port-set number*]

Parameters

<i>interface slot/port</i>	Enter the interface type followed by the line card slot and port number.
<i>linecard number port-set number</i>	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 8.3.1.0 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 mark](#) Set the DEI value on egress according to the color currently assigned to the packet.

vlan-stack access

C **E** **S** 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

Version 8.2.1.0	Introduced on the E-Series ExaScale
Version 7.6.1.0	Support added for C-Series and S-Series
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

C **E** **S** 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

Version 8.2.1.0	Introduced on the E-Series ExaScale
Version 7.6.1.0	Support added for C-Series and S-Series
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.

```
FTOS#show vlan
```

```
Codes: * - Default VLAN, G - GVRP VLANs
```

	NUM	Status	Q Ports
*	1	Inactive	
	2	Active	M Gi 13/13 M Gi 13/0-2
	3	Active	M Po1(Gi 13/14-15) M Gi 13/18 M Gi 13/3
	4	Active	M Po1(Gi 13/14-15) M Gi 13/18 M Gi 13/4
	5	Active	M Po1(Gi 13/14-15) M Gi 13/18 M Gi 13/5

```
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 <i>value</i>	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 <i>value</i>	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 *VLAN tag*). If you do not configure this command, FTOS assigns the value 0x9100.

Syntax `vlan-stack protocol-type number`

Parameters

- number* Enter the hexadecimal number as the Stackable VLAN tag.
- On the E-Series: FTOS accepts the Most Significant Byte (MSB) and then appends zeros for the Least Significant Byte (LSB).
E-Series Range: 0-FF
 - On the C-Series and S-Series: You may specify both bytes of the 2-byte S-Tag TPID.
C-Series and S-Series Range: 0-FFFF
Default: 9100

Defaults 0x9100

Command Modes CONFIGURATION

Command History

- Version 8.2.1.0 Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.
- Version 8.2.1.0 Introduced on the E-Series ExaScale
- Version 7.6.1.0 Support added for C-Series and S-Series
- E-Series original Command

Usage Information

Refer to the *FTOS 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 62-153, "Configuring a TPID on the E-Series TeraScale," in VLAN Stacking.](#)

Table 62-153. Configuring a TPID on the E-Series TeraScale

<i>number</i>	Resulting TPID
1	0x0100
10	0x1000
More than two characters.	Configuration rejected.

On E-Series ExaScale, C-Series, and S-Series, four characters you enter in the CLI for *number* are interpreted as follows:

Table 62-154. Configuring a TPID on the E-Series TeraScale

<i>number</i>	Resulting TPID
1	0x0001
10	0x0010
81	0x0081
8100	0x8100

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

To remove a trunk port designation from the selected interface, enter **no vlan-stack trunk**.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

- Version 8.2.1.0 Introduced on the E-Series ExaScale
- Version 7.8.1.0 Functionality augmented for C-Series and S-Series to enable multi-purpose use of the port. Refer to Usage Information, below.
- Version 7.7.1.0 Functionality augmented for E-Series to enable multi-purpose use of the port. Refer to Usage Information, below.
- Version 7.6.1.0 Introduced for C-Series and S-Series
E-Series original Command

Usage Information

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 FTOS 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. Refer to [Chapter 54, Service Provider Bridging](#).

Starting with FTOS 7.8.1.0 for C-Series and S-Series (FTOS 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. Refer to [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. Refer to [portmode hybrid](#) in [Interfaces](#).

Example 1

```
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)#do show vlan

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

      NUM      Status      Description                               Q Ports
*      1        Inactive
      20        Active        T Gi 0/42
      100       Active        M Gi 0/42
FTOS(conf-if-vl-20)#

```

Example 2 Figure 62-1. Adding a Stackable VLAN Trunk Port to Tagged and Untagged VLANs

```

FTOS(config)#vlan-stack protocol-type 88A8
FTOS(config)#interface gigabitethernet 3/10
FTOS(conf-if-gi-3/10)#no shutdown
FTOS(conf-if-gi-3/10)#switchport
FTOS(conf-if-gi-3/10)#vlan-stack access
FTOS(conf-if-gi-3/10)#exit

FTOS(config)#interface tenGigabitethernet 8/0
FTOS(conf-if-te-10/0)#no shutdown
FTOS(conf-if-te-10/0)#portmode hybrid
FTOS(conf-if-te-10/0)#switchport
FTOS(conf-if-te-10/0)#vlan-stack trunk
FTOS(conf-if-te-10/0)#exit

FTOS(config)#interface vlan 10
FTOS(conf-if-vlan)#vlan-stack compatible
FTOS(conf-if-vlan)#member Gi 7/0, Gi 3/10, TenGi 8/0
FTOS(conf-if-vlan)#exit

FTOS(config)#interface vlan 30
FTOS(conf-if-vlan)#untagged TenGi 8/0

```

```
FTOS(conf-if-vlan)#exit
FTOS(config)#

FTOS(config)#interface vlan 40
FTOS(conf-if-vlan)#tagged TenGi 8/0
FTOS(conf-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: E

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 X

(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

<i>name</i>	Enter the name for the VRF CAM profile. Maximum: 16 characters.
10M-CAM	Set the CAM size to 10M.

Command Modes CONFIGURATION

Command History

Version 8.2.1.0	Introduced on the E-Series Exascale.
-----------------	--------------------------------------

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
Updating the cam-profile will need a chassis reboot.
System configuration has been modified. Save? [yes/no]: y
```

```
Nov 3 21:57:27: %RPM0-P:CP %FILEMGR-5-FILESAVED: Copied running-config to
startup-config in flash by default
Synchronizing data to peer RPM
!!!!
Proceed with reload [confirm yes/no]: y
```

```
FTOS# show cam-profile
```

```
-- Chassis CAM Profile --
```

```
CamSize          : 40-Meg
                  : Current Settings
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 reload the system to activate the CAM profile (refer to 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 **T** (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
FTOS (conf)#do reload
-- Chassis CAM Profile --
CamSize          : 18-Meg
                  : Current Settings : Next Boot
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
EgL2ACL          : 1K entries        : 1K entries
EgIPv4ACL        : 12K entries       : 12K entries
Reserved         : 2K entries        : 2K entries
IPv6FIB          : 0 entries         : 0 entries
IPv6ACL          : 0 entries         : 0 entries
IPv6Flow         : 0 entries         : 0 entries
EgIPv6ACL        : 0 entries         : 0 entries
MicroCode Name   : Ipv4-Vrf         : Ipv4-Vrf
-- Line card 1 - per Port Pipe --
CamSize          : 18-Meg
                  : Current Settings : Next Boot
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
EgL2ACL          : 1K entries        : 1K entries
EgIPv4ACL        : 12K entries       : 12K entries
Reserved         : 2K entries        : 2K entries
IPv6FIB          : 0 entries         : 0 entries
IPv6ACL          : 0 entries         : 0 entries
IPv6Flow         : 0 entries         : 0 entries
EgIPv6ACL        : 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 T (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
                  : Current Settings : Next Boot
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
EgL2ACL         : 1K entries         : 1K entries
EgIPv4ACL        : 11K entries       : 11K entries
Reserved         : 2K entries        : 2K entries
IPv6FIB          : 18K entries       : 18K entries
IPv6ACL          : 4K entries         : 4K entries
IPv6Flow         : 3K entries        : 3K entries
EgIPv6ACL        : 1K entries        : 1K entries
MicroCode Name   : Ipv4-V6-Vrf      : Ipv4-V6-Vrf
```

```
-- Line card 1 - per Port Pipe --
CamSize          : 18-Meg
                  : Current Settings : Next Boot
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
EgL2ACL         : 1K entries         : 1K entries
EgIPv4ACL        : 11K entries       : 11K entries
Reserved         : 2K entries        : 2K entries
IPv6FIB          : 18K entries       : 18K entries
IPv6ACL          : 4K entries         : 4K entries
IPv6Flow         : 3K entries        : 3K entries
EgIPv6ACL        : 1K entries        : 1K entries
MicroCode Name   : Ipv4-V6-Vrf      : Ipv4-V6-Vrf
FTOS(conf)#
```

Usage Information Reload the systems after entering this command to activate the CAM profile.

Related Commands [cam-profile ipv4-vrf](#) Set the VRF CAM profile for IPv4 only.

cam-profile ipv4-vrf

E (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`
FTOS(conf)#`do reload`
-- Chassis CAM Profile --

```
CamSize           : 18-Meg
                  : Current Settings : Next Boot
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
EgL2ACL           : 1K entries        : 1K entries
EgIPv4ACL         : 12K entries       : 12K entries
Reserved          : 2K entries        : 2K entries
IPv6FIB           : 0 entries         : 0 entries
IPv6ACL           : 0 entries         : 0 entries
IPv6Flow          : 0 entries         : 0 entries
EgIPv6ACL         : 0 entries         : 0 entries
MicroCode Name    : Ipv4-Vrf         : Ipv4-Vrf
```

```
-- Line card 1 - per Port Pipe --
CamSize           : 18-Meg
                  : Current Settings : Next Boot
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
EgL2ACL           : 1K entries        : 1K entries
EgIPv4ACL         : 12K entries       : 12K entries
Reserved          : 2K entries        : 2K entries
IPv6FIB           : 0 entries         : 0 entries
IPv6ACL           : 0 entries         : 0 entries
IPv6Flow          : 0 entries         : 0 entries
EgIPv6ACL         : 0 entries         : 0 entries
MicroCode Name    : Ipv4-Vrf         : Ipv4-Vrf
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.

ip vrf

E Create a non-default VRF instance by specifying the VRF name and ID.



Note: Starting in FTOS 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

<i>vrf-name</i>	Enter the name of the VRF instance. Maximum: 32 characters.
<i>vrf-id</i>	Enter the VRF ID number. VRF ID range: 1 to 14 and 0 (default VRF)

Command Modes CONFIGURATION

Command History

Version 8.4.2.1	The <code>ip vrf {default-vlan vrf-name}</code> is deprecated and replaced by the <code>ip vrf vrf-name vrf-id</code> command.
Version 8.2.1.0	Introduced on the E-Series

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.

FTOS supports up to 15 VRF instances on an E-Series router: 1 to 14 and the default VRF 0.

ip vrf forwarding

E Assign this interface to the VLAN specified.

Syntax `ip vrf forwarding vrf-name`

Parameters

<i>vrf-name</i>	Enter the name of the VRF instance to which this interface will belong. If no name is entered, <i>default-vrf</i> is assigned.
-----------------	---

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)#
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	ip vrf	Set the name of the VRF instance the VRF, or specify the default-vrf.
	ip vrf-vlan-block	Configure the total number of VLANs that can be configured per VRF.
	start-vlan-id	Set the starting VLAN ID for a VRF instance.

ip vrf-vlan-block

E Configure the total number of VLANs that can be configured per VRF.

Starting in FTOS 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

<i>number</i>	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

Version 8.4.2.1	The ip vrf-vlan-block <i>number</i> command is deprecated.
Version 8.2.1.0	Introduced on the E-Series

Example

```
FTOS#conf
FTOS (conf) #ip vrf-vlan-block 1024
FTOS (conf) #
```

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

E 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

E 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.
<CR> displays information on the default-vrf.

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

E Set the starting VLAN ID for a VRF instance.

Starting in FTOS 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 `start-vlan-id vlan-start-id`

Parameters

<i>vlan-start-id</i>	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

Version 8.4.2.1	The start vrf-vlan-id <i>vlan-start-id</i> command is deprecated.
Version 8.2.1.0	Introduced on the E-Series

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

ip vrf forwarding	Assign this interface to the VLAN specified.
ip vrf-vlan-block	Configure the total number of VLANs that can be configured per VRF.
show run vrf	View information about the current running VRF instances.

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](#)
- [IPv6 VRRP Commands](#)

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](#)

advertise-interval

C **E** **S** 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.
Range: 1 to 255, in increments of 25 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

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 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

C **E** **S** 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

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 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

C **E** **S**

Clear the counters recorded for IPv4 VRRP operations.

Syntax `clear counters vrrp [vrid | vrf instance]`

Parameters

vrid (OPTIONAL) Enter the number of the VRRP group ID.
Range: 1 to 255

vrf instance (OPTIONAL) **E-Series only**: Enter the name of a VRF instance (32 characters maximum) to clear the counters of all VRRP groups in the specified VRF.

Command Modes EXEC Privilege

Command History

Version 8.4.1.0	Support was added for VRRP groups in non-default VRF instances.
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

debug vrrp

C **E**

Allows you to enable debugging of IPv4 VRRP.

Syntax `debug vrrp interface [vrid] { all | packets | state | timer }`

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 Range: 1-128
E-Series Range: 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 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.

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 7.5.1.0	Introduced on C-Series
pre-Version 6.2.1.1	Introduced on E-Series

Usage Information

If no options are specified, debug is active on all interfaces and all VRRP groups.

description

C **E** **S**

Configure a short text string describing the VRRP group.

Syntax **description** *text*

Parameters *text* Enter a text string up to 80 characters long.

Defaults Not enabled.

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

disable

C **E** **S**

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

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 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 `hold-time time`

Parameters

<i>time</i>	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

Usage Information If a switch is a MASTER and you change the hold timer, you must [disable](#) and re-enable VRRP for the new hold timer value to take effect.

Related Commands [disable](#) Disable a VRRP group.

preempt



Permit a BACKUP router with a higher priority value to preempt or become the MASTER router.

Syntax `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

C **E** **S**

Specify a VRRP priority value for the VRRP group. This value is used by the VRRP protocol during the MASTER election process.

Syntax `priority priority`

Parameters

priority Enter a number as the priority. Enter 255 only if the router's virtual address is the same as the interface's primary IP address (that is, the router is the OWNER).
Range: 1 to 255.
Default: 100.

Defaults 100

Command Modes VRRP

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

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

C **E** **S**

View the non-default VRRP configuration.

Syntax `show config [verbose]`

Parameters

verbose (OPTIONAL) Enter the keyword **verbose** to view all VRRP group configuration information, including defaults.

Command Modes VRRP

Command History

Version 8.3.2.0	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

Example

```
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 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 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 8.4.1.0	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 1 (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 2 100 Y Master 200.200.200.200 200.200.200.202 200.200.200.203
Gi 10/37 3 100 Y Master 1.1.1.1 1.1.1.2
Gi 10/37 4 100 Y Master 200.200.200.200 200.200.200.206 200.200.200.207
Gi 10/37 254 254 Y Master 200.200.200.200 200.200.200.204 200.200.200.205
```

Table 64-155. Command Example Description: show vrrp brief

Item	Description
Interface	Lists the interface type, slot and port on which the VRRP group is configured.
Grp	Displays the VRRP group ID.

Table 64-155. Command Example Description: show vrrp brief

Item	Description
Pri	Displays the priority value assigned to the interface. If the <code>track</code> command is configured to track that interface and the interface is disabled, the <code>COSf</code> is subtracted from the priority value assigned to the interface.
Pre	States whether preempt is enabled on the interface. <ul style="list-style-type: none"> • Y = Preempt is enabled. • N = Preempt is not enabled.
State	Displays the operational state of the interface by using one of the following: <ul style="list-style-type: none"> • NA/IF (the interface is not available). • MASTER (the interface associated with the MASTER router). • BACKUP (the interface associated with the BACKUP router).
Master addr	Displays the IP address of the MASTER router.
Virtual addr(s)	Displays the virtual IP addresses of the VRRP routers associated with the interface.

**Example 2
(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)
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: 310
Virtual MAC address:
  00:00:5e:00:02:01
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 64-156. Command Example Description: show vrrp

Line Beginning with	Description
GigabitEthernet...	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.
VRF	VRF instance to which the interface (on which the VRRP group is configured) belongs
State: master...	Displays the interface's state: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
Adv rcvd:...	This line displays counters for the following: <ul style="list-style-type: none"> • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Gratuitous ARP sent displays the number of gratuitous ARPs sent.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Authentication:...	States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.
Tracking states...	Displays information on the tracked interfaces or objects configured for a VRRP group (track command), including: <ul style="list-style-type: none"> • UP or DOWN state of the tracked interface or object (Up or Dn) • Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object • Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN

track

C **E** **S**

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 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 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.

Range: 1 to 254. Default: 10.

Defaults `cost = 10`

Command Modes VRRP

Command History

Version 8.4.1.0	Support for the <i>object-id</i> 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

C **E** **S**

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 to 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space.
The IP addresses must be on the same subnet as the interface's primary IP address.

Defaults Not configured.

Command Modes VRRP

Command History

Version 8.3.2.0	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

C **E** **S**

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 $(16 \times 10) + 2$, 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.

The following example 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 Force10 or non-Dell Force10) in the same VRRP group in order for all routers to interoperate.

Example

```
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

[virtual-address](#)

Assign up to 12 virtual IP addresses per VRRP group.

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

vrid (OPTIONAL) Enter the number of an IPv6 VRRP group. Range: 1 to 255

vrf instance (OPTIONAL) **E-Series only**: Enter the name of a VRF instance (32 characters maximum) to clear the counters of all IPv6 VRRP groups in the specified VRF.

Command Modes

EXEC Privilege

Command History

Version 8.4.1.0

Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.

Version 8.3.2.0

Introduced on E-Series TeraScale

debug vrrp ipv6



Allows you to enable debugging of VRRP.

Syntax `debug vrrp ipv6 interface [vrid] {all | packets | state | timer}`

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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.
<i>vrid</i>	(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

<i>vrid</i>	(OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. Range: 1 to 255.
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> 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 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

Example

```
FTOS#show vrrp ipv6
-----
GigabitEthernet 5/6, IPv6 VRID: 255, Version: 3, Net: fe80::201:e8ff:fe7a:6bb9
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 64-157. Command Example Description: show vrrp ipv6

Line Beginning with	Description
GigabitEthernet...	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.
VRF	VRF instance to which the interface (on which the VRRP group is configured) belongs
State: master...	Displays the interface's state: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
Adv rcvd:...	This line displays counters for the following: <ul style="list-style-type: none"> • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Bad pkts rcvd displays the number of invalid packets received on the interface.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Tracking states...	Displays information on the tracked interfaces or objects configured for a VRRP group (track command), including: <ul style="list-style-type: none"> • UP or DOWN state of the tracked interface or object (Up or Dn) • Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object • Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN

vrrp-ipv6-group

E C S

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 $(16 \times 10) + 2$, 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 Force10 or non-Dell Force10) 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.

E-Series ExaScale Debugging and Diagnostics

Overview

This document is for E-Series ExaScale E1200i and the E600i only and support begins with FTOS versions 8.1.1.0 and 8.1.1.2 respectively as denoted by the platform symbol .

FTOS supports an extensive suite of protocol-specific debug commands for packet- and event-level debugging. These commands are described throughout this document. In addition, FTOS supports commands for diagnosing suspected hardware issues.

This chapter contains the following sections:

- [Diagnostics and Monitoring Commands](#)
- [Offline Diagnostic Commands](#) (not supported in FTOS version 8.1.1.0)
- [Hardware Commands](#)

Diagnostics and Monitoring Commands

The diagnostics and monitoring commands are:

- `dataplane-diag disable loopback`
- `dataplane-diag disable dfo-reporting`
- `dataplane-diag disable dfo-reporting`
- `diag sfm`
- `ip control-plane egress-filter-traffic`
- `logging coredump kernel disable`
- `logging coredump kernel disable`
- `logging coredump kernel server`
- `logging coredump linecard`
- `power-off/on sfm`
- `reset sfm`
- `show command-history`
- `show console`
- `show diag sfm`
- `show processes ipc`
- `show processes ipc flow-control`
- `show revision`
- `show tech-support`

In addition to these debug commands, FTOS 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 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

Related Commands

[show diag sfm](#) Display the loopback test results

Usage Information

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.



Note: Only the Primary RPM can perform runtime dataplane loopback test.

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

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

[diag sfm](#) Initiate a manual dataplane loopback test.
[show diag sfm](#) Display the loopback test results



Note: This command is not supported on the E600i chassis.

diag sfm



Execute a manual dataplane loopback test.

Syntax `diag sfm all-loopback`

Parameters `all-loopback` (OPTIONAL) Enter the keyword `all-loopback` to execute a dataplane loopback test from the RPMs and all line cards.

Defaults No default behavior or value

Command Modes EXEC

Command History
Version 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

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 (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 `reset sfm` Reset the SFM and bring it back online.

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

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.

logging coredump kernel disable



Disable 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

Command History

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

Usage Information

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

logging coredump linecard	Enable core-dump logging on line cards
logging coredump kernel server	Save core-dump logging files to an alternate server

logging coredump kernel server

E **X** Designate the logging core-dump files to be saved to a remote server rather than flash.

Syntax **logging coredump kernel server**

To save the logging core-dump files to flash (the default), use the **no logging coredump kernel server** command.

Defaults Saved on flash

Command Modes CONFIGURATION

Command History

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

Related Commands

[logging coredump linecard](#) Enable core-dump logging on line cards
[logging coredump kernel disable](#) Disable kernel core-dump logging

logging coredump linecard

E **X** Enable line card core-dump logging on a specific line card or on all line cards.

Syntax logging coredump linecard { *slot_number* [port-shutdown | no-port-shutdown] | all }

To disable line card coredump logging, use the **no logging coredump linecard** [*slot_number* | all] command.

Parameters

linecard *slot number* Enter the keyword **linecard** 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.

port-shutdown Enter the keyword **port-shutdown** to configure the system to shutdown the physical interfaces during a software exception and the subsequent core dump.

no-port-shutdown Enter the keyword **no-port-shutdown** 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 **port-shutdown** option.

linecard all Enter the keyword **linecard all** to enable core-dump logging details on all line cards.

Defaults Disabled (core-dump logging is off)

Command Modes CONFIGURATION

Command History

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

Usage Information

The line card core-dump is stored on flash in a directory:

- Storage Directory Name: flash:CORE_DUMP_DIR
— Line Card core-dump naming convention is: f10lp*Slot_Number*.core.gz

For example: `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 `port-shutdown` option to shutdown the physical interfaces during the core dump, allowing for a failover to a backup system.

**Related
Commands**

[logging coredump kernel server](#)
[logging coredump kernel disable](#)

Save core-dump logging files to an alternate server.
Disable kernel core-dump logging.

power-off/on sfm



Power on or off a specified SFM.

Syntax `power-{off | on} sfm slot-number`

Parameters

<code>power-off</code>	Enter the keyword <code>power-off</code> to power off the SFM.
<code>power-on</code>	Enter the keyword <code>power-on</code> to power on the SFM
<code>sfm slot-number</code>	Enter the keyword <code>sfm</code> 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 8.1.1.2	Introduced on E-Series ExaScale E600i
Version 8.1.1.0	Introduced on E-Series ExaScale E1200i

**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.

**Example 1
(power-off sfm
with data traffic
warning)**

```
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.

**Example 2
(power-off sfm
with switch fabric
down warning)**

```
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 %TSM-6-SFM_SWITCHFAB_STATE: Switch Fabric: DOWN
Feb 16 00:03:20: %RPM1-P:CP %CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down
FTOS#
```

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.

**Example 3
(show sfm all)**

```
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 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

Example

```
FTOS#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. FTOS 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”?

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. 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 Force10 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 `lp slot-number` (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 a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

Defaults No default behavior or values

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

Example
FTOS#show console lp 0
MINI FIFO CONTROL = 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 = 11
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 11
FTOS#
```

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

Command History

Version 8.1.1.0 Introduced on E-Series ExaScale

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.

Example 1 (error message)

```
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).

Example 2

```
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

[power-off/on sfm](#) Power on/off an SFM

show diag sfm

E **X** 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 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

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    on          pass         Mar 26 2007 12:41:56
  1    off         none
-- Line cards --
Slot  Test Status  Last Result  Time Stamp
-----
  0    off         none
  1    off         none
  2    on          pass         Mar 26 2007 12:41:56
  3    off         none
  4    off         none
  5    off         none
  6    off         none
  7    off         none
  8    off         none
  9    off         none
 10   off         none
 11   on          pass         Mar 26 2007 12:41:56
 12   off         none
 13   off         none
FTOS#
```

show processes ipc

E **X** Display IPC messaging used internally between FTOS processes.

Syntax **show processes ipc** [recv-stats | send-stats] [cp | rp1 | rp2 | lp *linecard-number*]

Parameters	recv-stats	(OPTIONAL) Enter the keyword recv-stat 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 <i>linecard-number</i>	(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 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

Example (show processes ipc recv-stats)

```
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      6376   0      0
IPC: 3 ->          TME: 3    16215  0      41600      0      0      0
CLI: 0 ->          SYSADMTSK: 3 11483  0      41600      0      0      0
FTOS#
```

Example 2 (show processes ipc send-stats)



```
FTOS#show processes ipc send-stats
IPC Send Statistics on CP
Memory Used by Send DB on this processor: 2303000 bytes
SeqNo - Last sent guaranteed IPC pkt sequence no from this source to destination
Success - No of successfull 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 millisecs
```

NonG-S - No of non-guaranteed IPC pkts succesfully 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 succesfully sent
 SWP-F - No of non-guaranteed SWP IPC pkt transmission failures

```
Source->      Destination      SeqNo      Success      1st-R      2nd-R      Fails      RTT(ms) NonG-S
NonG-F SWP-S SWP-F
TME: 0 ->      TME: 1      15868      1            0            0            0            1            0
0            0            0
FTOS#
```

Usage Information These commands should be used only when you are working directly with Dell Force10 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

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

Example 1 (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->ipMgr0        0    0  0  0    0    0    25   25
FTOS#
```

Example 2
(show processes
ipc flow-control lp)

```

FTOS#show processes ipc flow-control lp 10
Q Statistics on LP 10
  TxProcess  RxProcess  Cur    High    Time    Retries  Msg    Ack    Aval    Max
                Len      Mark   Out      Sent    Rcvd   Retra  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
  IFAGT10       IFMGR0    0      1      0      0      1      1      8      8
LPDMACAGENT10  MACMGR0   0      0      0      0      0      0     25     25
FTOS#

```

Table 65-158. show processes ipc flow-control Display Definitions

Field	Description
TxProcess	Sender Process
RxProcess	Receiver Process
Cur Len	The number of messages, in the sender process, waiting to be sent to the receiver process
High Mark	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
Time Out	The time period the sender process waits for acknowledgement from the receiver process before attempting to resend the queued messages
Retries	The number of successive attempts (retries) the sender process will make to send the messages to the receiver process
Msg Sent	The accumulated number of messages sent between the sender and receiver processes from the time the queue was created.
Ack Rcvd	The number of acknowledgements received from the receiver process
Aval Retrans	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
Max Retrans	The max number of retransmission attempts configured for a sender - receiver pair

**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 queue³ 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, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

show revision

E **X** 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 8.1.1.2	Introduced on E-Series ExaScale E600i
Version 8.1.1.0	Introduced on E-Series ExaScale E1200i

Example 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 the necessary information for the Dell Force10 Technical Assistance Center to assist and perform troubleshooting.

Syntax show tech-support [page]

Parameters

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

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.

Example

```
FTOS#show tech-support
----- show version -----
Dell 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 -----
18:23:19.799 UTC Fri Mar 16 2007
----- show HA information -----
-- RPM Status --
-----
RPM Slot ID:          0
RPM Redundancy Role:  Primary
RPM State:           Active
RPM SW Version:      7.4.1.1
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

-- RPM Failover Record --
-----
Failover Count:      0
Last failover timestamp: None
Last failover Reason: None

----- 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

show version	Display the FTOS version.
show linecard	Display the line card(s) status.
show environment (C-Series and E-Series)	Display system component status.
show processes memory (C-Series and E-Series)	Display memory usage based on running processes.

Offline Diagnostic Commands

Offline diagnostics are not supported in FTOS version 8.1.1.0.

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](#)

diag linecard



Not supported in FTOS version 8.1.1.0
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

- number* 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.
- alllevels** Enter the keyword **alllevels** to run the complete offline diagnostic test.
- level0** Enter the keyword **level0** to check the device inventory and verify the existence of the devices.
- level1** Enter the keyword **Level1** to verify that the devices are accessible via the designated paths (line integrity tests) and test the internal registers of the devices.
- level2** Enter the keyword **level2** to perform on-board loopback tests on various data paths (data Port-Pipe and Ethernet).
- terminate** Enter the keyword **terminate** to stop the offline diagnostics tests.

Defaults All Levels (**alllevels**)

Command Modes

EXEC
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

offline



Not supported in FTOS version 8.1.1.0
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 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

online



Not supported in FTOS version 8.1.1.0
Place a line card in an online state.

Syntax `online {linecard number | rpm number}`

Parameters

linecard <i>number</i>	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 8.1.1.2	Introduced on E-Series ExaScale E600i
Version 8.1.1.0	Introduced on E-Series ExaScale E1200i

show diag



Not supported in FTOS version 8.1.1.0
Display current diagnostics information.

Syntax `show diag {information} [linecard number [detail | periodic | summary]]`

Parameters

information	Enter the keyword information to view current diagnostics information in the system.
linecard <i>number</i>	(OPTIONAL) 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.
detail	(OPTIONAL) Enter the keyword detail to view detailed diagnostics information.
periodic	(OPTIONAL) Enter the keyword periodic to display diagnostics results periodically.
summary	(OPTIONAL) Enter the keyword summary to view a summary of the diagnostics information.

Defaults **summary**

Command Mode

EXEC
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

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 Force10 TAC (Technical Assistance Center) while troubleshooting a problem. Do not use these command without the assistance of a Dell Force10 TAC representative. To contact Dell Force10 TAC for assistance:

E-mail Direct Support: support@Force10networks.com

Web: www.force10networks.com/support/

Telephone support:

US and Canada customers: 866-965-5800

International customers: 408-965-5800

The commands are:

- [clear hardware btm](#)
- [clear hardware rpm mac counters](#)
- [hardware monitor linecard](#)
- [hardware monitor mac](#)
- [hardware watchdog](#)
- [show control-traffic](#)
- [show control-traffic ingress | egress](#)
- [show control-traffic linecard](#)
- [show control-traffic rpm-switch](#)
- [show cpu-interface-stats](#)
- [show hardware btm](#)
- [show hardware fpc forward](#)
- [show hardware fpc lookup detail](#)
- [show hardware rpm mac counters](#)
- [show interfaces link-status](#)
- [show interfaces phy](#)
- [show interfaces transceiver](#)
- [show ipc-traffic](#)
- [show ipc-traffic ingress | egress](#)
- [show ipc-traffic linecard](#)
- [show ipc-traffic rpm-switch](#)
- [show logging driverlog](#)

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 <i>number</i>	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 <i>pipe-number</i>	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 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

Example

```
FTOS#clear hardware linecard 2 port-set 0 btm ingress errors
FTOS#clear hardware rpm 1 port-set 0 btm ingress errors
FTOS#clear hardware rpm 0 port-set 0 btm ingress errors
% Error: RPM 0 is not active.
FTOS#
```

Related Commands [show hardware btm](#) Display the BTM counters

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

slot-number Enter the RPM slot number.
Range: 0 -1

Defaults No default behavior or values

Command Mode	EXEC	
	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

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 }



Parameters	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.

Defaults None

Command Mode CONFIGURATION

Command History	Version 8.1.1.2	Introduced on E-Series ExaScale E600i
	Version 8.1.1.0	Introduced on E-Series ExaScale E1200i

hardware monitor mac

  Configure the system to shut down all ports on a line card upon a MAC hardware error.

Syntax hardware monitor mac action-on-error port-shutdown

Defaults None

Command Mode CONFIGURATION

Command History	Version 8.1.1.2	Introduced on E-Series ExaScale E600i
	Version 8.1.1.0	Introduced on E-Series ExaScale E1200i

hardware watchdog

E **X** Set the watchdog timer to trigger a reboot and restart the system.

Syntax **hardware watchdog**

Defaults Disabled

Command Mode CONFIGURATION

Command History

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

show control-traffic

E **X** Show information related to CP, RP1 or RP2, and ACL-FPGA related control traffic.

Syntax **show control-traffic rpm** [0-1] {cp | rp1 | rp2 | acl-fpga} {counters | statistics}

Parameters

cp	Enter the keyword cp to view IPC information on the CPs counters or statistics.
rp1	Enter the keyword rp1 to display the RP1's control counters or statistics
rp2	Enter the keyword rp2 to display the RP2's controlcounters or statistics.
acl-fpga	Enter the keyword acl-fpga to display the counters for packets transmitted through acl-fpga.

Defaults No default behavior or values

Command Modes

EXEC
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

show control-traffic ingress | egress

E **X** Display information related to packet drops and counters for ingress or egress IPC traffic.

Syntax **show control-traffic rpm** [0-1] {ingress| egress} {counters | drops }



Parameters

ingress	Enter the keyword ingress to view control information on the ingress (LC-to-RPM) path.
egress	Enter the keyword egress to view control information on the egress (RPM-to-LC) path.
counters	(OPTIONAL) Enter the keyword counters to display the control counters.
drops	(OPTIONAL) Enter the keyword drops to display control drop-related error counters.

Defaults No default behavior or values

Command Modes	EXEC	
	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

show control-traffic linecard

  Display information relating to packet counts for the selected linecard's control traffic.

Syntax `show control-traffic rpm [0-1] linecard # {lc-switch counters | lc-port counters}`

Parameters	linecard	Enter the keyword linecard <0>-to display the RPM Switch's control related information.
	counters	(OPTIONAL) Enter the keyword counters to display the control counters.
	lc-switch	(OPTIONAL) Enter the keyword lc-switch to display the counter information for the LC-Switch.
	lc-port	(OPTIONAL) Enter the keyword lc-port to display information for the LC-port.

Defaults No default behavior or values

Command Modes	EXEC
	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

show control-traffic rpm-switch

  Display information relating to packet counts for the RPM Switch's control traffic.

Syntax `show control-traffic rpm [0-1] rpm-switch {counters | configuration | qos-counters | qos-configuration | cp-port | rp1-port | rp2-port | lc-switch # | Peer-RPM} {counters | configuration | qos-counters | qos-configuration}`

Parameters	rpm-switch	Enter the keyword rpm-switch to display the RPM Switch's control related information.
	counters	(OPTIONAL) Enter the keyword counters to display the control counters.
	drops	(OPTIONAL) Enter the keyword drops to display control drop-related error counters.
	configuration	(OPTIONAL) Enter the keyword configuration to display the RP-Switch related control configuration.
	qos-counters	(OPTIONAL) Enter the keyword qos-counters to display the RP-Switch qos-counters..
	qos-cofiguration	(OPTIONAL) Enter the keyword qos-configuration to display the RP-Switch qos-configuration.
	cp-port	(OPTIONAL) Enter the keyword cp-port to display the RP-Switch information for the CP port.
	rp1-port	(OPTIONAL) Enter the keyword rp1-port to display the RP-Switch information for the RP1 port.

rp2-port	(OPTIONAL) Enter the keyword rp2-port to display the RP-Switch information for the CRP2 port.
lc-switch	(OPTIONAL) Enter the keyword lc-switch to display the counter information for the LC-Switch.
peer-rpm	(OPTIONAL) Enter the keyword peer-rpm to display information for the peer RPM.

Defaults No default behavior or values

Command Modes EXEC
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

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 Force10 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
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 8.1.1.2 Introduced on E-Series ExaScale E600i
Version 8.1.1.0 Introduced on E-Series ExaScale E1200i

Example 1
(show
cpu-interface-stats
lp)

```

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 2
(show
cpu-interface-stats
cp)

```

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 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*]}

Parameters

rpm	Enter the keyword rpm to display RPM error counters, status registers, or packet queue from the BTM.
linecard <i>number</i>	Enter the keyword linecard followed by the line card slot number to display BTM error counters, status registers, or packet queue 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 <i>pipe-number</i>	Enter the keyword port-set followed by the number of the line card's Port-Pipe. Range: 0 to 1
egress errors status queues	(OPTIONAL) Enter the keywords egress errors , egress status , or egress queues to view egress BTM error counters, status registers, or packet queue.
ingress errors status queues	(OPTIONAL) Enter the keywords ingress errors , ingress status , or ingress queues to view ingress BTM error counters, status registers, or packet queue.

all errors | status | queues (OPTIONAL) Enter the keywords **all errors**, **all status**, or **all queues** to view all BTM error counters, status registers, or packet queue

register *starting-value* [*number_of_registers*] Enter the keyword **register** followed by the starting value of the register to read from.
 Range: 0 to 16777212
 Optionally, enter the number of registers to read from. If no value is specified, only one line is displayed.
 Range: 1 to 512

Defaults No default behavior or values

Command Modes EXEC
 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



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  [0x00238]     =    50331648
Output for portpipe 0 Egress
  FC_BAD_CRC_ERR_CNTR    [0x000250]    =    150994944
FTOS#
  
```

Related Commands [clear hardware btm](#) Clear the btm counters

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

Example 1
(show hardware fpc forward drops)

```
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_IC_DROP                   : 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_IC_DROP                   : 0
CMB_LG_DROP                   : 0
CMB_SF_DROP                   : 0
CMB_IPM_DROP                  : 0
CMB_OPM_DROP                  : 0
FTOS#
```

Example 2
(show hardware fpc forward counters)

```
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
CMB_IC_DROP              : 0
CMB_LG_DROP              : 0
CMB_SF_DROP              : 0

CMB_IPM_DROP             : 0
CMB_OPM_DROP             : 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
CMB_IC_DROP              : 0
CMB_LG_DROP              : 0
CMB_SF_DROP              : 0
CMB_IPM_DROP             : 0
CMB_OPM_DROP             : 0
FTOS#

```

**Related
Commands**

[show hardware fpc lookup detail](#)

Display fpc lookup information.

show hardware fpc lookup detail

E **X** 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

linecard <i>number</i>	Enter the keyword linecard followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300
port-set <i>pipe-number</i>	Enter the keyword port-set followed by the number of the line card's Port-Pipe. Range: 0 to 1

Defaults No default values or behavior

Command Modes EXEC
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

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   P E 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
          p                   x
```

```
21554 50697065.5f302045.72726f72.2026204d.61736b20 0x52656769
0x73746572 0x2044756d 1879719229 1027423549 1027423549
```

Summary of Last 16 CamHits

=====

```
I  Hit0/      Hit1/      S   R   P E 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
                   e           x
```

```

0 0/0x00000 0/0x00000 0x00 0x00 00 0 00
1 0/0x00000 0/0x00000 0x00 0x00 00 0 00
2 0/0x00000 0/0x00000 0x00 0x00 00 0 00
3 0/0x00000 0/0x00000 0x00 0x00 00 0 00
4 0/0x00000 0/0x00000 0x00 0x00 00 0 00
5 0/0x00000 0/0x00000 0x00 0x00 00 0 00
6 0/0x00000 0/0x00000 0x00 0x00 00 0 00
7 0/0x00000 0/0x00000 0x00 0x00 00 0 00
8 0/0x00000 0/0x00000 0x00 0x00 00 0 00
9 0/0x00000 0/0x00000 0x00 0x00 00 0 00
10 0/0x00000 0/0x00000 0x00 0x00 00 0 00
11 0/0x00000 0/0x00000 0x00 0x00 00 0 00
12 0/0x00000 0/0x00000 0x00 0x00 00 0 00
13 0/0x00000 0/0x00000 0x00 0x00 00 0 00
FTOS#

```

Example 2
(show hardware rpm)

```

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
    640 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#

```

Related Commands

[show hardware fpc forward](#) Display information related to FPC forward.

show hardware rpm mac counters

E **X** 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

<i>slot-number</i>	Enter the RPM slot number 0 or 1.
port <i>port-number</i>	(OPTIONAL) Enter the keyword port followed by the port number of the party-bus control switch. Range: 0 to 24

Defaults No default values or behavior

Command Modes

EXEC
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

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 65-159. show hardware rpm mac counters Command Example Information

Slot ID #	Port number on the party-bus control switch.
RX Frames	Number of packets received by the party-bus switch from the processor in the specified slot.
TX Frames	Number of packets sent by the party-bus switch to the processor in the specified slot.

show interfaces link-status



Displays 10-Gigabit Ethernet link fault signaling and port status information.

Syntax `show interfaces tenGigabitEthernet slot/port link-status`

Parameters tenGigabitEthernet Enter the keyword tenGigabitEthernet followed by the slot/port information.

Command Modes EXEC
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

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 65-160. Lines in show interfaces tengigabitethernet Command Example

Line	Description
Loss of Signal	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.
Rx Signal Lock Error	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.
PCS Link State	Display the state of the PCS (Physical Coding sub-layer). The state is either up or down.
Link Fault Remote.	Indicates if the remote device has detected a fault, is inhibiting transmission of frames, and may be continuously transmitting idle messages.
Link Fault Local.	Indicates if a local fault is detected that may inhibit transmission of frames, and may be continuously transmitting remote fault signals.
Link Fault Idle Error	Indicates the detections of a non-idle symbol during an idle period.
Link Fault Illegal Symbol	Indicates the detections of an illegal symbol, other than an error symbol, while receiving data frames.
Link Fault Error Symbol.	Indicates the detections of an error symbol while receiving data frames.

show interfaces phy

E **X** Display auto-negotiation and link partner information.

Syntax `show interfaces gigabitethernet slot/port phy`

Parameters
gigabitethernet Enter the keyword `gigabitethernet` followed by the slot/port information.

Command Modes
EXEC
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

Example

```
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 65-161. Lines in show interfaces gigabitethernet Command Example

Line	Description
Mode Control	Indicates if auto negotiation is enabled. If so, indicates the selected speed and duplex.
Mode Status	Displays auto negotiation fault information. When the interface completes auto negotiation successfully, the autoNegComplete field and the linkstatus field read "True."
AutoNegotiation Advertise	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.

Table 65-161. Lines in show interfaces gigabitethernet Command Example

Line	Description
AutoNegotiation Remote Partner's Ability	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
AutoNegotiation Expansion	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.
1000Base-T Control	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.
Phy Specific Control	Values are: 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

show interfaces transceiver



Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

Syntax show interfaces gigabitethernet *slot/port* transceiver

Parameters gigabitethernet Enter the keyword **gigabitethernet** followed by the slot/port information.

Command Modes EXEC
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

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 Transceiver Code = 0x00 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 Name = FINISAR CORP.
SFP 0 Vendor OUI = 0x00 0x90 0x65
SFP 0 Vendor PN = FTRJ8519P1BNL
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

FTOS#

```

show ipc-traffic

E **X** Show information related to CP, RP1 or RP2 related IPC traffic.

Syntax **show IPc-traffic rpm** [0-1] {cp | rp1 | rp2 } {counters | statistics}

Parameters

cp Enter the keyword **cp** to view IPC information on the CPs counters or statistics.
rp1 Enter the keyword **rp1** to display the RP1's IPC counters or statistics
rp2 Enter the keyword **rp2** to display the RP2's IPC counters or statistics.

Defaults No default behavior or values



Command Modes

EXEC
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

show ipc-traffic ingress | egress

  Display information related to packet drops and counters for ingress or egress IPC traffic.

Syntax `show ipc-traffic rpm [0-1] {ingress| egress} {counters | drops}`

Parameters

ingress	Enter the keyword ingress to view IPC information on the ingress (LC-to-RPM) path.
egress	Enter the keyword egress to view IPC information on the egress (RPM-to-LC) path.
counters	(OPTIONAL) Enter the keyword counters to display the IPC counters.
drops	(OPTIONAL) Enter the keyword drops to display IPC drop-related error counters.

Defaults No default behavior or values

Command Modes

EXEC
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

show ipc-traffic linecard

  Display information relating to packet counts for the selected linecard's IPC traffic.

Syntax `show ipc-traffic rpm [0-1] linecard # {lc-cpu counters | lc-switch counters}`

Parameters

linecard	Enter the keyword linecard <0> to display the RPM Switch's IPC related information.
counters	(OPTIONAL) Enter the keyword counters to display the IPC counters.
lc-cpu	(OPTIONAL) Enter the keyword lc-port to display information for the LC-CPU.
lc-switch	(OPTIONAL) Enter the keyword lc-switch to display the counter information for the LC-Switch.

Defaults No default behavior or values

Command Modes

EXEC
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

show ipc-traffic rpm-switch



Display information relating to packet counts for the RPM Switch's IPC traffic.

Syntax show ipc-traffic rpm [0-1] rpm-switch {counters | configuration | qos-counters | qos-configuration | cp-port | rp1-port | rp2-port | lc-switch # | Peer-RPM} {counters | configuration | qos-counters | qos-configuration}

Parameters

rpm-switch Enter the keyword **rpm-switch** to display the RPM Switch's IPC related information.

counters (OPTIONAL) Enter the keyword **counters** to display the IPC counters.

drops (OPTIONAL) Enter the keyword **drops** to display IPC drop-related error counters.

configuration (OPTIONAL) Enter the keyword **configuration** to display the RP-Switch related IPC configuration.

qos-counters (OPTIONAL) Enter the keyword **qos-counters** to display the RP-Switch qos-counters..

qos-configuration (OPTIONAL) Enter the keyword **qos-configuration** to display the RP-Switch qos-configuration.

cp-port (OPTIONAL) Enter the keyword **cp-port** to display the RP-Switch information for the CP port.

rp1-port (OPTIONAL) Enter the keyword **rp1-port** to display the RP-Switch information for the RP1 port.

rp2-port (OPTIONAL) Enter the keyword **rp2-port** to display the RP-Switch information for the CRP2 port.

lc-switch (OPTIONAL) Enter the keyword **lc-switch** to display the counter information for the LC-Switch.

peer-rpm (OPTIONAL) Enter the keyword **peer-rpm** to display information for the peer RPM.

Defaults No default behavior or values

Command Modes EXEC
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

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 [cp | linecard number |stack-unit unit#]`

Parameters

- cp** Enter **cp** to display the driver log for the Control Processor.
- linecard *number*** (OPTIONAL) Enter the keyword **linecard** followed by the line card slot number to display the driver log for 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, 0 to 7 on a C300, 0 to 3 on a C150.
- 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 11

Defaults No default values or behavior

Command Modes EXEC
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

Usage Information This command displays internal software driver information which may be useful during troubleshooting line card initialization errors, such as downed Port-Pipe.

E-Series Debugging and Diagnostics

Overview

FTOS supports an extensive suite of protocol-specific debug commands for packet- and event-level debugging. These commands are described throughout this document. In addition, FTOS 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`
- `show tech-support`

In addition to these debug commands, FTOS 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

E 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

show diag sfm	Display the loopback test results
dataplane-diag disable sfm-bringdown	Disable the automatic SFM bringdown
dataplane-diag disable sfm-walk	Disable the automatic SFM walk

Usage Information 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 (refer to the following example).



Note: Only the Primary RPM can perform runtime dataplane loopback test.

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

E Disable the automatic bringdown 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 bringdown, use the `no dataplane-diag disable sfm-bringdown` 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 single faulty SFM. If confirmed, the single faulty SFM is identified and disabled by default. This command disables the automatic bringdown of that suspect SFM.

Related Commands

dataplane-diag disable loopback	Disable the runtime dataplane loopback test
dataplane-diag disable sfm-walk	Disable the automatic SFM walk
show diag sfm	Display the loopback test results

dataplane-diag disable sfm-walk

E 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

dataplane-diag disable loopback	Disable the runtime dataplane loopback test
dataplane-diag disable sfm-bringdown	Disable the automatic SFM bringdown.
show diag sfm	Display the loopback test results

dataplane-diag disable dfo-reporting

E 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

diag sfm	Initiate a manual dataplane loopback test.
show diag sfm	Display the loopback test results



Note: This command is not supported on the E600i chassis.

diag linecard

 Run a diagnosis on a line card.

Syntax `diag linecard [slot] [alllevels | level0 | level1 | level2 | terminate]`

Parameters

<code>slot</code>	Enter the slot number of the card you wish to diagnose.
<code>alllevels level0 level1 level2</code>	(OPTIONAL) Enter the level of diagnostic desired.
<code>terminate</code>	Enter the keyword <code>terminate</code> to stop the test

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

<code>all-loopback</code>	(OPTIONAL) Enter the keyword <code>all-loopback</code> to execute a dataplane loopback test from the RPMs and all line cards.
<code>rpm-loopback</code>	(OPTIONAL) Enter the keyword <code>rpm-loopback</code> to execute a dataplane loopback test on the RPMs only.

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 (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

reset sfm	Reset the SFM and bring it back online.
---------------------------	---

ip control-plane egress-filter-traffic

E 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 Version 7.6.1.0 Introduced on the E-Series only

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

E 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

Command History Version 7.6.1.0 Introduced on E-Series

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.

logging coredump kernel disable

E Disable 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

Command History Version 6.5.4.0 Introduced

Usage Information 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: f10rp*ProcessorID*.kcore.gz

For example: F10rp1.kcore.gz

- Application core-dump naming convention is:

rp*ProcessorID*_*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

[logging coredump linecard](#)

Enable core-dump logging on line cards

[logging coredump kernel server](#)

Save core-dump logging files to an alternate server

logging coredump kernel server

E Designate the logging core-dump files to be saved to a remote server rather than flash.

Syntax logging coredump kernel server

To save the logging core-dump files to flash (the default), use the no logging coredump kernel server command.

Defaults Saved on flash

Command Modes	CONFIGURATION	
Command History	Version 6.5.4.0	Introduced
Related Commands	logging coredump linecard	Enable core-dump logging on line cards
	logging coredump kernel disable	Disable kernel core-dump logging

logging coredump linecard

E Enable line card core-dump logging on a specific line card or on all line cards.

Syntax logging coredump linecard { *slot_number* [port-shutdown | no-port-shutdown] | all}
 To disable line card coredump logging, use the no logging coredump linecard [*slot_number* | all] command.

Parameters	linecard <i>slot number</i>	Enter the keyword linecard 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.
	port-shutdown	Enter the keyword port-shutdown to configure the system to shutdown the physical interfaces during a software exception and the subsequent core dump.
	no-port-shutdown	Enter the keyword no-port-shutdown 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 port-shutdown option.
	linecard all	Enter the keyword linecard all to enable core-dump logging details on all line cards.
Defaults	Disabled (core-dump logging is off)	


Command Modes	CONFIGURATION	
Command History	Version 7.6.1.0	Introduced the port-shutdown and no-port-shutdown variables
	Version 6.5.4.0	Introduced

Usage Information The line card core-dump is stored on flash in a directory:

- Storage Directory Name: flash:CORE_DUMP_DIR
 - Line Card core-dump naming convention is: f10lp*Slot_Number*.core.gz
For example: 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 **port-shutdown** option to shutdown the physical interfaces during the core dump, allowing for a failover to a backup system.

Related Commands	logging coredump kernel server	Save core-dump logging files to an alternate server.
	logging coredump kernel disable	Disable kernel core-dump logging.

power on/off linecard

 Power on or off a specified line card.

Syntax power-{off | on} linecard *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 <i>slot-number</i>	Enter the keyword 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 Version 6.5.4.0 Introduced

Related Commands [show linecard](#) Display the current line card status.

power-off/on sfm

 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 <i>slot-number</i>	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.0

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 bringdown 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.

Example 1

```
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 (refer to the following example).

Example 2

```
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 %TSM-6-SFM_SWITCHFAB_STATE: Switch Fabric: DOWN
Feb 16 00:03:20: %RPM1-P:CP %CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down
FTOS#
```

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 (refer to the following example).

Example 3

```
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

E 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

```

FTOS#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. FTOS 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” (refer to the example above).

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 (refer to the example above). 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 Force10 Technical Assistance Center (TAC) to assist in troubleshooting.



Note: No password information is saved to the trace command history log.

show console

E Display, onto the console, background resets, calls, initialization etc. of the designated line card.

Syntax show console lp *slot-number*

Parameters lp *slot-number* (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 a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

Defaults No default behavior or values.

Command Modes EXEC Privilege

Command History	Version 7.5.1.0	Introduced
Example	<pre> FTOS#show console lp 0 MINI FIFO CONTROL = 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 = 5 frrpaProcessIfmNotif(): Default case. type = 5 frrpaProcessIfmNotif(): Default case. type = 11 FTOS# </pre>	

reset linecard

E 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

E 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 (refer to Example 1 below).

Example 1

```
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 (refer to Example 2 below).

Example 2

```
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 [power-off/on sfm](#) Power on/off an SFM

show diag sfm

E 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 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    on          pass         Mar 26 2007 12:41:56
  1    off          none
```

```
-- Line cards --
```

Slot	Test Status	Last Result	Time Stamp
0	off	none	
1	off	none	
2	on	pass	Mar 26 2007 12:41:56
3	off	none	
4	off	none	
5	off	none	
6	off	none	
7	off	none	
8	off	none	
9	off	none	
10	off	none	
11	on	pass	Mar 26 2007 12:41:56
12	off	none	
13	off	none	

FTOS#

show processes ipc

(E) Display IPC messaging used internally between FTOS processes.

Syntax show processes ipc [recv-stats | send-stats] [cp | rp1 | rp2 | lp *linecard-number*]

Parameters

recv-stats	(OPTIONAL) Enter the keyword recv-stat 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 <i>linecard-number</i>	(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 (show processes ipc recv-stats)

```
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      6376       0      0
IPC: 3 ->          TME: 3     16215  0           41600      0          0      0
CLI: 0 ->          SYSADMTSK: 3 11483  0           41600      0          0      0
FTOS#
```

Example (show processes ipc send-stats)

```
FTOS#show processes ipc send-stats
IPC Send Statistics on CP
Memory Used by Send DB on this processor: 2303000 bytes
SeqNo - Last sent guaranteed IPC pkt sequence no from this source to destination
Success - No of successfull 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 millisecs
NonG-S - No of non-guaranteed IPC pkts succesfully 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 succesfully sent
SWP-F - No of non-guaranteed SWP IPC pkt transmission failures
```

```
Source->          Destination  SeqNo  Success  1st-R  2nd-R  Fails  RTT(ms)
NonG-S NonG-F  SWP-S  SWP-F
TME: 0 ->          TME: 1     15868  1        0      0      0      1
0      0      0      0
FTOS#
```

Usage Information

These commands should be used only when you are working directly with Dell Force10 TAC (Technical Assistance Center) while troubleshooting a problem.

show processes ipc flow-control

E 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.

Defaults No default values or behavior.

Command Modes

EXEC
EXEC Privilege

Command History

Version 7.5.1.0 Introduced

Example 1

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->ipMgr0      0   0   0   0   0     0  25 25
FTOS#
```

Example 2

FTOS#show processes ipc flow-control lp 10

Q Statistics on LP 10

```
      TxProcess  RxProcess    Cur   High  Time  Retries  Msg   Ack   Aval  Max
      Len      Mark   Out           Sent  Rcvd  Retra  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
IFAGT10       IFMGR0       0     1     0     0         1     1     8     8
LPDMACAGENT10 MACMGR0      0     0     0     0         0     0     25    25
FTOS#
```

Table 66-162, "show processes ipc flow-control Display Definitions," in *E-Series Debugging and Diagnostics* defines the fields displayed in Example 2 above.

Table 66-162. show processes ipc flow-control Display Definitions

Field	Description
TxProcess	Sender Process
RxProcess	Receiver Process
Cur Len	The number of messages, in the sender process, waiting to be sent to the receiver process
High Mark	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
Time Out	The time period the sender process waits for acknowledgement from the receiver process before attempting to resend the queued messages
Retries	The number of successive attempts (retries) the sender process will make to send the messages to the receiver process
Msg Sent	The accumulated number of messages sent between the sender and receiver processes from the time the queue was created.
Ack Rcvd	The number of acknowledgements received from the receiver process
Aval Retrans	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
Max Retrans	The max number of retransmission attempts configured for a sender - receiver pair

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 queue³ 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 Example 2 above, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

show revision

E 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 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

- E** Display a collection of data from other show commands, the information is necessary for Dell Force10 technical support to perform troubleshooting.

Syntax show tech-support [**linecard** | **page**] {**display** | **except** | **find** | **grep** | **no-more** | **save**}

Parameters	linecard {0 - 6}	(OPTIONAL) Enter the keyword linecard followed by the line card number to view information relating to a specific line card.
	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.
	display, except, find, grep, no-more	When using the pipe command (), enter one of these keywords to filter command output. Refer to <i>CLI Basics</i> in the <i>FTOS Command Reference Guide</i> 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))

Command Modes EXEC Privilege

Command History	Version 7.8.1.0	Added save option
	Version 7.5.1.0	Introduced on C-Series
	Version 6.5.4.0	Show clock included in display

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.

Example

```

FTOS#show tech-support
----- show version -----
Dell 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 -----
18:23:19.799 UTC Fri Mar 16 2007
----- show HA information -----
-- RPM Status --
-----
RPM Slot ID:          0
RPM Redundancy Role: Primary
RPM State:           Active
RPM SW Version:      7.4.1.1
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

```

```

-- RPM Failover Record --
-----
Failover Count:          0
Last failover timestamp: None
Last failover Reason:   None

----- 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

show version	Display the FTOS version.
show linecard	Display the line card(s) status.
show environment (C-Series and E-Series)	Display system component status.
show processes memory (C-Series and E-Series)	Display memory usage based on running processes.

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](#)

diag linecard

E 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

number 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.

alllevels Enter the keyword **alllevels** to run the complete offline diagnostic test.

level0 Enter the keyword **level0** to check the device inventory and verify the existence of the devices.

level1 Enter the keyword **Level1** to verify that the devices are accessible via the designated paths (line integrity tests) and test the internal registers of the devices.

level2 Enter the keyword **level2** to perform on-board loopback tests on various data paths (data Port-Pipe and Ethernet).

terminate Enter the keyword **terminate** to stop the offline diagnostics tests.

Defaults All Levels (**alllevels**)

Command Modes

EXEC
EXEC Privilege

Command History

Version 6.5.4.0 Introduced

offline

E 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

E Place a line card in an online state.

Syntax `online {linecard number | rpm number}`

Parameters

<i>linecard number</i>	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

E Display current diagnostics information.

Syntax `show diag {information} [linecard number [detail | periodic | summary]]`

Parameters

<i>information</i>	Enter the keyword information to view current diagnostics information in the system.
<i>linecard number</i>	(OPTIONAL) 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.
<i>detail</i>	(OPTIONAL) Enter the keyword detail to view detailed diagnostics information.
<i>periodic</i>	(OPTIONAL) Enter the keyword periodic to display diagnostics results periodically.
<i>summary</i>	(OPTIONAL) Enter the keyword summary to view a summary of the diagnostics information.

Defaults *summary*

Command Mode

EXEC
EXEC Privilege

Command History

Version 6.5.4.0	Introduced
-----------------	------------

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 Force10 TAC (Technical Assistance Center) while troubleshooting a problem. Do not use these command without the assistance of a Dell Force10 TAC representative. To contact Dell Force10 TAC for assistance:

E-mail Direct Support: support@Force10networks.com

Web: www.force10networks.com/support/

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](#)
- [show hardware fpc forward](#)
- [show hardware fpc lookup detail](#)
- [show hardware rpm cp](#)
- [show hardware rpm mac counters](#)
- [show hardware rpm rp1/rp2](#)
- [show interfaces link-status](#)
- [show logging driverlog](#)
- [show running-config hardware-monitor](#)

Refer also to [Chapter 25, Interfaces](#):

- [show interfaces phy](#)
- [show interfaces transceiver](#)

clear hardware btm

E 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

<code>rpm</code>	Enter the keyword <code>rpm</code> to clear BTM error counters or status registers on the RPM.
<code>linecard <i>number</i></code>	Enter the keyword <code>linecard</code> 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

<code>port-set <i>pipe-number</i></code>	Enter the keyword <code>port-set</code> followed by the number of the line card or RPM's Port-Pipe. Range: 0 to 1
<code>egress errors status</code>	(OPTIONAL) Enter the keywords <code>egress errors</code> or <code>egress status</code> to clear egress BTM error counters or ingress BTM status registers.
<code>ingress errors status</code>	(OPTIONAL) Enter the keywords <code>ingress errors</code> or <code>ingress status</code> to clear ingress BTM error counters or ingress BTM status registers.
<code>all errors status</code>	(OPTIONAL) Enter the keywords <code>all errors</code> or <code>all status</code> 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

Example

```
FTOS#clear hardware linecard 2 port-set 0 btm ingress errors
FTOS#clear hardware rpm 1 port-set 0 btm ingress errors
FTOS#clear hardware rpm 0 port-set 0 btm ingress errors
% Error: RPM 0 is not active.
FTOS#
```

Related Commands [show hardware btm](#) Display the BTM counters

clear hardware rpm mac counters

E 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 `slot-number` Enter the RPM slot number.
Range: 0 -1

Defaults No default behavior or values.

Command Mode EXEC
EXEC Privilege

Command History Version 6.5.4.0 Introduced

hardware monitor linecard

E Configure the system to take an action upon a line card hardware error.

Syntax 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 7.7.1.0 Introduced

hardware monitor mac

E Configure the system to shut down all ports on a line card upon a MAC hardware error.

Syntax hardware monitor mac action-on-error port-shutdown

Defaults None

Command Mode CONFIGURATION

Command History Version 7.7.1.0 Introduced

hardware watchdog

E Set the watchdog timer to trigger a reboot and restart the system.

Syntax 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 FTOS switch/router with a single unresponsive RPM. This is a last resort mechanism intended to prevent a manual power cycle.

show cpu-interface-stats

E 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 Force10 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
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 (show cpu-interface-stats lp)

```
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 (show
cpu-interface-stats
cp)**

```

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 btm

E 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]}`

Parameters

rpm	Enter the keyword rpm to display RPM error counters, status registers, or packet queue from the BTM.
linecard <i>number</i>	Enter the keyword linecard followed by the line card slot number to display BTM error counters, status registers, or packet queue 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 <i>pipe-number</i>	Enter the keyword port-set followed by the number of the line card's Port-Pipe. Range: 0 to 1
egress errors status queues	(OPTIONAL) Enter the keywords egress errors , egress status , or egress queues to view egress BTM error counters, status registers, or packet queue.
ingress errors status queues	(OPTIONAL) Enter the keywords ingress errors , ingress status , or ingress queues to view ingress BTM error counters, status registers, or packet queue.
all errors status queues	(OPTIONAL) Enter the keywords all errors , all status , or all queues to view all BTM error counters, status registers, or packet queue
register <i>starting-value</i> [<i>number_of_registers</i>]	Enter the keyword register followed by the starting value of the register to read from. Range: 0 to 16777212 Optionally, enter the number of registers to read from. If no value is specified, only one line is displayed. Range: 1 to 512

Defaults No default behavior or values.

Command Modes EXEC
EXEC Privilege

Command History Version 6.5.4.0 Introduced

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  [0x00238]    =   50331648
Output for portpipe 0 Egress
  FC_BAD_CRC_ERR_CNTR   [0x000250]   =   150994944
FTOS#

```

**Related
Commands**

[clear hardware btm](#) Clear the btm counters

show hardware fpc forward

E 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 (show
hardware fpc
forward drops)**

```

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_IC_DROP                           : 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_IC_DROP       : 0
CMB_LG_DROP       : 0
CMB_SF_DROP       : 0
CMB_IPM_DROP      : 0
CMB_OPM_DROP      : 0
FTOS#

```

Example
(show hardware
fpc forward
counters)

```

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
CMB_IC_DROP              : 0
CMB_LG_DROP              : 0
CMB_SF_DROP              : 0

CMB_IPM_DROP             : 0
CMB_OPM_DROP             : 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
CMB_IC_DROP                                 : 0
CMB_LG_DROP                                 : 0
CMB_SF_DROP                                 : 0
CMB_IPM_DROP                                : 0
CMB_OPM_DROP                                : 0
FTOS#

```

**Related
Commands**

[show hardware fpc lookup detail](#) Display fpc lookup information.

show hardware fpc lookup detail

E 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

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/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's Port-Pipe.
Range: 0 to 1

Defaults No default values or behavior.

Command Modes

EXEC
EXEC Privilege

**Command
History**

Version 6.5.4.0 Introduced

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   P E 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
          p           x
21554 50697065.5f302045.72726f72.2026204d.61736b20 0x52656769
0x73746572 0x2044756d 1879719229 1027423549 1027423549

```

```

Summary of Last 16 CamHits
=====
I   Hit0/   Hit1/   S   R   P E 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
           e           x
0 0/0x00000 0/0x00000 0x00 0x00 00 0 00
1 0/0x00000 0/0x00000 0x00 0x00 00 0 00
2 0/0x00000 0/0x00000 0x00 0x00 00 0 00
3 0/0x00000 0/0x00000 0x00 0x00 00 0 00
4 0/0x00000 0/0x00000 0x00 0x00 00 0 00
5 0/0x00000 0/0x00000 0x00 0x00 00 0 00
6 0/0x00000 0/0x00000 0x00 0x00 00 0 00
7 0/0x00000 0/0x00000 0x00 0x00 00 0 00
8 0/0x00000 0/0x00000 0x00 0x00 00 0 00
9 0/0x00000 0/0x00000 0x00 0x00 00 0 00
10 0/0x00000 0/0x00000 0x00 0x00 00 0 00
11 0/0x00000 0/0x00000 0x00 0x00 00 0 00
12 0/0x00000 0/0x00000 0x00 0x00 00 0 00
13 0/0x00000 0/0x00000 0x00 0x00 00 0 00
FTOS#

```

Related Commands

[show hardware fpc forward](#)

Display information related to FPC forward.

show hardware rpm cp

(E) Display advanced debugging information for the RPM processors.

Syntax

`show hardware rpm slot-number cp {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

Defaults No default values or behavior.

Command Modes EXEC
EXEC Privilege

Command History Version 6.5.4.0 Introduced

Example

```

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
  640 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

- E** 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 party-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

```
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 66-163, "show hardware rpm mac counters Command Example Information," in [E-Series Debugging and Diagnostics](#) defines the fields displayed in the example above.

Table 66-163. show hardware rpm mac counters Command Example Information

Slot ID #	Port number on the party-bus control switch.
RX Frames	Number of packets received by the party-bus switch from the processor in the specified slot.
TX Frames	Number of packets sent by the party-bus switch to the processor in the specified slot.

show hardware rpm rp1/rp2

E Display advanced debugging information for the RPM processors.

Syntax show hardware rpm *slot-number* {rp1 | rp2} {data-plane | party-bus} {counters | statistics}

Parameters

<i>slot-number</i>	Enter the RPM slot number 0 or 1.
rp1 rp2	Enter either the keyword rp1 or rp2 to designate which route processor debug information to display.
data-plane	(OPTIONAL) Enter the keywords data-plane to display control processor information on the dataplane of 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

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

E Displays 10-Gigabit Ethernet link fault signaling and port status information.

Syntax show interfaces tenGigabitEthernet *slot/port* link-status

Parameters tenGigabitEthernet Enter the keyword **tenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC
EXEC Privilege

Command History Version 6.5.4.0 Introduced

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 66-164, "Lines in show interfaces tengigabitethernet Command Example," in E-Series Debugging and Diagnostics defines the information displayed in the example above.

Table 66-164. Lines in show interfaces tengigabitethernet Command Example

Line	Description
Loss of Signal	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.
Rx Signal Lock Error	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.
PCS Link State	Display the state of the PCS (Physical Coding sub-layer). The state is either up or down.
Link Fault Remote.	Indicates if the remote device has detected a fault, is inhibiting transmission of frames, and may be continuously transmitting idle messages.
Link Fault Local.	Indicates if a local fault is detected that may inhibit transmission of frames, and may be continuously transmitting remote fault signals.
Link Fault Idle Error	Indicates the detections of a non-idle symbol during an idle period.
Link Fault Illegal Symbol	Indicates the detections of an illegal symbol, other than an error symbol, while receiving data frames.
Link Fault Error Symbol.	Indicates the detections of an error symbol while receiving data frames.

show logging driverlog



Display the driver log for the RPM or stack-unit CP processor or for the line card CPU in the specified slot.

Syntax `show logging driverlog [cp | linecard number |stack-unit unit#]`

Parameters

cp

Enter **cp** to display the driver log for the Control Processor.

linecard *number*

Enter the keyword **linecard** followed by the line card slot number to display the driver log for 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, 0 to 7 on a C300, 0 to 3 on a C150.

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 11

Defaults No default values or behavior

Command Modes EXEC

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

Usage Information 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

E Display the hardware-monitor action-on-error settings.

Syntax show running-config hardware-monitor

Defaults No default values or behavior

Command Modes EXEC Privilege

Command History	Version 7.8.1.0	Introduced
------------------------	-----------------	------------

Example

```

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#

```


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 67-165. ICMP Messages and their definitions

Symbol	Type	Code	Description	Query	Error
•			Timeout (no reply)		
!	0	3	echo reply	•	
U	3		destination unreachable:		
		0	network unreachable		•
		1	host unreachable		•
		2	protocol unreachable		•
		3	port unreachable		•
		4	fragmentation needed but don't fragment bit set		•
		5	source route failed		•
		6	destination network unknown		•
		7	destination host unknown		•
		8	source host isolated (obsolete)		•
		9	destination network administratively prohibited		•
		10	destination host administratively prohibited		•
		11	network unreachable for TOS		•
		12	host unreachable for TOS		•
		13	communication administratively prohibited by filtering		•
		14	host precedence violation		•
		15	precedence cutoff in effect		•
C	4	0	source quench		•
	5		redirect		•
		0	redirect for network		•
		1	redirect for host		•
		2	redirect for type-of-service and network		•
		3	redirect for type-of-service and host		•
	8	0	echo request	•	
	9	0	router advertisement	•	
	10	0	router solicitation	•	

Table 67-165. ICMP Messages and their definitions

Symbol	Type	Code	Description	Query	Error
&	11		time exceeded:		
		0	time-to-live equals 0 during transit		•
		1	time-to-live equals 0 during reassembly		•
	12		parameter problem:		
		1	IP header bad (catchall error)		•
		2	required option missing		•
	13	0	timestamp request	•	
	14	0	timestamp reply	•	
	15	0	information request (obsolete)	•	
	16	0	information reply (obsolete)	•	
	17	0	address mask request	•	
	18	0	address mask reply	•	

SNMP Traps

This chapter lists the traps sent by FTOS. Each trap is listed by the fields Message ID, Trap Type, and Trap Option, and the next is the message(s) associated with the trap.

Table 68-166. SNMP Traps and Error Messages

Message ID	Trap Type	Trap Option
COLD_START	SNMP	COLDSTART
%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.		
WARM_START	SNMP	WARMSTART
COPY_CONFIG_COMPLETE	SNMP	NONE
SNMP Copy Config Command Completed		
LINK_DOWN	SNMP	LINKDOWN
%IFA-1-PORT_LINKDN: changed interface state to down:%d		
LINK_UP	SNMP	LINKUP
%IFA-1-PORT_LINKUP: changed interface state to up:%d		
AUTHENTICATION_FAIL	SNMP	AUTH
%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.		
EGP_NEIGHBOR_LOSS	SNMP	NONE
OSTATE_DOWN	SNMP	LINKDOWN
%IFM-1-OSTATE_DN: changed interface state to down:%s		
%IFM-5-CSTATE_DN:Changed interface Physical state to down: %s		
OSTATE_UP	SNMP	LINKUP
%IFM-1-OSTATE_UP: changed interface state to up:%s		
%IFM-5-CSTATE_UP: Changed interface Physical state to up: %s		
RMON_RISING_THRESHOLD	SNMP	NONE
%RPM0-P:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID <oid>		
RMON_FALLING_THRESHOLD	SNMP	NONE
%RPM0-P:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID <oid>		
RMON_HC_RISING_THRESHOLD	SNMP	NONE
%RPM0-P:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID <oid>		
RMON_HC_FALLING_THRESHOLD	SNMP	NONE
%RPM0-P:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID <oid>		
RESV	NONE	NONE
N/A		

Table 68-166. SNMP Traps and Error Messages (Continued)

Message ID	Trap Type	Trap Option
CHM_CARD_DOWN	ENVMON	NONE
%CHMGR-1-CARD_SHUTDOWN: %sLine card %d down - %s %CHMGR-2-CARD_DOWN: %sLine card %d down - %s		
CHM_CARD_UP	ENVMON	NONE
%CHMGR-5-LINECARDUP: %sLine card %d is up		
CHM_CARD_MISMATCH	ENVMON	NONE
%CHMGR-3-CARD_MISMATCH: Mismatch: line card %d is type %s - type %s required.		
CHM_CARD_PROBLEM	ENVMON	NONE
CHM_ALARM_CUTOFF	ENVMON	NONE
CHM_SFM_UP	ENVMON	NONE
CHM_SFM_DOWN	ENVMON	NONE
CHM_RPM_UP	ENVMON	NONE
%RAM-6-RPM_STATE: RPM1 is in Active State %RAM-6-RPM_STATE: RPM0 is in Standby State		
CHM_RPM_DOWN	ENVMON	NONE
%CHMGR-2-RPM_DOWN: RPM 0 down - hard reset %CHMGR-2-RPM_DOWN: RPM 0 down - card removed		
CHM_RPM_PRIMARY	ENVMON	NONE
%RAM-5-COLD_FAILOVER: RPM Failover Completed %RAM-5-HOT_FAILOVER: RPM Failover Completed %RAM-5-FAST_FAILOVER: RPM Failover Completed		
CHM_SFM_ADD	ENVMON	NONE
%TSM-5-SFM_DISCOVERY: Found SFM 1		
CHM_SFM_REMOVE	ENVMON	NONE
%TSM-5-SFM_REMOVE: Removed SFM 1		
CHM_MAJ_SFM_DOWN	ENVMON	NONE
%CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down		
CHM_MAJ_SFM_DOWN_CLR	ENVMON	NONE
%CHMGR-5-MAJOR_SFM_CLR: Major alarm cleared: Switch fabric up		
CHM_MIN_SFM_DOWN	ENVMON	NONE
%CHMGR-2-MINOR_SFM: Minor alarm: No working standby SFM		
CHM_MIN_SFM_DOWN_CLR	ENVMON	NONE
%CHMGR-5-MINOR_SFM_CLR: Minor alarm cleared: Working standby SFM present		
CHM_PWRSRC_DOWN	ENVMON	SUPPLY
%CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module %s		

Table 68-166. SNMP Traps and Error Messages (Continued)

Message ID	Trap Type	Trap Option
CHM_PWRSRC_CLR	ENVMON	SUPPLY
%CHMGR-5-PEM_OK: Major alarm cleared: power entry module %s is good		
CHM_MAJ_ALARM_PS	ENVMON	SUPPLY
%CHMGR-0-MAJOR_PS: Major alarm: insufficient power %s		
CHM_MAJ_ALARM_PS_CLR	ENVMON	SUPPLY
%CHMGR-5-MAJOR_PS_CLR: major alarm cleared: sufficient power		
CHM_MIN_ALARM_PS	ENVMON	SUPPLY
%CHMGR-1-MINOR_PS: Minor alarm: power supply non-redundant		
CHM_MIN_ALARM_PS_CLR	ENVMON	SUPPLY
%CHMGR-5-MINOR_PS_CLR: Minor alarm cleared: power supply redundant		
CHM_MIN_ALRM_TEMP	ENVMON	TEMP
%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature		
CHM_MIN_ALRM_TEMP_CLR	ENVMON	TEMP
%CHMGR-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)		
CHM_MAJ_ALRM_TEMP	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)		
CHM_MAJ_ALRM_TEMP_CLR	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)		
CHM_FANTRAY_BAD	ENVMON	FAN
For E1200: %CHMGR-2-FAN_TRAY_BAD: Major alarm: fan tray %d is missing or down		
%CHMGR-2-ALL_FAN_BAD: Major alarm: all fans in fan tray %d are down.		
For E600 and E300: %CHMGR-2-FANTRAYBAD: Major alarm: fan tray is missing		
%CHMGR-2-FANSBAD: Major alarm: most or all fans in fan tray are down		
CHM_FANTRAY_BAD_CLR	ENVMON	FAN
For the E1200: %CHMGR-5-FAN_TRAY_OK: Major alarm cleared: fan tray %d present		
For the E600 and E300: %CHMGR-5-FANTRAYOK: Major alarm cleared: fan tray present		
CHM_MIN_FANBAD	ENVMON	FAN
For the E1200: %CHMGR-2-FAN_BAD: Minor alarm: some fans in fan tray %d are down		
For the E600 and E300: %CHMGR- 2-1FANBAD: Minor alarm: fan in fan tray is down		
CHM_MIN_FANBAD_CLR	ENVMON	FAN
For E1200: %CHMGR-2-FAN_OK: Minor alarm cleared: all fans in fan tray %d are good		
For E600 and E300: %CHMGR-5-FANOK: Minor alarm cleared: all fans in fan tray are good		
TME_TASK_SUSPEND	ENVMON	NONE
%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s		
TME_TASK_TERM	ENVMON	NONE
%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s		
CHM_CPU_THRESHOLD	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)		
CHM_CPU_THRESHOLD_CLR	ENVMON	NONE

Table 68-166. SNMP Traps and Error Messages (Continued)

Message ID	Trap Type	Trap Option
%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)		
CHM_MEM_THRESHOLD	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)		
CHM_MEM_THRESHOLD_CLR	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)		
MACMGR_STN_MOVE	ENVMON	NONE
%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d		
VRRP_BDAUTH	PROTO	NONE
%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication type mismatch.		
%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication failure.		
VRRP_GO_MASTER	PROTO	NONE
%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER		
BGP4_ESTABLISHED	PROTO	NONE
%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s		
BGP4_BACKW_XSITION	PROTO	NONE
%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s		

Index

Numerics

cam-profile template 410
802.3x pause frames 549

A

aaa accounting suppress 1209
aaa authentication login 1216
ABR 959, 960
Access Control Lists (ACLs) 187
access control lists. See ACL.
access-class (common IP ACL) 190
ACCESS-LIST Mode 24
ACL 23, 24
 deny 659
 deny tcp 661
 deny udp 663
 description 251
 Important Points to Remember 657
 IP trace lists 1253
 ipv6 access-group 665
 permit 666
 permit tcp 668
 permit udp 670
 remark 672
 seq 674
 show ipv6 accounting access-list 677
ACL VLAN Group
 acl-vlan-group 275
 description 276
 ip access-group 276
 member vlan 277
 show acl-vlan-group 277
 show acl-vlan-group detail 278
 show config 279
 show running config acl-vlan-group 279
action-list command 476
address family ipv4 multicast (MBGP) 373
address family ipv6 unicast (BGP IPv6) 762
Address Resolution Protocol, See ARP.
address-family
 bgp 296, 703
adjacency-check (ISIS_IPv6) 789
admin-email 477
Administrator's email address 477, 478
advertise 789
advertise (ISIS) 789
advertise med guest-voice 872
advertise-interval 1392, 1403
AFI/SAFI 321
aggregate-address 296, 704
aggregate-address (BGP IPv6) 704, 762
aggregate-address (BGP) 296

aggregate-address (MBGP) 373
ais-shut 1312
alarm-report 1312
ANSI/TIA-1057 871
archive 432
archive backup 432
archive config 432
Area Border Router. See ABR.
area default-cost 959
area default-cost (OSPF) 959
area nssa 960
area nssa (OSPF) 960
area range 960
area range (OSPF) 960
area stub 961
area stub (OSPF) 961
area virtual-link 961
area virtual-link (OSPF) 961
area-password 789
area-password (ISIS) 790
arp 608
arp timeout 610
AS 293, 701, 957
ASBR 990
asymmetric flow control 550
audience 15
authentication-type 1392
authentication-type simple 1392
auto-cost 963
auto-cost (OSPF) 963
auto-negotiation 563
Autonomous System. See AS.
auto-summary 1168

B

bandwidth-percentage 1123
bandwidth-percentage (policy QoS) 1123
base VLAN 1091
BFD 281
bfd all-neighbors 283
bfd disable 281
bfd enable 282
bfd interval 282
bfd neighbor 284
bfd protocol-liveness 285
BGP 293, 701
 bgp four-octet-as-support 306, 711
 passive peering 337, 741
 soft reconfiguration 717, 718
bgp add-path 297
bgp always-compare-med 298, 705
bgp always-compare-med (BGP IPv6) 705

bgp asnotation 298
 bgp bestpath as-path ignore 299, 705
 bgp bestpath as-path ignore (BGP IPv6) 705
 bgp bestpath med confed 299, 706
 bgp bestpath med confed (BGP IPv6) 706
 bgp bestpath med missing-as-best 300
 bgp bestpath med missing-as-best (BGP IPv6) 706
 bgp bestpath router-id-ignore 300
 bgp client-to-client reflection 301, 706
 bgp client-to-client reflection (BGP IPv6) 706
 bgp cluster-id 301, 311, 312, 707, 716
 bgp cluster-id (BGP IPv6) 707
 bgp confederation identifier 302, 708
 bgp confederation identifier (BGP IPv6) 708
 bgp confederation peers 303, 708
 bgp confederation peers (BGP IPv6) 708
 bgp dampening 304, 374, 709, 763
 bgp dampening (BGP IPv6) 709, 763
 bgp dampening (MBGP) 374
 bgp default local-preference 305, 710
 bgp default local-preference (BGP IPv6) 710
 bgp enforce-first-as 305, 710
 bgp fast-external-fallover 306, 711
 bgp fast-external-fallover (BGP IPv6) 711
 bgp graceful-restart 307, 712
 bgp graceful-restart (BGP IPv6) 712
 bgp log-neighbor-changes 307, 712
 bgp log-neighbor-changes (BGP IPv6) 712
 bgp non-deterministic-med 308, 713
 bgp non-deterministic-med (BGP IPv6) 713
 bgp recursive-bgp-next-hop 308, 713
 bgp regex-eval-optz-disable 309, 714
 bgp router-id 310, 715
 bgp router-id (BGP IPv6) 715
 bgp soft-reconfig-backup 311, 375, 715
 boot change 62, 64
 boot change command 62
 boot messages 63
 boot messages command 63
 boot selection 64
 boot selection command 64
 boot zero command 64
 boot, interrupting 61
 BOOT_ADMIN mode (was BOOT_USER) 61
 BOOT_USER mode 61
 BPDU 904, 1110, 1200, 1348
 break sequence 61
 Bridge Protocol Data Units. *See* *BPDU*.
 bridge-priority 1345
 bridge-priority (RSTP) 1198
 Broadcast/Unknown Unicast Rate Limiting 1337
 bsr 1066
 BTM 1428, 1471
 Buffer Traffic Manager (BTM) 1428, 1471

Bulk Configuration
 see interface range 554
 Bulk Configuration Macro
 see interface range macro 556

C

calendar set 1356
 call-home 477
 call-home service 475
 CAM (Content Addressable Memory) 847
 cam ipv4flow command 426
 cam l2acl command 429
 CAM Profiling
 Important Points to Remember 409, 415
 cam-ipv4flow command 426
 cam-l2acl command 429
 cam-optimization 417
 cam-profile ipv4-vrf 1381, 1383, 1385
 cam-profile microcode command 418
 capture bgp-pdu max-buffer-size 312
 capture bgp-pdu max-buffer-size (BGP IPv6) 716
 capture bgp-pdu neighbor 311
 capture bgp-pdu neighbor (BGP IPv6) 716
 card type 95
 card-type 95
 case-number command 478
 channel-member 594
 class-map (policy QoS) 1124
 clear arp-cache 610
 clear bfd counters 285
 clear command history 80
 clear config 790
 clear config (ISIS) 790
 clear counters 542
 clear counters ip access-group (common IP ACL) 190
 clear counters ip trace-group 1253
 clear counters mac access-group 231
 clear counters vrrp 1393, 1403
 clear dampening 543
 clear frp 468
 clear gvrp statistics interface 506
 clear hardware btm 1428, 1471
 clear hardware rpm mac counters 1428, 1472
 clear host 611
 clear host (DNS) 611
 clear ip bgp 312, 376, 720
 clear ip bgp (BGP IPv6) 717, 718
 clear ip bgp * (asterisk) 312, 716
 clear ip bgp * (BGP IPv6) 717
 clear ip bgp dampening 313
 clear ip bgp flap-statistics 314
 clear ip igmp groups 526
 clear ip mroute 915, 916, 924

- clear ip ospf 963
- clear ip ospf statistics 964
- clear ip pim rp-mapping 1044
- clear ip pim tib 1044
- clear ip prefix-list 243
- clear ip rip 1168
- clear ip route 612
- clear ipv6 neighbor 932
- clear ipv6 ospf process 1016
- clear isis 791
- clear lacp port 829
- clear logging 1300
- clear mac-address-table dynamic 836
- clear qos statistics (policy QoS) 1125
- clear queue statistics egress (QoS) 1157
- clear queue statistics ingress (QoS) 1158
- clear tcp statistics 613
- CLI
 - case sensitivity 20
 - partial keywords 20
- CLI Modes
 - AS-PATH ACL 24
 - CONFIGURATION 22
 - EXEC 22
 - EXEC Privilege 22
 - INTERFACE 22
 - IP ACCESS LIST 24
 - IP COMMUNITY LIST 25
 - LINE 23
 - MAC ACCESS LIST 23
 - MULTIPLE SPANNING TREE 26
 - PREFIX-LIST 24
 - REDIRECT-LIST 25
 - ROUTE-MAP 24
 - ROUTER BGP 27
 - ROUTER ISIS 27
 - ROUTER OSPF 26
 - ROUTER RIP 26
 - SPANNING TREE 25, 26
 - TRACE-LIST 23
- cli-command (FTSA command) 479
- cli-debug (FTSA command) 479
- cli-show (FTSA command) 480
- clns host 791
- clns host (ISIS) 791
- clock read-calendar 1356
- clock set 1357
- clock source 1313
- clock summer-time date 1358
- clock summer-time recurring 1359
- clock timezone 1360
- clock update-calendar 1360
- Command Modes 22
- command modes 18
- community port 1092
- community VLAN 1091
- conf confirm 434
- conf replace 434
- conf terminal 434
- CONFIGURATION (conf-callhome) mode 477
- CONFIGURATION mode 22
- configuration mode exclusive 435
- Configuration Rollback
 - archive 432
 - archive backup 432
 - archive config 432
 - conf confirm 434
 - conf replace 434
 - conf terminal 434
 - configuration mode exclusive 435
 - maximum (number) 436
 - show archive 437
 - show run diff 438
 - time-period 439
- configuration, multiple users 17
- contact-address 480, 482
- contact-name 481
- contact-notes 481
- Content Addressable Memory (CAM) 847
- contiguous subnet masks 194
- continue (Route Map) 250
- control break sequence 61
- copy (Streamline Upgrade) 36
- copy running-config startup-config duplicate 37
- Core Dump Files
 - naming conventions 1411, 1455
- Core-Dump 41
- CPU Traffic Statistics 81, 108
- crypto key generate 1242
- CX4-cable-length command 544

D

- dampen (FTSA command) 482
- dampening 545
- dataplane-diag disable dfo-reporting 1409, 1452
- dataplane-diag disable loopback 1408, 1450
- dataplane-diag disable sfm-bringdown 1451
- dataplane-diag disable sfm-walk 1451
- debug arp 613
- debug bfd 286
- debug callhome 482
- debug fefd 461
- debug firp 468
- debug gvrp 507
- debug ip bgp 314, 316, 317, 377, 723
- debug ip bgp (BGP IPv6) 721
- debug ip bgp (ipv6) 721

debug ip bgp dampening 315
 debug ip bgp events 316, 722
 debug ip bgp events (BGP IPv6) 722
 debug ip bgp events (ipv6) 722
 debug ip bgp ipv4 multicast dampening (MBGP) 377
 debug ip bgp ipv6 dampening 722
 debug ip bgp ipv6 unicast dampening 722, 765
 debug ip bgp ipv6 unicast updates 765, 766
 debug ip bgp keepalives 316, 723
 debug ip bgp keepalives (BGP IPv6) 723
 debug ip bgp modify 317, 724
 debug ip bgp notifications (BGP IPv6) 724
 debug ip bgp peer-group updates (MBGP) 378
 debug ip bgp soft-reconfiguration 317
 debug ip bgp updates 318, 378, 724, 765
 debug ip bgp updates (BGP IPv6) 724
 debug ip dhcp 614
 debug ip icmp 615
 debug ip igmp 526
 debug ip ospf 964
 debug ip packet 616
 debug ip pim 1045, 1065
 debug ip rip 1169
 debug ip ssh 1243
 debug ip udp-helper 605
 debug ipv6 ospf packet 1016
 debug isis 791
 debug isis adj-packets 792
 debug isis local-updates 792, 793
 debug isis snp-packets 793
 debug isis spf-triggers 793
 debug isis update-packets 793
 debug lacp 830
 debug ntp 1361
 debug ppp 1313
 debug protocol-tunnel 1268
 debug radius 1226
 debug spanning-tree 1346
 debug spanning-tree mstp 902
 debug spanning-tree rstp 1198
 debug tacacs+ 1231
 debug track (Object Tracking) 940
 debug vrrp 1393, 1404
 default logging buffered 1301, 1303
 default logging console 1301
 default logging monitor 1301
 default logging trap 1302, 1308
 Default VLAN 854
 default vlan-id 854
 default-action 483
 default-gateway 65
 default-gateway command 65
 default-information originate 966
 BGP 318
 IS-IS 794
 OSPF 966
 RIP 1169
 default-information originate (ISIS) 794
 default-information originate (OSPF IPv6) 1017
 default-information originate (RIP) 1169
 default-metric
 BGP 318, 725
 OSPF 967
 RIP 1170
 default-metric (BGP IPv6) 725
 default-metric (BGP) 318
 default-metric (OSPF) 967
 default-metric (RIP) 1170
 default-test 483
 define interface range macro 556
 delay (Object Tracking) 940
 delay triggers line 1314
 delete
 BOOT_USER mode 65
 EXEC privilege mode 37
 delete command 65
 Denial of Service 1253
 deny 1254
 AS-Path Access list 267
 extended IP ACL 200
 IP ACL (standard) 194
 standard IP ACL 194
 Trace list 1254
 deny (AS-Path) 267
 deny (BGP) 400
 deny (Extended MAC ACL) 237
 deny (IP Community List) 270
 deny (IP prefix ACL) 243
 deny (standard MAC ACL) 233
 deny arp (extended IP ACL) 202
 deny ether-type 203
 deny ether-type (extended IP ACLs) 203
 deny icmp (extended IP ACLs) 205
 deny regex (BGP) 400
 deny tcp 1254
 IP ACL 208
 Trace list 1254
 deny tcp (extended IP ACLs) 208
 deny udp 1255
 IP ACL 210
 Trace list 1255
 deny udp (extended IP ACLs) 210
 description 1033, 1126
 ACL 188
 INTERFACE 546
 VRRP 1394, 1404
 description (ACL) 188
 description (BGP) 401

- description (FRRP) 469
- description (interface) 546
- description (Object Tracking) 941
- description (OSPF) 967
- description (Route Map) 251
- description (VLAN) 853, 967
- description (VRRP) 1394
- description command (ACL VLAN) 276
- description, spanning-tree 319, 484, 726, 795, 902, 1086, 1102, 1171, 1199, 1347
- DHCP 621, 622
 - UDP ports 621
- DHCP broadcast messages 621
- DHCP server 621
- diag linecard 1425, 1453, 1469
- diag sfm 1410, 1453
- dir
 - BOOT_USER mode 66
 - EXEC privilege mode 38
- dir command 66
- disable
 - Spanning Tree Protocol 795, 902, 1102, 1199, 1347
 - VRRP 1394
- disable (FRRP) 469
- disable (GVRP) 507
- disable (MSTP) 903
- disable (PVST+) 1102
- disable (RSTP) 1199
- disable (STP) 1347
- disable (VRRP) 1394
- disable-on-sfm-failure
 - INTERFACE 547
- disable-on-sfm-failure (interface) 547
- discontiguous subnet masks 194
- display parameter 21
- distance
 - IS-IS 795
 - OSPF 968
 - RIP 1171
- distance (ISIS) 795
- distance (OSPF) 968
- distance (RIP) 1171
- distance bgp 319, 484, 726
- distance bgp (BGP IPv6) 726
- distance bgp (IPv6) 766
- distance bgp (MBGP) 379
- distance ospf 968
- distribute-list (ISIS) 796
- distribute-list (OSPF) 969, 970
- distribute-list (RIP) 1172
- distribute-list in
 - IS-IS 796
 - OSPF 969
 - RIP 1172

- distribute-list out
 - IS-IS 796
 - OSPF 970
 - RIP 1172
- distribute-list redistributed-override (ISIS) 797
- distribute-list redistributed-override in
 - IS-IS 797
- DNS commands 619, 624, 687
- do 83
- Document conventions 15
- domain-name 484
- domain-password 798
- domain-password (ISIS) 798
- DOS 1253
- dot1p-priority 1114
- dot1p-priority (QoS) 1114
- dot1x auth-fail-vlan 176, 1235
- dot1x auth-server radius 176, 1236
- dot1x guest-vlan 177, 179, 1236
- dot1x max-eap-req 178, 1237
- dot1x port-control 179, 1237
- dot1x quiet-period 180, 1238
- dot1x reauthentication 180, 1238
- dot1x reauth-max 180, 1239
- dot1x server-timeout 181, 1239
- dot1x supplicant-timeout 181, 1240
- dot1x tx-period 182, 1240
- download alt-boot-image 38
- down-when-looped 1315
- duplex 547, 548
- duplex (Management) 547
- duplex flow control 549
- dynamic LAG 593

E

- ECMP 455, 458
- egress ACLs 191
- email addresses
 - FTSA Administrator 477, 478
 - FTSA recipient, ftsa@force10networks.com 493
- email encryption keys 497
- email messages from the switch 475
- enable 66, 83, 485
- enable (CAM-profile template) 410
- enable command 66
- enable inverse mask
 - OSPF 970
- enable inverse mask (OSPF) 970
- Enable password 22
- enable password 1218, 1219
- enable restricted 1219
- enable-all 486
- encap 1315

- encrypt 486
- encryption keys, email 497
- end 84
- except parameter 21
- EXEC mode 22
- exec-banner 86
- exec-timeout 86
- exit 87
- extended MAC ACL 239
- external flash, number of files supported 35

F

- Far-End Failure Detection (FEFD) 461
- fast-convergence
 - OSPF 971
- fast-convergence (OSPF) 971
- fefd 462
- fefd disable 463
- fefd interval 463
- fefd mode 462
- fefd reset 464
- fefd-global 462
- fefd-global interval 464
- File naming convention
 - application core-dump 1411, 1455
- files, number supported on external flash 35
- find parameter 21
- flood-2328 (OSPF) 971
- flow (cam-profile template) 411
- flow control values 551
- flow control, asymmetric 550
- flow control, duplex 549
- flow-based enable 1086
- flowcontrol 549
- Force10 Service Agent (FTSA) 475
- format 67
- format (C-Series and E-Series) 40
- format command 67
- format flash (S-Series) 40
- forward-delay 1347
- forward-delay (MSTP) 903
- forward-delay (RSTP) 1200
- forward-delay (STP) 1347
- Forwarding Information Base (FIB) entries 639, 640
- framing 1316
- frequency 487
- ftp-server enable 87
- ftp-server topdir 88
- ftp-server username 88
- FTSA (Call Home), start 477
- FTSA commands 486
 - action-list 476
 - admin-email 477

- call-home 477
- case-number 478
- debug callhome 482
- domain-name 484
- enable 485
- enable-all 486
- frequency 487
- keyadd 487
- recipient 493
- server 495
- show configuration 496
- show debugging 496
- show keys 497
- smtp server-address 497

G

- GARP (Generic Attribute Registration Protocol) 505
- garp timers 508
- GARP VLAN Registration Protocol. See GVRP.
- GID (GARP Information Declaration) 505
- GIP (GARP Information Propagation) 505
- graceful-restart
 - OSPF 972, 973
- graceful-restart grace-period
 - OSPF 972
- graceful-restart grace-period (OSPF) 972
- graceful-restart helper-reject
 - OSPF 972
- graceful-restart helper-reject (OSPF) 972
- graceful-restart ietf
 - IS-IS 798
- graceful-restart interval
 - IS-IS 799
- graceful-restart mode
 - OSPF 973
- graceful-restart mode (OSPF) 973
- graceful-restart restart-wait
 - IS-IS 801
- graceful-restart role
 - OSPF 973
- graceful-restart role (OSPF) 973
- graceful-restart t1
 - IS-IS 799
- graceful-restart t2
 - IS-IS 800
- graceful-restart t3
 - IS-IS 800
- grep command option 21
- grep parameter 21
- group (LAG sharing) 595
- group (LAG) 595
- GVRP 26
- GVRP (GARP VLAN Registration Protocol) 505

gvrp enable 509
gvrp registration 509

H

HA commands 515
hardware monitor mac 1429, 1473
hardware monitor mac action-on-error port-shutdown 1316
hardware watchdog 1430, 1473
Hash Message Authentication Code (HMAC) 790
hash-algorithm ecmp (C-Series and S-Series) 458
hello padding (ISIS) 801
hello-time 1348
hello-time (MSTP) 904
hello-time (RSTP) 1200
hello-time (STP) 1348
hitless 515
hitless dynamic LACP states 829
hitless protocol 515
hitless upgrade 518
HMAC (Hash Message Authentication Code) 790
hold-time 1395
hold-time (VRRP) 1395
hostname 89
hostname dynamic 802
hostname dynamic (ISIS) 802

I

ICMP 627
IEEE 802.1d 1101
IETF Draft draft-ietf-bfd-base-03 281
IETF RFCs
 1058 1167
 2328 958
 2453 1167
 2966 790
IFM (interface management) 140
IGMP Snooping 534
 Important Things to Remember for IGMP Querier 535
 Important Things to Remember for IGMP
 Snooping 535
IGMP Snooping Commands 534
ignore enable-password 67, 68
ignore enable-password command 67
ignore startup-config command 68
ignore-case sub-option 21
ignore-lsp-errors 802
ignore-lsp-errors (ISIS) 802
IGP (Interior Gateway Protocol) 957
ingress ACLs 191
interface 551
 interface command 551
interface (FRRP) 470
interface loopback 552

interface management (IFM) 140
interface management ethernet ip address 68, 69
interface management ethernet ip address command 68, 69
interface management ethernet mac-address command 69
interface management ethernet port command 69
interface management port config 70
interface management port config command 70
interface ManagementEthernet 553
interface null 553
interface port-channel 596
interface range 554
interface range macro 557
interface rate-interval 566
interface sonet 1316
interface suppress threshold (dampening) 546
Interface vlan 558
interface vlan 558
Interior Gateway Protocol (IGP) 957
Internet Control Message Protocol. See ICMP.
ip access-group 276
ip access-group (common IP ACL) 191
ip access-list extended 212
ip access-list extended (extended IP ACLs) 212
ip access-list standard 195
ip address 618
ip as-path access-list 267
ip community-list 271
ip control-plane egress-filter-traffic 1410, 1454
ip default-network 619
ip directed-broadcast 618
ip domain-list 619
ip domain-lookup 619
ip domain-name 620
IP DSCP bit 1141
ip extcommunity-list (BGP) 401
ip fib download-igp-only 621
ip ftp password 89
ip ftp source-interface 90
ip ftp username 91
ip helper-address 621
ip helper-address hop-count disable 622
ip host 622, 687
ip igmp access-group 527
ip igmp immediate-leave 528
ip igmp last-member-query-interval 528
ip igmp querier-timeout 529
ip igmp query-interval 529
ip igmp query-max-resp-time 530
ip igmp static-group 531
ip local-proxy-arp command 1092
ip max-frag-count 623
ip mroute 916
ip mtu 623
ip multicast-lag-hashing 917

- ip multicast-limit 918
- ip multicast-routing 917, 918, 925
- ip name-server 624, 687
- ip ospf auth-change-wait-time 974
 - OSPF 974
- ip ospf authentication-key 974
- ip ospf cost 975
- ip ospf dead-interval 975
- ip ospf hello-interval 976
- ip ospf message-digest-key 976
- ip ospf mtu-ignore 977
- ip ospf network 977
- ip ospf priority 978
- ip ospf retransmit-interval 978
- ip ospf transmit-delay 979
- ip pim dr-priority 1047, 1066
- ip pim query-interval 1049, 1067
- ip pim rp-address 1050
- ip poison-reverse 1173
- ip poison-reverse (RIP) 1173
- ip prefix-list 244
- ip proxy-arp 625
- ip radius source-interface 1226
- ip redirect-group 1033, 1034
- ip redirect-list 1034
 - description 1033
- ip redirects 625
- ip rip receive version 1174
- ip rip send version 1174
- ip route 626
- ip route bfd 287
- ip router isis 802
- ip scp topdir 1244
- ip source-route 627
- ip split-horizon 1175
- ip split-horizon (RIP) 1175
- ip ssh authentication-retries 1244
- ip ssh connection-rate-limit 1245
- ip ssh hostbased-authentication enable 1245
- ip ssh key-size 1246
- ip ssh password-authentication enable 1246
- ip ssh pub-key-file 1247
- ip ssh rhostsfile 1247
- ip ssh rsa-authentication 1249
- ip ssh rsa-authentication enable 1248
- ip ssh server 1249
- ip ssh server enable 1249
- ip tacacs source-interface 1231
- ip telnet server enable 91
- ip telnet source-interface 92
- ip tftp source-interface 93
- IP trace lists 1253
- ip trace-group 1256
- ip trace-list 1257
- ip udp-broadcast-address 605
- ip udp-helper udp-port 606
- ip unreachable 627
- ip vlan-flooding 628
- ip-redirect-list 1034
- IPv6
 - clear ipv6 fib 685
- IPv6 ACLs 657
 - cam-acl 416, 417, 658
 - clear counters ipv6 access-group 659
 - deny icmp 660
 - deny tcp 661
 - deny udp 663
 - ipv6 access-group 665
 - ipv6 access-list 666
 - permit 666
 - permit icmp 667
 - permit tcp 668
 - permit udp 670
 - remark 672
 - resequence access-list 672
 - resequence prefix-list ipv6 673
 - seq 674
 - show cam-acl 675
 - show config 676
 - show ipv6 accounting access-list 677
 - show running-config acl 678
- ipv6 control-plane egress-filter-traffic 1454
- ipv6 nd managed-config-flag 932
- ipv6 nd max-ra-interval 933
- ipv6 nd other-config-flag 934
- ipv6 nd prefix 934
- ipv6 nd ra-lifetime 935
- ipv6 nd reachable-time 935
- ipv6 nd suppress-ra 936
- ipv6 neighbor 936
- ipv6 ospf 1018
- ipv6 ospf cost 1020
- ipv6 ospf dead-interval 1021
- ipv6 ospf hello-interval 1022
- ipv6 ospf priority 1022
- IPv6 PIM debugging, set 1065
- IPv6 PIM Router-Query messages, set frequency 1067
- IPv6 PIM sparse mode, enable 1070
- IPv6 Route Map
 - match ipv6 address 680
 - match ipv6 next-hop prefix-list 681
 - match ipv6 route-source prefix-list 681
 - route-map 682
 - set ipv6 next-hop 682
 - show config 683
 - show route-map 683
- ipv6 router isis (ISIS_IPv6) 803
- ipv6 router ospf 1023

IS-IS

- isis hello padding 806
- isis bfd all-neighbors 287
- isis circuit-type 803
- IS-IS commands 787
- isis csnp 804
- isis csnp-interval 804
- isis hello padding 806
- isis hello-interval 805
- isis hello-multiplier 805
- isis ipv6 metric 806
- isis metric 806, 807
- isis network point-to-point 807
- isis password 807
- isis priority 808
- isolated port 1092
- isolated VLAN 1091
- is-type 809
- is-type (ISIS) 809

K

- keepalive 558, 1317
- kernel core-dump 1411, 1455
- keyadd 487

L

- L2PT (Layer 2 Protocol Tunneling) 1267

LACP

- clear lacp counters 829
- debug lacp 830
- lacp port-priority 831
- port-channel mode 832
- port-channel-protocol lacp 833
- show lacp 833
- lacp system-priority 832

LAG

- channel-member 594
- group 595
- interface port-channel 596
- minimum-links 597
- port-channel failover-group 597
- show interfaces port-channel 598
- show port-channel-flow 600
- LAG failover group 597
- LAG failover-group 599
- LAG fate-sharing group 599
- LAG supergroup 595
- LAGs 829
- Layer 2 Protocol Tunneling (L2PT) 1267
- layer-2 (cam-profile template) 411
- layer-3 (cam-profile template) 411, 412
- line 94
- linecard 95

- Link Aggregation Control Protocol (LACP) 829

- link debounce interface 559

- Link Layer Detection Protocol (LLDP) 863

- Link State Advertisements. See LSA.

- link-state protocol 957

- LLDP 863

- LLDP-MED (Media Endpoint Discovery) 871

- load-balance 628, 629

- log-adjacency-changes 809, 979

- log-adjacency-changes (ISIS) 809

- logging 1302

- logging buffered 1303

- logging console 1303

- logging coredump kernel disable 1411, 1455

- logging coredump kernel server 1412, 1455

- logging coredump linecard 1412, 1456

- logging facility 1304

- logging history 1305

- logging history size 1305

- logging monitor 1306

- logging on 1306

- logging source-interface 1307

- logging synchronous 1308

- logging trap 1308

- login authentication 1220

- log-messages 488

- log-only 489

- loopback 1317

- lp pim bsr-border 1046

- LSA 961, 978

- lsp-gen-interval 809

- lsp-gen-interval (ISIS) 809

- lsp-mtu 810

- lsp-mtu (ISIS) 810

- lsp-refresh-interval 811

- lsp-refresh-interval (ISIS) 811

M

- mac access-group 231

- mac access-list extended (Extended MAC ACL) 239

- mac access-list standard (standard MAC ACL) 234

- mac accounting destination 836

- MAC ACL, extended 239

- MAC address station-move trap 838

- mac cam fib-partition 840

- mac learning limit (dynamic or no-station-move) 840

- mac learning-limit 840

- mac learning-limit learn-limit-violation 842

- mac learning-limit reset 843

- mac learning-limit station-move-violation 842

- mac-address-table aging-time 837

- mac-address-table static 838

- mac-address-table station-move 838

- mac-address-table station-move refresh-arp 839
- mac-address-table station-move threshold 838, 839
- Management interface 553, 694
- management route 631
- Management static route 631
- management unit, S-Series 1330
- master unit, S-Series 1330
- match (FTSA command) 490
- match as-path (Route Map) 251
- match community (Route Map) 252
- match extcommunity (BGP) 402
- match interface (Route Map) 252
- match ip access-group 1125
- match ip access-group (policy QoS) 1125
- match ip address (Route Map) 253
- match ip dscp 1127
- match ip dscp (policy QoS) 1127
- match ip next-hop (Route Map) 254
- match ip precedence 1128
- match ip precedence (policy QoS) 1128
- match ip route-source (Route Map) 254
- match mac access-group (policy QoS) 1129
- match mac dot1p (policy QoS) 1129, 1130
- match metric (Route Map) 255
- match origin (Route Map) 255
- match route-type (Route Map) 256
- match tag (Route Map) 256
- max-age 1348
- max-age (MSTP) 904
- max-age (RSTP) 1201
- max-age (STP) 1348
- max-area-addresses 812
- max-area-addresses (ISIS) 812
- max-hops (MSTP) 905
- maximum (number) 436
- maximum-paths 980
 - BGP 320, 727
 - IS-IS 813, 814
 - OSPF 980
 - RIP 1175
- maximum-paths (BGP IPv6) 727
- maximum-paths (BGP) 320
- maximum-paths (ISIS) 813
- maximum-paths (RIP) 1175
- max-lsp-lifetime 812
- max-lsp-lifetime (ISIS) 812
- MBGP Commands 371, 761
- Media Endpoint Discovery 871
- member 1373
- member (Stackable VLAN) 1373
- member vlan command 277
- member-vlan (FRRP) 471
- message-format (FTSA command) 490
- metric-style 813

- metric-style (ISIS) 813
- mib-binding 980
- microcode (cam-profile template) 412
- minimum-links 597
- mode (FRRP) 471
- modes, command 18
- module power-off 96
- monitor interface 559
- monitor session 1087
- motd-banner 96
- MSDP 891
- msti (MSTP) 905
- MSTP 901
 - debug spanning-tree mstp 902
- mtrace 920
- mtu 562
- Multicast Source Discovery Protocol
 - see MSDP 891
- MULTIPLE SPANNING TREE 26
- Multiple Spanning Tree Protocol 901
 - see MSTP 901
- Multiprotocol BGP (MBGP) 371
- multi-topology (ISIS) 814

N

- name (MSTP) 906
- name (VLAN) 856
- Naming conventions
 - Core dump files 1411, 1455
- NDP 931
- negotiation auto 563
- neighbor 1176
- neighbor (RIP) 1176
- neighbor activate (BGP IPv6) 727, 767
- neighbor activate (BGP) 321
- neighbor activate (MBGP) 380
- neighbor advertisement-interval (BGP IPv6) 728, 768
- neighbor advertisement-interval (BGP) 322, 327
- neighbor advertisement-interval (MBGP) 380
- neighbor advertisement-start(BGP) 322
- neighbor allowas-in 323, 729
- neighbor allowas-in (BGP) 323, 729
- neighbor default-originate 323, 729
- neighbor default-originate (BGP IPv6) 729, 768
- neighbor default-originate (BGP) 323
- neighbor default-originate (MBGP) 381
- neighbor description 324, 730
- neighbor description (BGP IPv6) 730
- neighbor description (BGP) 324
- Neighbor Discovery Protocol 931
- neighbor distribute-list 324, 730
- neighbor distribute-list (BGP IPv6) 730, 769
- neighbor distribute-list (BGP) 324

- neighbor distribute-list (MBGP) 381
- neighbor ebgp-multihop 325, 731
- neighbor ebgp-multihop (BGP IPv6) 731
- neighbor ebgp-multihop (BGP) 325
- neighbor fall-over (BGP) 325
- neighbor filter-list 326, 732
- neighbor filter-list (BGP IPv6) 732
- neighbor filter-list (BGP) 326
- neighbor filter-list aspath (BGP IPv6) 769
- neighbor filter-list aspath (MBGP) 382
- neighbor graceful-restart 327
- neighbor graceful-restart (BGP) 327
- neighbor local-as 327
- neighbor maximum-prefix 328, 733
- neighbor maximum-prefix (BGP IPv6) 733, 770
- neighbor maximum-prefix (BGP) 328
- neighbor maximum-prefix (MBGP) 383
- neighbor next-hop-self 329, 734
- neighbor next-hop-self (BGP IPv6) 734, 770
- neighbor next-hop-self (BGP) 329
- neighbor next-hop-self (MBGP) 383
- neighbor password 329
- neighbor password (BGP) 329
- neighbor peer-group 330, 331, 735, 736
- neighbor peer-group (BGP IPv6) 735
- neighbor peer-group (BGP) 330, 331
- neighbor peer-group (creating group) (BGP IPv6) 736
- neighbor peer-group passive (BGP IPv6) 736
- neighbor peer-group passive (BGP) 332
- neighbor remote-as 333, 737
- neighbor remote-as (BGP IPv6) 737
- neighbor remote-as (BGP) 333
- neighbor remove-private-as 333, 737
- neighbor remove-private-as (BGP IPv6) 737, 771
- neighbor remove-private-as (BGP) 333
- neighbor remove-private-as (MBGP) 384
- neighbor route-map 334, 738
- neighbor route-map (BGP IPv6) 738
- neighbor route-map (BGP) 334
- neighbor route-map (MBGP) 384
- neighbor route-reflector-client (BGP IPv6) 739, 772
- neighbor route-reflector-client (BGP) 335
- neighbor route-reflector-client (MBGP) 385
- neighbor send-community 335, 739
- neighbor send-community (BGP IPv6) 739
- neighbor send-community (BGP) 335
- neighbor shutdown 336, 740
- neighbor shutdown (BGP IPv6) 740
- neighbor shutdown (BGP) 336
- neighbor soft-reconfiguration inbound (BGP) 336, 385, 740
- neighbor subnet 741
- neighbor subnet (BGP IPv6) 741
- neighbor subnet (BGP) 337
- neighbor timers 337, 742
- neighbor timers (BGP IPv6) 742
- neighbor timers (BGP) 337
- neighbor update-source 338, 742
- neighbor update-source (BGP) 338
- neighbor update-source loopback (BGP IPv6) 742
- neighbor weight 339, 743
- neighbor weight (BGP IPv6) 743
- neighbor weight (BGP) 339
- net 814
- network
 - BGP 339, 387, 744, 773
 - RIP 1176
- network (BGP IPv6) 744, 773
- network (BGP) 339
- network (MBGP) 387
- network (OSPF) 981
- network (RIP) 1176
- network area
 - OSPF 981
- network backdoor 340, 744
- network backdoor (BGP IPv6) 744
- network backdoor (BGP) 340
- Network Time Protocol (NTP) 1355
- Network Time Protocol. *See* NTP.
- NIC Teaming 839
- no-more 21
- no-more parameter 21
- non-contiguous subnet masks 194
- Not So Stubby Area. *See* NSSA.
- NSSA 960
- NTP 1361
- NTP (Network Time Protocol) 1355
- ntp authenticate 1361
- ntp authentication-key 1362
- ntp broadcast client 1362
- ntp disable 1363
- ntp multicast client 1364
- ntp server 1364
- ntp source 1365
- ntp trusted-key 1365
- ntp update-calendar 1366

O

- Object tracking
 - overview 939
- offline 1425, 1469
- Offline Diagnostics 1424, 1468
- offset-list 1177
- offset-list (RIP) 1177
- online 1426, 1470
- OSPF
 - clear ipv6 ospf process 1016

- clear ospfv3 process 1016
- ipv6 ospf area 1018
- ipv6 router ospf 1023
- link-state 957
- show ipv6 ospf database 1029
- show ipv6 ospf neighbor 1031
- output-delay 1177
- output-delay (RIP) 1177

P

- Packet Over SONET/SDH (POS/SDH) 1311

- passive-interface

- IS-IS 814

- OSPF 981

- RIP 1178

- passive-interface (ISIS) 814

- passive-interface (OSPF IPv6) 1023

- passive-interface (OSPF) 981

- passive-interface (RIP) 1178

- password 1221

- password, Enable 22

- pause frames 549

- PBR 1033

- PBR (Policy-Based Routing) 1273

- permit 1257

- IP ACL (extended) 213

- Trace list 1257

- permit (AS-Path) 268

- permit (BGP) 402

- permit (extended IP ACLs) 213

- permit (Extended MAC ACL) 240

- permit (IP Community List) 271

- permit (IP prefix ACL) 245

- permit (redirect list) 1035

- permit (standard MAC ACL) 235

- permit arp 214

- permit arp (extended IP ACLs) 214

- permit ether-type 216

- permit ether-type (extended IP ACLs) 216

- permit icmp (extended IP ACLs) 217

- permit regex (BGP) 403

- permit tcp 1258

- IP ACL 219

- Trace list 1258

- permit tcp (extended IP ACLs) 219

- permit udp 1259

- IP ACL 221

- Trace list 1259

- permit udp (extended IP ACLs) 221

- per-port QoS 1114

- PGP keys 497

- PIM

- Sparse-Mode 1043

- PIM-SM 891

- ping 96

- PoE (Power over Ethernet) chapter 1079

- Point-to-Point Protocol (PPP) encapsulation 1311

- policy (FTSA command) 491

- policy-action-list (FTSA command) 492

- policy-aggregate (policy QoS) 1130

- Policy-Based QoS 1122

- Policy-based Routing (PBR) 1033

- Policy-map

- description 1126

- policy-map-input 1131

- policy-map-input (policy QoS) 1131

- policy-map-output (policy QoS) 1132

- policy-test-list 492

- policy-test-list (FTSA command) 492

- Port Channel-Specific Commands 593

- Port Mirroring

- Important Points to Remember 1085

- port types (private VLAN) 1092

- port-based QoS 1114

- port-channel failover-group 597

- port-channel mode 832

- port-channel supergroup 595

- port-channel-protocol lacp 833

- port-channels 829

- Port-Channel-Specific Commands 593

- portmode hybrid command 565

- power budget 1079

- power inline 1080, 1081

- power inline priority 1080

- Power over Ethernet (PoE) chapter 1079

- power-{off | on} sfm 1413, 1457

- power-off 99

- power-on 99

- ppp authentication 1318

- ppp chap hostname 1319

- ppp chap password 1319

- ppp chap rem-hostname 1320

- ppp chap rem-password 1320

- PPP encapsulation 1311

- ppp next-hop 1321

- ppp pap hostname 1321

- ppp pap password 1321

- ppp pap rem-hostname 1322

- ppp pap rem-password 1322

- preemphasis, CX4 cable length 544

- preempt 1395

- preempt (VRRP) 1395

- PREFIX-LIST Mode 24, 25

- primary port 600

- primary VLAN 1091

- priority 1396

- priority (VRRP) 1396

- private VLANs (PVLANS) 632
- private-vlan mapping secondary-vlan command 1094
- private-vlan mode command 1093
- privilege exec 1213
- privilege level (CONFIGURATION mode) 1213
- privilege level (LINE mode) 1213
- pr-number (FTSA command) 493
- promiscuous port 1092
- PROTOCOL
 - Per-VLAN SPANNING TREE Mode 25
 - SPANNING TREE Mode 25
- protocol frp (FRRP) 471
- protocol gvrp 510
- PROTOCOL GVRP Mode 26
- PROTOCOL MULTIPLE SPANNING TREE Mode 26
- protocol route 631
- protocol spanning-tree 1349
- protocol spanning-tree mstp 906
- protocol spanning-tree pvst (PVST+) 1103
- protocol spanning-tree rstp 1201
- protocol, hitless 515
- protocol-tunnel enable 1269
- protocol-tunnel rate-limit 1270
- protocol-tunnel stp 1268, 1269
- provision type 1334
- PVST+ (Per-VLAN Spanning Tree plus) 1101

Q

- QinQ 1371
- QoS
 - clear qos statistics 1125
 - Per Port 1114
 - Policy-Based 1122
 - rate-limit 1136
 - threshold 1154
- QoS, per-port 1114
- QoS, port-based 1114
- qos-policy-input 1133
- qos-policy-input (policy QoS) 1133
- qos-policy-output 1134
- queue egress multicast linecard (policy QoS) 1135
- queue ingress multicast (policy QoS) 1134, 1136
- Queue Level Debugging 1157
 - clear queue statistics ingress 1157, 1158
 - show queue statistics egress 1158
- Queuing Statistics 1157

R

- radius-server deadtime 1227
- radius-server host 1227
- radius-server key 1229
- radius-server retransmit 1229
- radius-server timeout 1230

- RAPID SPANNING TREE Mode 26
- rate limit 1115
- rate limit (QoS) 1115
- rate police (QoS) 1116
- rate shape (QoS) 1117
- rate-interval 566
- rate-limit 1136
- rate-police 1137
- rate-shape (policy QoS) 1138
- recipient 493
- redirect 1036
- redirect list, create 1033
- redistribute
 - BGP 341, 387, 745, 773
 - IS-IS 815
 - OSPF 983
 - RIP 1179
- redistribute (BGP IPv6) 745, 773
- redistribute (BGP) 341
- redistribute (ISIS) 815
- redistribute (MBGP) 387
- redistribute (OSPF IPv6) 1024
- redistribute (OSPF) 983
- redistribute bgp 984
- redistribute bgp (ISIS) 816
- redistribute bgp (OSPF) 984
- redistribute isis
 - OSPF 984
 - RIP 1179
- redistribute isis (BGP) 342
- redistribute isis (OSPF) 984
- redistribute ospf
 - BGP 388
 - IS-IS 817
 - isis 342
 - RIP 1180
- redistribute ospf (BGP IPv6) 746
- redistribute ospf (BGP) 343
- redistribute ospf (ISIS) 817
- redistribute ospf (MBGP) 388
- redundancy auto-failover-limit 517
- redundancy disable-auto-reboot 517, 1329
- redundancy disable-auto-reboot rpm 1329
- redundancy force-failover 518, 1330
- redundancy force-failover rpm 518
- redundancy primary rpm 519
- redundancy protocol lacp 519
- redundancy protocol xstp 519
- redundancy reset-counter 520
- redundancy synchronize 521
- reload 70, 100
- reload command 70
- remark 188, 672
- Remote Network Monitoring (RMON) 1185

- rename 71
- rename command 71
- resequence access-list 197
- resequence access-list (extended IP ACLs) 223
- resequence prefix-list ipv4 198
- resequence prefix-list ipv4 (extended IP ACLs) 224
- reset 100, 101
- reset linecard 1460
- reset sfm 1416, 1460
- reset stack-unit 1330
- resetting S-Series member unit 1330
- restore factory-defaults command 71
- revision (MSTP) 907
- RFC 1858 371
- RFC 3069 1091
- RFC 4360 399
- RFC-2328 971
- RFCs. See IETF RFCs
- RIP 1167
 - version 1 1167
 - version 2 1167
- RMON 1185
- rmon alarm 1186
- rmon collection history 1187
- rmon collection statistics 1187
- rmon event 1188
- rmon hc-alarm 1188
- Route Map
 - match ip address 680
 - match ipv6 next-hop 681
 - match ipv6 route-source 681
 - route-map 682
 - set ipv6 next-hop 682
 - show config 683
- route-map 257
- ROUTE-MAP Mode 24
- router bgp 296, 704
- router bgp (BGP IPv6) 747
- router bgp (BGP) 344
- Router Information Protocol. See RIP.
- router isis 818
- ROUTER ISIS Mode 27
- router ospf 986
- router rip 1180
- ROUTER RIP Mode 26, 27
- router-id 985
- router-id (OSPF IPv6) 1024
- router-id (OSPF) 985
- routing policies, apply 1033
- run-cpu (FTSA command) 494
- running config defined 36

S

- sample-rate (FTSA command) 494
- scramble-atm 1323
- scramble-atm (SONET) 1323
- searching show commands 21
 - display 21
 - except 21
 - find 21
 - grep 21
- secondary VLAN 1091
- secure copy 35
- Secure Copy (SCP) 35
- Security
 - aaa accounting 1208
 - aaa accounting suppress 1209
 - aaa authorization 1211
 - show accounting 1210
- see Neighbor Discovery Protocol 931
- see Storm-Control 1337
- seq 1260
 - IP ACL (extended) 228
 - Redirect list 1037
 - standard IP ACL 198
 - Trace list 1260
- seq (extended IP ACLs) 225, 227, 228
- seq (Extended MAC ACL) 241
- seq (IP prefix ACL) 245
- seq (redirect list) 1037
- seq (standard MAC ACL) 236
- seq arp 225
- seq ether-type 227
- server (FTSA command) 495
- service password-encryption 1222
- service timestamps 102
- service-class dynamic dotIp 1118
- service-class dynamic dotIp (QoS) 1118, 1119
- service-policy input 1139
- service-policy output 1139
- service-queue 1140
- set (policy QoS) 1141
- set as-path prepend (Route Map) 258
- set automatic-tag (Route Map) 258
- set comm-list (Route Map) 259
- set community (Route Map) 260
- set extcommunity rt (BGP) 404
- set extcommunity soo (BGP) 404
- set level (Route Map) 261
- set local-preference (Route Map) 261
- set metric (Route Map) 262
- set metric-type (Route Map) 262
- set next-hop (Route Map) 263
- set origin (Route Map) 264
- set tag (Route Map) 264

- set weight (Route Map) 265
- set-overload-bit 819
- set-overload-bit (ISIS) 819
- sFlow 1274
- sflow collector 1274
- sFlow commands 1273
- sflow enable (globally) 1275
- sflow enable (Interface) 1276
- sflow extended-gateway enable 1276
- sflow extended-router 1277
- sflow extended-switch enable 1278
- sflow polling-interval (Global) 1278
- sflow polling-interval (Interface) 1279
- sflow sample-rate (Global) 1279
- sflow sample-rate (Interface) 1280
- SFM 99
- shortest path first (SPF) 1012
- show acl-vlan-group command 277
- show acl-vlan-group detail command 278
- show alarms 103
- show archive 437
- show arp 631
- show bfd counters 288
- show bfd neighbors 289
- show boot selection 72
- show boot selection command 72
- show bootflash 72
- show bootflash command 72
- show bootvar
 - BOOT_USER mode 73
- show bootvar command 73
- show cam layer2-qos (policy QoS) 1141
- show cam layer3-qos (policy QoS) 1142
- show cam mac linecard 843
- show cam mac stack-unit 847
- show cam maccheck linecard 844
- show cam pbr 1038
- show cam-acl 419
- show cam-ipv4flow command 427
- show cam-l2acl command 430
- show cam-usage command 422
- show capture bgp-pdu neighbor 344
- show capture bgp-pdu neighbor (BGP IPv6) 747
- show chassis 104
- show command-history 105, 1414, 1458
- show config 676, 1261
 - Access list 189
 - BGP 345, 748
 - Interface 566
 - IS-IS 819
 - OSPF 986
 - RIP 1181
 - Spanning Tree 598, 856, 1202, 1349
 - Trace list 1261
 - VRRP 1396
- show config (ACL) 189
- show config (AS-Path) 269
- show config (BGP IPv6) 748
- show config (BGP) 345
- show config (from INTERFACE RANGE mode) 567
- show config (GVRP) 510
- show config (interface configuration) 566
- show config (IP Community List) 272
- show config (IP prefix ACL) 246
- show config (ISIS) 819
- show config (LAG) 598
- show config (MSTP) 908
- show config (OSPF) 986
- show config (port monitor) 1088
- show config (Route Map) 265
- show config (RSTP) 1202
- show config (STP) 1349
- show config (VLAN) 856
- show config (VRRP) 1396
- show config command (ACL VLAN group) 279
- show configuration (FTSA command) 496
- show console lp 1415, 1459
- show controllers (SONET) 1323
- show controllers sonet 1323
- show control-traffic 1430, 1444
- show control-traffic egress 1430
- show control-traffic linecard 1431
- show control-traffic rpm-switch 1431
- show cpu-interface-stats 1430, 1432, 1444, 1474
- show crypto 1250
- show debugging 109, 137
- show debugging (FTSA command) 496
- show default-gateway 73
- show default-gateway command 73
- show diag 1426, 1470
- show diag sfm 1417, 1461
- show dot1x cos-mapping interface 182
- show dot1x interface 183, 1241
- show environment 110, 111
- show frp 472
- show garp timers 510
- show gvrp 511
- show gvrp statistics 512
- show hardware btm 1434, 1476
- show hardware linecard fpc forward 1435, 1477
- show hardware linecard fpc lookup detail 1438, 1479
- show hardware rpm cp 1480
- show hardware rpm mac counters 1440, 1482
- show hardware rpm rp1/rp2 1483
- show hosts 634
- show interface management ethernet 74
- show interface rate 1119
- show interfaces 568, 582

show interfaces configured 574
 show interfaces dampening 575
 show interfaces debounce 576
 show interfaces description 576
 show interfaces gigabitethernet transceiver 584, 1443
 show interfaces linecard 576, 578
 show interfaces management ethernet command 74
 show interfaces port-channel 598
 show interfaces private-vlan command 1095
 show interfaces rate (QoS) 1119
 show interfaces sonet 1325
 show interfaces stack-unit 581
 show interfaces switchport 583
 show interfaces tenGigabitEthernet link-status 1441, 1483
 show ip accounting access-list (common IP ACL) 192
 show ip accounting access-lists 1261
 show ip accounting trace-lists 1261
 show ip as-path-access-lists 269
 show ip bgp 346, 392, 774
 show ip bgp cluster-list 347, 389, 749, 776
 show ip bgp cluster-list (BGP IPv6) 749
 show ip bgp community 348, 354, 389, 751, 776
 show ip bgp community-list 350, 390, 777
 show ip bgp dampened-paths 352, 390, 777
 show ip bgp detail 352, 751
 show ip bgp extcommunity-list 354
 show ip bgp filter-list 354, 391, 779
 show ip bgp flap-statistics 356, 391, 752, 779
 show ip bgp inconsistent-as 357, 392, 780
 show ip bgp ipv4 extcommunity-list 405
 show ip bgp ipv4 multicast 392
 show ip bgp ipv4 multicast (MBGP) 392
 show ip bgp ipv4 multicast cluster-list (MBGP) 389
 show ip bgp ipv4 multicast community (MBGP) 389
 show ip bgp ipv4 multicast community-list (MBGP) 390
 show ip bgp ipv4 multicast dampened-paths (MBGP) 390
 show ip bgp ipv4 multicast filter-list (MBGP) 391
 show ip bgp ipv4 multicast flap-statistics (MBGP) 391
 show ip bgp ipv4 multicast inconsistent-as (MBGP) 392
 show ip bgp ipv4 multicast peer-group (MBGP) 396
 show ip bgp ipv4 multicast summary (MBGP) 397
 show ip bgp ipv6 344, 747
 show ip bgp ipv6 unicast 749, 774
 show ip bgp ipv6 unicast cluster-list 776
 show ip bgp ipv6 unicast community 750, 776
 show ip bgp ipv6 unicast community-list 750, 777
 show ip bgp ipv6 unicast dampened-paths 751, 777
 show ip bgp ipv6 unicast detail 777
 show ip bgp ipv6 unicast extcommunity-list 751
 show ip bgp ipv6 unicast filter-list 752, 779
 show ip bgp ipv6 unicast flap-statistics 752, 779
 show ip bgp ipv6 unicast inconsistent-as 753, 780
 show ip bgp ipv6 unicast neighbors 753, 780
 show ip bgp ipv6 unicast peer-group 756, 783
 show ip bgp ipv6 unicast summary 758, 784
 show ip bgp neighbor 358, 393, 753, 780
 show ip bgp neighbors 358, 393
 show ip bgp next-hop 362, 758
 show ip bgp next-hops 362, 756
 show ip bgp paths 362, 396, 758, 783
 show ip bgp paths as-path 364, 759
 show ip bgp paths community 365, 406, 759
 show ip bgp paths extcommunity 406, 759
 show ip bgp peer-group 366, 396, 756, 783
 show ip bgp regexp 367
 show ip bgp regexp (BGP IPv6) 760
 show ip bgp summary 369, 397, 784
 show ip bgp summary (BGP IPv6) 757
 show ip bgpipv6 unicast community-list 750
 show ip cam 635, 638
 show ip cam linecard 635
 show ip cam stack-unit 638
 show ip community-lists 273
 show ip extcommunity-list 407
 show ip fib linecard 639, 640, 693
 show ip fib stack-unit 640
 show ip flow 641
 show ip flow interface 641
 show ip igmp groups 532
 show ip igmp interface 533
 show ip interface 642
 show ip management-route 644
 show ip mroute 921
 show ip ospf 987
 show ip ospf asbr 988
 show ip ospf database 989
 show ip ospf database asbr-summary 990
 show ip ospf database database-summary 1001
 show ip ospf database external 992
 show ip ospf database network 994
 show ip ospf database nssa-external 995
 show ip ospf database opaque-area 996
 show ip ospf database opaque-as 998
 show ip ospf database opaque-link 998
 show ip ospf database router 999
 show ip ospf database summary 1001
 show ip ospf interface 1003
 show ip ospf neighbor 1005
 show ip ospf routes 1006
 show ip ospf statistics global 1006
 show ip ospf virtual-links 1010
 show ip pim interface 1055, 1058, 1071
 show ip pim neighbor 1056, 1058, 1071
 show ip pim rp mapping 1057, 1072
 show ip pim tib 1059, 1061, 1062, 1073
 show ip prefix-list detail 246
 show ip protocols 645
 show ip redirect-list 1039

show ip rip database 1181
 show ip route 646
 show ip route list 648
 show ip route summary 649
 show ip ssh 1251
 show ip ssh client-pub-keys 1251
 show ip ssh rsa-authentication 1252
 show ip traffic 650
 show ip udp-helper 606
 show ipc-traffic 1430, 1431, 1445, 1446
 show ipc-traffic egress 1445
 show ipc-traffic ingress 1445
 show ipc-traffic linecard 1445
 show ipc-traffic rpm-switch 1446
 show ipv6 accounting access-list 677
 show ipv6 cam stack-unit 692
 show ipv6 fib stack-unit 693
 show ipv6 neighbors 937
 show ipv6 ospf 1030
 show ipv6 ospf neighbor 1031
 show isis database 820
 show isis hostname 822
 show isis interface 823
 show isis neighbors 824
 show isis protocol 825
 show isis traffic 825
 show keys (FTSA command) 497
 show lacp 833
 show linecard 47, 118
 show logging 1309
 show logging driverlog 1447, 1484
 show mac accounting access-list 232
 show mac accounting destination 850
 show mac cam 851
 show mac learning-limit 851
 show mac-address-table 848
 show mac-address-table aging-time 849
 show memory 122, 123
 show monitor session 1088
 show ntp associations 1367
 show ntp status 1369
 show port-channel-flow 600
 show port-channel-flow command 601
 show power detail 1081
 show power inline 1082
 show power supply 1083
 show privilege 1223
 show processes cpu 124, 126
 show processes ipc 1418, 1462
 show processes ipc flow-control 1419, 1463
 show processes memory 132, 135
 show processes switch-utilization 137
 show protocol-termination-table linecard 652
 show protocol-tunnel 1271
 show qos class-map 1144
 show qos policy-map 1145
 show qos policy-map-input 1146
 show qos policy-map-output 1147
 show qos qos-policy-input 1148
 show qos qos-policy-output 1148
 show qos statistics 1149
 show qos wred-profile 1152
 show queue statistics egress (QoS) 1158
 show queue statistics ingress (QoS) 1162
 show range 588
 show redundancy 518, 1330, 1331
 show revision 1421, 1465
 show rmon 1189
 show rmon alarms 1190
 show route-map 266, 683
 show route-map (Route Map) 266
 show rpm 138
 show run diff 438
 show running config acl-vlan-group command 279
 show running-config acl 678
 show running-config extcommunity-list 371, 407, 1182
 show running-config hardware-monitor 1485
 show running-config monitor session 1089
 show running-config track (Object Tracking) 942, 1063
 show sflow 1281
 show sfm 51
 show snmp 1284, 1285, 1286
 show software ifm 140
 show spanning-tree 0 1350
 show spanning-tree 0 (STP) 1350
 show spanning-tree mst configuration 908
 show spanning-tree msti 909
 show spanning-tree pvst 1104
 show spanning-tree rstp (RSTP) 1202
 show system 142
 show system brief (S-Series) 142
 show system stack-ports 1332
 show system stack-unit (S-Series) 142
 show tcp statistics 654
 show tcp statistics 654
 show tdr 603
 show tech-support 33, 40, 41, 45, 46, 63, 64, 65, 67, 68, 69, 70, 71, 72, 73, 74, 160, 1422, 1466
 show tech-support (S-Series) 147
 show track (Object Tracking) 943
 show track ipv6 route (Object Tracking) 951
 show users 1223
 show version 53
 show vlan 857
 show vlan command 857
 show vlan private-vlan command 1096
 show vlan private-vlan mapping command 1098
 show vrrp 1397, 1404

- show-ipc traffic 1444
 - shutdown 589
 - Single Window Protocol (SWP) 1420, 1465
 - Single Window Protocol Queue (SWPQ) 129
 - Site-of-Origin (soo) 400
 - SMTP (Simple Mail Transfer Protocol) server 478, 497
 - smtp server-address 497
 - smtp server-address (FTSA command) 497
 - SNMP
 - number of traps supported 1283
 - versions supported 1283
 - snmp ifmib ifalias long 1287
 - snmp trap link-status 1299
 - snmp-server community 1288
 - snmp-server contact 1289
 - snmp-server enable traps 1290
 - snmp-server host 1293
 - snmp-server location 1295, 1296
 - snmp-server trap-source 1296
 - soo (Site-of-Origin) 400
 - source (port monitoring) 1090
 - Spanning Tree Protocol
 - BPDU guard 1353
 - interface cost 1353
 - portfast 1353
 - spanning-tree 1353
 - spanning-tree (MSTP) 911
 - spanning-tree msti 911
 - spanning-tree mstp edge-port 912
 - spanning-tree pvst 1107
 - spanning-tree rstp (RSTP) 1204
 - speed 590, 591, 1327
 - 100/1000 Base-T Ethernet interfaces 590
 - Management interface 591
 - SPF (Shortest Path First) 965
 - spf-interval 827
 - spf-interval (ISIS) 827
 - S-Series master unit 1330
 - S-Series member unit, resetting 1330
 - S-Series model identifier 1334
 - S-Series stacking 1329
 - S-Series-only commands
 - redundancy disable-auto-reboot rpm 1329
 - reset stack-unit 1330
 - show environment 111
 - show inventory 116
 - show memory 123
 - show processes cpu 126
 - show redundancy 1331
 - show system stack-ports 1332
 - stack-unit priority 1334
 - stack-unit provision 1334
 - stack-unit renumber 1335
 - upgrade system stack-unit 1336
 - SSH
 - ssh-peer-rpm 150
 - ssh 1252
 - stack member identifier 1334
 - stack standby unit 1330
 - Stackable VLAN feature 1371
 - Stackable VLANs (VLAN-Stacking) 1267
 - stacking, S-Series 1329
 - stack-unit priority 1334
 - stack-unit provision 1334
 - stack-unit renumber 1335
 - standby master 1330
 - Start FTSA (Call Home) 477
 - static LAG commands 829
 - static route 631
 - Storm-Control 1337
 - Important Points to Remember 1337
 - STP
 - PVST+ 1101
 - Streamline Upgrade 36
 - strict-priority queue (QoS) 1121
 - subnet masks 194
 - summary-address 1011
 - summary-address (OSPF) 1011
 - suppress threshold (dampening), interface 546
 - switchport 591
 - switchport backup interface 591
 - switchport mode private-vlan command 1099
 - SWP (Single Window Protocol) 1420, 1465
 - SWPQ (Single Window Protocol Queue) 129
- ## T
- TAB key 62
 - tacacs-server host 1232
 - tacacs-server key 1233
 - tagged 859
 - tagged command 859
 - tc-flush-standard 1206
 - tc-flush-standard (MSTP) 913
 - tc-flush-standard (PVST+) 1109
 - TDR
 - Important Points to Remember 602
 - TDR (Time Domain Reflectometer) 602
 - tdr-cable-test 603
 - Telnet
 - number of Telnet sessions supported 94
 - telnet 151
 - terminal length 152, 153
 - terminal monitor 1310
 - test cam-profile (cam-profile template) 414
 - test cam-usage 424, 678
 - test-condition command (comparing FTSA samples) 498
 - test-limit (FTSA command) 502

- test-list (FTSA command) 503
- TFTP server, copy running-config to 36
- threshold 1154
- threshold metric (Object Tracking) 944
- Time Domain Reflectometer (TDR) 602
 - Important Points to Remember 602
- timeout login response 1224
- time-period 439
- timer (FRRP) 473
- timers basic 1183
- timers bgp 371, 760
- timers bgp (BGP IPv6) 760
- timers spf 1012
- timers spf (OSPF) 1012
- TOS 991, 993, 995, 997, 1000, 1002
- traceroute 153
- track 1400, 1406
- track (Object Tracking) 946
- track (VRRP) 1400
- track interface ip route metric threshold 946
- track interface ip route reachability (Object Tracking) 947
- track interface ip routing (Object Tracking) 948
- track interface ipv6 route metric threshold (Object Tracking) 954
- track interface ipv6 route reachability (Object Tracking) 955
- track interface ipv6 routing (Object Tracking) 953
- track interface line-protocol (Object Tracking) 949
- track ip command 860
- track resolution ip route (Object Tracking) 950
- track resolution ipv6 route (Object Tracking) 956
- tracking. *See Object tracking.*
- trap, MAC address station-move 838
- tree information base (tib) 1064
- Troubleshooting 1487, 1489, 1493
- trunk port 1092
- trust diffserv 1154
- trust ipv6-diffserv 698
- Type of Service. *See TOS.*

U

- undebg all 155
- untagged 861
- untagged command 861
- upgrade fpga-image 60
- upgrade sfm-fpga 58
- upgrade system stack-unit 1336
- username 1225

V

- version 1184
- Virtual LANs. *See VLANs.*
- virtual-address 1401

- virtual-address (VRRP) 1401
- VLAN
 - description 853, 967
 - vlan bridge-priority (PVST+) 1109
 - vlan forward-delay (PVST+) 1110
 - vlan hello-time (PVST+) 1110
 - vlan max-age (PVST+) 1111
 - VLAN types (private VLAN) 1091
- VLANs
 - ACL support 558
 - definition 853
 - IP features not supported 853
 - vlan-stack access 1375
 - vlan-stack compatible 1375
 - vlan-stack protocol-type 1377
 - vlan-stack trunk 1378
- VLAN-Stack VLANs
 - Important Points to Remember 1371
- VLAN-Stacking 1371
- VLAN-Stacking (Stackable VLANs) 1267
- VMAN tag 1377

VRF

- cam-profile 1381
- cam-profile ipv4-v6-vrf 1384
- cam-profile ipv4-vrf 1383, 1385
- ip vrf 1386
- ip vrf forwarding 1386
- ip vrf-vlan-block 1387
- show ip vrf 1388
- start-vlan-id 1389
- vrrp bfd neighbor interval 291
- vrrp-group 1401, 1406

W

- wanport command 592
- warm upgrade 518
- Weighted Fair Queuing (WFQ) 1135
- Weighted Random Early Detection (WRED) 1131
- WFQ 1135
- WRED 1131
- wred 1156
- WRED (Weighted Random Early Detection) 1141
- wred-profile 1156
- write 160

X

- XML
 - terminal xml 153

Command Index

A

- aaa accounting 1208
- aaa accounting suppress 1209
- aaa authorization 1211, 1212
- Access list
 - access-class 190, 1217
 - clear counters ip access-group 190
 - ip access-group 191
 - show config 189, 265
 - show ip accounting access-list 192
- Access list (extended)
 - deny 200
 - deny arp 202
 - deny ether-type 203
 - deny tcp 208, 1254
 - deny udp 210
 - ip access-list extended 212
 - permit 213, 1257
 - permit arp 214
 - permit ether-type 216
 - permit tcp 219
 - permit udp 221, 1259
 - seq 228
 - seq arp 225
 - seq ether-type 227
- Access list (standard)
 - deny 194
 - ip access-list standard 195
 - permit 196
 - seq 198
- access-class 190
- access-group 1217
- ACL
 - description 188
- acl-vlan-group 275
- action-list 476
- address family ipv4 multicast (MBGP) 373
- address family ipv6 unicast (BGP IPv6) 762
- adjacency-check 789
- admin-email 477
- advertise dot1-tlv 864
- advertise dot3-tlv 864
- advertise management -tlv 865
- advertise med guest-voice-signaling 872
- advertise med location-identification 873
- advertise med power-via-mdi 874
- advertise med softphone-voice 874
- advertise med streaming-video 875
- advertise med video-conferencing 876
- advertise med video-signaling 876
- advertise med voice 877
- advertise med voice-signaling 878

- aggregate-address (BGP) 296, 703
- Alarms
 - audible cut-off 76
 - clear alarms 80
 - show alarms 103
- area authentication (OSPF IPv6) 1014
- area encryption (OSPF IPv6) 1015
- ARP
 - arp 608
 - arp timeout 610
 - clear arp-cache 610
 - debug arp 613
 - show arp 631
- AS-PATH Access list
 - deny 267
 - ip as-path access-list 267
 - permit 268
 - show config 269
 - show ip as-path-access-list 269

B

- bandwidth-percentage 1123
- banner exec 76
- banner login 77
- banner motd 79
- bfd all-neighbors (OSPF) 283
- bfd enable (Configuration) 282
- bfd enable (Interface) 282
- bfd interval 282
- bfd neighbor 284
- bfd protocol-liveness 285
- BGP
 - aggregate-address 296, 373, 703, 704, 762
 - bgp always-compare-med 298, 705
 - bgp asnotation 298
 - bgp bestpath as-path ignore 299, 705
 - bgp bestpath med confed 299, 706
 - bgp client-to-client reflection 301, 706
 - bgp cluster-id 301, 707
 - bgp confederation identifier 302
 - bgp confederation peers 303, 708
 - bgp dampening 304, 374, 709, 763
 - bgp default local-preference 305, 710
 - bgp fast-external-fallover 306, 711
 - bgp graceful-restart 307, 712
 - bgp log-neighbor-changes 307, 712
 - bgp non-deterministic-med 308, 713
 - bgp router-id 310, 715
 - bgp soft-reconfig-backup 311, 715
 - capture bgp-pdu max-buffer-size 312, 716
 - capture bgp-pdu neighbor (ipv4) 311

capture bgp-pdu neighbor (ipv6) 716
 clear ip bgp dampening 313
 clear ip bgp flap-statistics 314, 376, 764
 clear ip bgp ipv4 multicast soft 376
 clear ip bgp ipv6 dampening 719
 clear ip bgp ipv6 flap-statistics 719
 clear ip bgp ipv6 unicast soft 720
 clear ip bgp peer-group 313, 719
 clear ip bgp soft 312
 debug ip bgp 314, 721
 debug ip bgp dampening 315
 debug ip bgp events 316
 debug ip bgp events (ipv6) 722
 debug ip bgp ipv4 multicast soft-reconfiguration 377
 debug ip bgp ipv6 dampening 722
 debug ip bgp ipv6 unicast soft-reconfiguration 723
 debug ip bgp keepalives 316, 723
 debug ip bgp notifications 317, 724
 debug ip bgp soft-reconfiguration 317
 debug ip bgp updates 318, 378, 724, 765, 766
 default-metric 318, 725
 description 319, 726
 distance bgp 319, 726
 maximum-paths 320, 727
 neighbor activate 321, 727
 neighbor add-path 321
 neighbor advertisement-interval 322, 728
 neighbor allowas-in 323, 729
 neighbor default-originate 323, 729
 neighbor description 324, 730
 neighbor distribute-list 324, 381, 730, 769
 neighbor ebgp-multihop 325, 731
 neighbor filter-list 326, 732
 neighbor graceful-restart 327
 neighbor local-as 327
 neighbor maximum-prefix 328, 733
 neighbor next-hop self 329, 734
 neighbor password 329
 neighbor peer-group
 assigning peers 330, 735
 creating group 331, 736
 neighbor remote-as 333, 737
 neighbor remove-private-as 333, 737
 neighbor route-map 334, 384, 738, 771
 neighbor route-reflector-client 335, 739
 neighbor send-community 335, 739
 neighbor shutdown 336, 740
 neighbor subnet 337
 neighbor timers 337, 742
 neighbor update-source 338, 742
 neighbor weight 339, 743
 network 339, 744, 773
 network backdoor 340, 744
 redistribute 341, 387, 745, 773
 redistribute isis 746
 redistribute ospf 342, 343, 388, 746
 router bgp 344, 747
 show capture bgp-pdu neighbor (ipv4) 344
 show config 345, 748
 show ip bgp 346, 371
 show ip bgp cluster-list 347, 389
 show ip bgp community 348, 389, 776
 show ip bgp community-list 350, 390, 777
 show ip bgp dampened-paths 352, 390, 751, 777
 show ip bgp extcommunity-list 354, 751
 show ip bgp filter-list 391, 779
 show ip bgp flap-statistics 356, 391, 779
 show ip bgp inconsistent-as 357, 392, 753, 780
 show ip bgp ipv4 multicast neighbors 393
 show ip bgp ipv6 747, 749
 show ip bgp ipv6 unicast cluster-list 749
 show ip bgp ipv6 unicast community 750
 show ip bgp ipv6 unicast community-list 750
 show ip bgp ipv6 unicast detail 777
 show ip bgp ipv6 unicast filter-list 752
 show ip bgp ipv6 unicast flap-statistics 752
 show ip bgp ipv6 unicast neighbors 753
 show ip bgp ipv6 unicast summary 757
 show ip bgp neighbor 780
 show ip bgp neighbors 358
 show ip bgp next-hops 362, 758
 show ip bgp paths 362, 758
 show ip bgp paths as-path 364, 759
 show ip bgp paths community 365, 406, 407, 759
 show ip bgp peer-group 366, 396, 756, 783
 show ip bgp regexp 367, 760
 show ip bgp summary 369, 397, 784
 timers bgp 760
 bgp bestpath med missing-as-best 300
 bgp four-octet-as-support 306, 711
 bgp regex-eval-optz-disable 309, 714
 bgp soft-reconfig backup 311
 bgp soft-reconfig-backup 375
 boot change 62
 boot config 30
 boot host 31
 boot messages 63
 boot network 32
 boot selection 64
 boot system 32
 boot system gateway 33
 boot zero 64
 BOOT_USER 61
 boot change 62
 boot messages 63
 boot selection 64
 default-gateway 65
 delete 65

- dir 66
- enable 66
- format 67
- ignore enable-password 67
- ignore startup-config 68
- interface management ethernet ip address 68
- interface management ethernet mac-address 69
- interface management ethernet port 69
- interface management port config 70
- reload 70
- rename 71
- show boot selection 72
- show bootflash 72
- show bootvar 73
- show default-gateway 73
- show interfaces management ethernet 74
- bridge-priority (RSTP) 1198
- bridge-priority (STP) 1345

C

- calendar set 1356
- call-home 477
- cam l2acl 429
- cam-acl 416, 417, 658
- cam-audit linecard 79
- cam-ipv4flow (EtherScale) 426
- cam-l2acl 429
- cam-optimization 417
- cam-profile default microcode 418
- cam-profile eg-default microcode 418
- cam-profile ipv4-320k microcode 418
- cam-profile ipv4-egacl-16k microcode 418
- cam-profile ipv4-v6-vrf 1384
- cam-profile ipv6-etacl microcode 418
- cam-profile l2-ipv4-inacl microcode 418
- cam-profile microcode (Config mode) 418
- cam-profile unified-default microcode 418
- capture bgp-pdu max-buffer-size 312, 716
- capture bgp-pdu neighbor (ipv4) 311
- capture bgp-pdu neighbor (ipv6) 716
- case-number 478
- cd 34
- change bootflash-image 34
- channel-member 594
- class-map 1124
- clear alarms 80
- clear arp-cache 610
- clear bfd counters 285
- clear counters ip access-group 190
- clear counters ipv6 access-group 659
- clear counters mac access-group 231
- clear dampening 543

- clear frp 468
- clear gvrp statistics interface 506
- clear hardware btm 1428, 1471
- clear hardware rpm mac counters 1428, 1472
- clear host (DNS) 611
- clear ip bgp 375, 764
- clear ip bgp * (asterisk) 717
- clear ip bgp as-number 717
- clear ip bgp dampening 313
- clear ip bgp dampening ipv4 multicast (MBGP) 375
- clear ip bgp dampening ipv6 unicast 764
- clear ip bgp flap-statistics 314, 376, 764
- clear ip bgp ipv4 multicast 764
- clear ip bgp ipv4 multicast flap-statistics network (MBGP) 376
- clear ip bgp ipv4 multicast soft 376
- clear ip bgp ipv6 dampening 719
- clear ip bgp ipv6 flap-statistics 719
- clear ip bgp ipv6 unicast (BGP IPv6) 764
- clear ip bgp ipv6 unicast dampening 719
- clear ip bgp ipv6 unicast flap-statistics 719, 764
- clear ip bgp ipv6 unicast soft 720
- clear ip bgp ipv6-address 718
- clear ip bgp peer-group 313, 377, 719, 765
- clear ip bgp peer-group (BGP IPv6) 719
- clear ip bgp soft 312
- clear ip fib linecard 612
- clear ip mroute 915
- clear ip mroute snooping 916
- clear ip ospf statistics 964
- clear ip prefix-list 243
- clear ip route 612
- clear ipv6 fib 685
- clear ipv6 ospf process 1016
- clear ipv6 route 686
- clear lacp counters 829
- clear line 80
- clear lldp counters 865
- clear lldp neighbors 866
- clear logging 1300
- clear mac-address-table dynamic 836
- clear qos statistics 1125
- clear queue statistics ingress (QoS) 1157, 1158
- clear tcp statistics 613
- cli-command 479
- cli-debug 479
- cli-show (FTSA) 480
- clock read-calendar 1356
- clock set 1357
- clock summer-time date 1358
- clock summer-time recurring 1359
- clock timezone 1360
- clock update-calendar 1360
- Community Access list

- deny 270
- ip community-list 271
- permit 271
- show config 272
- show ip community-lists 273
- configure 81
- contact-address 480, 482
- contact-name 481
- contact-notes 481
- continue (Route Map) 250
- copy 35
- copy (Streamline Upgrade) 36
- copy flash 35, 56, 60
- copy ftp
 - 35, 56, 60
- copy rpm0flash
 - 35
- copy rpm0slot0
 - 35
- copy rpm1 35
- copy rpm1flash 35
- copy run start 41
- copy running-config 35
- copy running-config ftp
 - 36
- copy running-config startup-config duplicate 37
- copy running-config tftp
 - 36
- copy scp 35
- copy slot0 35
- copy startup-config 35
- copy tftp 35, 56, 60
- copy usbflash 35
- crypto key generate 1242
- cx4-cable-length 544

D

- dampen 482
- dampening 545
- dataplane-diag disable dfo-reporting 1409, 1452
- dataplane-diag disable loopback 1408, 1450
- dataplane-diag disable sfm-bringdown 1451
- dataplane-diag disable sfm-walk 1451
- Debug
 - debug arp 613
 - debug ftpserver 82
 - debug ip bgp 314
 - debug ip bgp (ipv6) 721
 - debug ip bgp dampening 315
 - debug ip bgp events 316
 - debug ip bgp events (ipv6) 722
 - debug ip bgp ipv4 soft-reconfiguration 377

- debug ip bgp ipv6 dampening 722
- debug ip bgp ipv6 unicast soft-reconfiguration 723
- debug ip bgp keepalives 316, 723
- debug ip bgp notifications 317, 724
- debug ip bgp soft-reconfiguration 317
- debug ip bgp updates 318, 378, 724, 765, 766
- debug ip icmp 615
- debug ip igmp 526
- debug ip msdp 892
- debug ip ospf 964
- debug ip packet 616
- debug ip pim 1045
- debug ip rip 1169
- debug ipv6 pim 1065
- debug isis 791
- debug isis adj-packets 792
- debug isis local-updates 792
- debug isis snp-packets 793
- debug isis spf-triggers 793
- debug isis update-packets 793
- debug multiple spanning-tree 902
- debug ntp 1361
- debug radius 1226
- debug spanning-tree 1346
- debug vrrp 1393, 1404
- show debugging 109
- undebg all 155
- debug bfd 286
- debug callhome 482
- debug cpu-traffic-stats 81
- debug fevd 461
- debug firp 468
- debug gvrp 507
- debug ip bgp ipv4 multicast dampening (MBGP) 377
- debug ip bgp peer-group updates (MBGP) 378
- debug ip bgp updates (MBGP) 378
- debug ip dhcp 614
- debug ip ssh 1243
- debug ip udp-helper 605
- debug ipv6 pim 1065
- debug lldp interface 866
- debug protocol-tunnel 1268
- debug spanning-tree rstp 1198
- default logging buffered 1301
- default logging console 1301
- default logging monitor 1301
- default logging trap 1302
- default-action 483
- default-gateway 65
- default-information originate (OSPF IPv6) 1017
- default-metric (BGP) 318
- default-test 483
- delete 37, 65
- deny 659

- Community Access list 270
- IP ACL (extended) 200
- MAC ACL (extended) 237
- MAC ACL (standard) 233
- Prefix List 243
 - standard IP ACL 194
- deny (AS-Path) 267
- deny (BGP) 400
- deny (Extended IP ACL) 200
- deny arp 202
- deny arp (Extended IP ACL) 202
- deny ether-type (Extended IP ACL) 203
- deny icmp (Extended IP ACL) 205
- deny regex (BGP) 400
- deny tcp 661
- deny tcp (Extended IP ACL) 208
- deny udp 663
- deny udp (Extended IP ACL) 210
- description (ACL VLAN) 276
- description (ACL) 188
- description (BGP) 319, 401, 726
- description (FRRP) 469
- description (FTSA) 484
- description (IS-IS) 795
- description (MSTP) 902
- description (PVST) 1102
- description (RIP) 1171
- description (Route Map) 251
- description (RSTP) 1199
- description (STP) 1347
- description (VLAN) 853, 967
- diag linecard 1425, 1453, 1469
- diag sfm 1410, 1453
- dir 38, 66
- disable 82
- disable (FRRP) 469
- disable (GVRP) 507
- disable (LLDP) 867
- disable (MSTP) 903
- disable (PVST+) 1102
- disable (RSTP) 1199
- disable (STP) 1347
- DNS
 - clear host 611
 - ip domain-list 619
 - ip domain-lookup 619
 - ip domain-name 620
- domain-name 484
- dot1x auth-fail-vlan 176, 1235
- dot1x auth-server 176, 1236
- dot1x guest-vlan 177, 1236
- dot1x max-eap-req 178, 1237
- dot1x port-control 179, 1237
- dot1x quiet-period 180, 1238

- dot1x reauthentication 180, 1238
- dot1x reauth-max 180, 1239
- dot1x server-timeout 181, 1239
- dot1x supplicant-timeout 181, 1240
- dot1x tx-period 182, 1240
- download alt-boot-image 38
- download alt-full-image 39
- duplex (10/100 Interfaces) 548
- duplex (Management) 547

E

- enable 66, 83, 485
- enable xfp-power-updates 84
- enable-all 486
- encrypt 486
- end 84
- epoch 85
- exec-banner 86
- exec-timeout 86
- exit 87

F

- failover group, LAG 595
- fate-sharing group, LAG 595
- FEFD 461
 - debug fefd 461
 - fefd 462
 - fefd disable 463
 - fefd interval 463
 - fefd mode 462
 - fefd reset 464
 - fefd-global 462
 - fefd-global interval 464
 - show fefd 464
- fefd 462
- fefd mode 462
- flow-based enable 1086
- flowcontrol 549
- format 67
- format (C-Series and E-Series) 40
- format flash (S-Series) 40
- forward-delay (MSTP) 903
- forward-delay (RSTP) 1200
- forward-delay (STP) 1347
- frequency 487
- FTP
 - debug ftpserver 82
 - ftp-server enable 87
 - ftp-server topdir 88
 - ftp-server username 88
 - ip ftp password 89

- ip ftp source-interface 90
- ip ftp username 91
- FTSA
 - description 484

G

- garp timers 508
- gvrp enable 509
- gvrp registration 509

H

- hardware monitor mac 1429, 1473
- hardware watchdog 1430, 1473
- hash-algorithm ecmp (C-Series and S-Series) 458
- hello (LLDP) 867
- hello-time (MSTP) 904
- hello-time (RSTP) 1200
- hello-time (STP) 1348
- hostname 89

I

IGMP

- clear ip igmp groups 526
- debug ip igmp 526
- igmp snooping fast-leave 536
- ip igmp immediate-leave 528
- ip igmp last-member-query-interval 528
- ip igmp querier-timeout 529
- ip igmp query-interval 529
- ip igmp query-ma-resp-time 530
- ip igmp static-group 531
- show ip igmp groups 531, 532
- show ip igmp interface 533

IGMP Snooping

- igmp snooping flood 536
- igmp snooping last-member-query-interval 537
- igmp snooping querier 538
- ip igmp snooping enable 535
- ip igmp snooping mroute 537
- show ip igmp snooping mrouter 538

- ignore enable-password 67

Interface

- clear counters 542
- description 546
- disable-on-sfm-failure 547
- dot1p-priority 1114
- interface 551
- interface loopback 552
- interface ManagementEthernet 553

- interface null 553
- interface port-channel 596
- interface sonet 1316
- interface vlan 558
 - ip unreachable 627
 - negotiation auto 563
 - show config 566
 - show interfaces 568, 579, 584, 1442, 1443, 1483
 - show interfaces linecard 578
 - show interfaces switchport 583
 - show ipv6 interfaces ManagementEthernet 694
 - shutdown 589
 - switchport 591
- interface (FRRP) 470
- interface management ethernet ip address 68
- interface management ethernet mac-address 69
- interface management ethernet port 69
- interface management port config 70
- interface range 554
- interface range macro (define) 556
- interface range macro name 557
- interface vlan 558
 - ip access-group 191, 276
 - ip access-list extended (Extended IP ACL) 212
 - ip access-list standard 195
 - ip address 618
 - ip as-path access-list 267
 - ip community-list 271
 - ip control-plane egress-filter-traffic 1410, 1454
 - ip directed-broadcast 618
 - ip extcommunity-list (BGP) 401
 - ip fib download-igp-only 621
 - ip helper-address 621
 - ip helper-address hop-count disable 622
 - ip host 622, 687
 - ip igmp snooping enable 535
 - ip igmp snooping fast-leave 536
 - ip igmp snooping flood 536
 - ip igmp snooping last-member-query-interval 537
 - ip igmp snooping mrouter 537
 - ip igmp snooping querier 538
 - ip local-proxy-arp 1092
 - ip max-frag-count 623
 - ip mroute 916
 - ip multicast-lag-hashing 917
 - ip multicast-limit 918
 - ip multicast-routing 918, 925
 - ip name-server 624, 687
 - ip pim bsr-border 1046
 - ip prefix-list 244
 - ip proxy-arp 625
 - ip radius source-interface 1226
 - ip redirects 625
 - ip route 626

- ip route bfd 287
- ip source-route 627
- ip ssh authentication-retries 1244
- ip ssh connection-rate-limit 1245
- ip ssh hostbased-authentication enable 1245
- ip ssh key-size 1246
- ip ssh password-authentication 1246
- ip ssh pub-key-file 1247
- ip ssh rhostsfile 1247
- ip ssh rsa-authentication (Config) 1248
- ip ssh rsa-authentication (EXEC) 1249
- ip ssh server 1249
- ip udp-broadcast-address 605
- ip udp-helper udp-port 606
- ip vrf 1386
- ip vrf forwarding 1388, 1389
- ip vrf-vlan-block 1387
- ipv6 access-list 666
- ipv6 control-plane egress-filter-traffic 1454
- ipv6 ospf area 1018
- ipv6 ospf authentication 1018
- ipv6 ospf cost 1020
- ipv6 ospf dead-interval 1021
- ipv6 ospf encryption 1019
- ipv6 ospf hello-interval 1022
- ipv6 ospf priority 1022
- IPv6 PIM
 - debug ipv6 pim 1065
 - ipv6 pim dr-priority 1066
 - ipv6 pim query-interval 1067
 - ipv6 pim sparse-mode 1070
 - show ipv6 pim bsr-router 1070
 - show ipv6 pim interface 1071
 - show ipv6 pim neighbor 1071
 - show ipv6 pim rp 1072
 - show ipv6 pim tib 1073
- ipv6 pim dr-priority 1066
- ipv6 pim query-interval 1067
- ipv6 pim sparse-mode 1070
- ipv6 route 688
- ipv6 router isis (ISIS_IPv6) 803
- ipv6 router ospf 1023, 1029
- IS-IS
 - advertise 789
 - area-password 790
 - clear config 790
 - clear isis 791
 - clns host 791
 - debug isis 791
 - debug isis adj-packets 792
 - debug isis local-updates 792
 - debug isis snp-packets 793
 - debug isis spf-triggers 793
 - debug isis update-packets 793
 - default-information originate 794
 - description 795
 - distance 795
 - distribute-list in 796
 - distribute-list out 796
 - domain-password 798
 - hello padding 801
 - hostname dynamic 802
 - ignore-lsp-errors 802
 - ip router isis 802
 - isis circuit-type 803
 - isis csnp-interval 804
 - isis hello-interval 805
 - isis hello-multiplier 805
 - isis metric 807
 - isis network point-to-point 807
 - isis password 807
 - isis priority 808
 - is-type 809
 - log-adjacency-changes 809
 - lsp-gen-interval 809
 - lsp-mtu 810
 - lsp-refresh-interval 811
 - max-area-addresses 812
 - maximum-paths 813
 - max-lsp-lifetime 812
 - metric-style 813
 - multi-topology 814
 - net 814
 - passive-interface 814
 - redistribute 815
 - redistribute ospf 817
 - router isis 818
 - set-overload-bit 819
 - show config 819
 - show isis database 820
 - show isis hostname 822
 - show isis interface 823
 - show isis neighbors 824
 - show isis protocol 825
 - spf-interval 827
- isis bfd all-neighbors 287
- isis hello padding 806

K

- keepalive 558, 1317
- keyadd 487
- keyword (comparison to a value) 500
- keyword message-text 501

L

lACP port-priority 831
 lACP system-priority 832

LAG

audit enable 93
 channel-member 594
 fate-sharing group 595
 interface port-channel 596
 minimum-links 597
 port-channel failover-group 597
 show config 598
 show interfaces port-channel 598
 show port-channel-flow 600

line 94

aux 94
 console 94
 vty 94

linecard 95

link debounce 559

load-balance 629

Logging

clear logging 1300
 default logging buffered 1301
 default logging console 1301
 default logging monitor 1301
 default logging trap 1302
 logging 1302
 logging buffered 1303
 logging console 1303
 logging facility 1304
 logging history 1305
 logging history size 1305
 logging monitor 1306
 logging on 1306
 logging source-interface 1307
 logging synchronous 1308
 logging trap 1308
 no logging on 1306
 show logging 1309

logging 1302

logging buffered 1303

logging console 1303

logging coredump kernel disable 1411, 1455

logging coredump kernel server 1412, 1455

logging coredump linecard 1412, 1456

logging facility 1304

logging history 1305

logging history size 1305

logging kernel-coredump 41

logging kernel-coredump server 42

logging monitor 1306

logging on 1306

logging source-interface 1307

logging synchronous 1308

logging trap 1308

log-messages 488

log-only 489

M**MAC Access list**

clear counters mac access-group 231

mac access-group 231

show mac accounting access-list 192, 232

MAC Access list (extended)

deny 237

mac-access-list extended 239

permit 240

seq 241

MAC Access list (standard)

deny 233

mac-access-list standard 234

permit 235

seq 236

mac access-group 231

mac access-list extended 239

mac access-list standard 234

mac accounting destination 836

mac cam fib-partition 840

mac learning-limit 840

mac learning-limit learn-limit-violation 842

mac learning-limit reset 843

mac learning-limit station-move-violation 842

mac-address-table aging-time 837

mac-address-table static 838

mac-address-table station-move refresh-arp 839

mac-address-table station-move threshold 838, 839

match 490

match as-path (Route Map) 251

match community (Route Map) 252

match extcommunity (BGP) 402

match interface (Route Map) 252

match ip access-group 1125

match ip address (Route Map) 253

match ip dscp 1126

match ip next-hop (Route Map) 254

match ip precedence 1128

match ip route-source (Route Map) 254

match ipv6 address 680

match ipv6 next-hop 681

match ipv6 route-source 681

match mac access-group (policy QoS) 1129

match mac dot1p (policy QoS) 1129

match metric (Route Map) 255

match origin (Route Map) 255

match route-type (Route Map) 256

- match tag (Route Map) 256
- max-age (MSTP) 904
- max-age (RSTP) 1201
- max-age (STP) 1348
- max-hops (MSTP) 905
- MBGP Commands 371, 761
- member (Stackable VLAN) 1373
- member vlan 277
- member-vlan (FRRP) 471
- message-format 490
- minimum-links 597
- mode (FRRP) 471
- mode (LLDP) 868
- monitor 559
- Monitor Session
 - description 1086
- monitor session 1087
- motd-banner 96
- MSDP
 - clear ip msdp peer 891
 - clear ip msdp sa-cache 892
 - debug ip msdp 892
 - ip msdp default-peer 893
 - ip msdp log-adjacency-changes 894
 - ip msdp mesh-group 894
 - ip msdp originator-id 894, 896
 - ip msdp peer 895
 - ip msdp shutdown 898
 - ip multicast-msdp 898
 - show ip msdp 898
- msti (MSTP) 905
- MSTP
 - debug spanning-tree mstp 902
 - disable 903
 - forward-delay 903
 - hello-time 904
 - max-age 904
 - max-hops 905
 - msti 905
 - name 906
 - protocol spanning-tree mstp 906
 - revision 907
 - show config 908
 - show spanning-tree mst configuration 908
 - show spanning-tree msti 909
 - spanning-tree 911
 - spanning-tree msti 911
 - spanning-tree mstp edge-port 912
- mtrace 920
- mtu 562
- Multiple Spanning Tree Protocol
 - see MSTP 901
- multiplier (LLDP) 868

N

- name (MSTP) 906
- name (VLAN) 856
- neighbor 770
 - neighbor activate (BGP IPv6) 767
 - neighbor activate (MBGP) 380
 - neighbor advertisement-interval (BGP IPv6) 768
 - neighbor advertisement-interval (MBGP) 380
 - neighbor default-originate (BGP IPv6) 768
 - neighbor default-originate (MBGP) 381
 - neighbor filter-list aspath (BGP IPv6) 769
 - neighbor filter-list aspath (MBGP) 382
 - neighbor maximum-prefix (BGP IPv6) 770
 - neighbor maximum-prefix (MBGP) 383
 - neighbor next-hop-self (BGP IPv6) 770
 - neighbor next-hop-self (MBGP) 383
 - neighbor peer-group passive (BGP) 332
 - neighbor remove-private-as (BGP IPv6) 771
 - neighbor remove-private-as (MBGP) 384
 - neighbor route-map (BGP IPv6) 771
 - neighbor route-reflector-client (BGP IPv6) 772
 - neighbor route-reflector-client (BGP) 335
 - neighbor soft-reconfiguration inbound 336, 385, 740
- network (BGP IPv6) 773
- network (MBGP) 387
- NTP
 - debug ntp 1361
 - ntp authenticate 1361
 - ntp authentication-key 1362
 - ntp broadcast client 1362
 - ntp disable 1363
 - ntp master 1363
 - ntp multicast client 1364
 - ntp server 1364
 - ntp source 1365
 - ntp trusted-key 1365
 - ntp update-calendar 1366
 - show ntp associations 1367
 - show ntp status 1369

O

- Object Tracking
 - debug track 940
 - delay 940
 - description 941
 - show running-config track 942
 - show track 943
 - show track ipv6 route 951
 - threshold metric 944
 - track 946
 - track interface ip route metric threshold 946

track interface ip route reachability 947
 track interface ip routing 948
 track interface ipv6 route metric threshold 954
 track interface ipv6 route reachability 955
 track interface ipv6 routing 953
 track interface line-protocol 949
 track resolution ip route 950
 track resolution ipv6 route 956
 offline 1425, 1469
 online 1426, 1470
 OSPF
 area default-cost 959
 area nssa 960
 area range 960
 area stub 961
 area virtual-link 961
 auto-cost 963
 clear ip ospf 963
 debug ip ospf 964
 default-information originate 966
 default-metric 967
 distance 968
 distance ospf 968
 distribute-list in 969
 distribute-list out 970
 enable inverse mask 970
 fast-convergence 971
 graceful-restart grace-period 972
 graceful-restart helper-reject 972
 graceful-restart mode 973
 graceful-restart role 973
 ip ospf auth-change-wait-time 974
 ip ospf authentication-key 974
 ip ospf cost 975
 ip ospf dead-interval 975
 ip ospf hello-interval 976
 ip ospf message-digest-key 976
 ip ospf mtu-ignore 977
 ip ospf network 977
 ip ospf priority 978
 ip ospf retransmit-interval 978
 ip ospf transmit-delay 979
 log-adjacency-changes 979
 maximum-paths 980
 mib-binding 980
 network area 981
 passive-interface 981
 redistribute 983
 redistribute isis 984
 router ospf 986
 show config 986
 show ip ospf 987
 show ip ospf database 989
 show ip ospf database asbr-summary 990

show ip ospf database database-summary 1001
 show ip ospf database external 992
 show ip ospf database network 994
 show ip ospf database nssa-external 995
 show ip ospf database opaque-area 996
 show ip ospf database opaque-as 998
 show ip ospf database opaque-link 998
 show ip ospf database router 999
 show ip ospf interface 1003
 show ip ospf neighbor 1005
 show ip ospf virtual-links 1010
 summary-address 1011
 timers spf 1012

P

passive-interface (OSPF IPv6) 1023
 permit 666
 AS-Path Access list 268
 Community Access list 271
 IP ACL (standard) 196
 MAC ACL (extended) 240
 MAC ACL (standard) 235
 Prefix list 245
 standard IP ACL 196
 permit (BGP) 402
 permit (Extended IP ACL) 213
 permit arp (Extended IP ACL) 214
 permit ether-type (Extended IP ACL) 216
 permit icmp (Extended IP ACL) 217
 permit regex (BGP) 403
 permit tcp 668
 permit tcp (Extended IP ACL) 219
 permit udp 670
 permit udp (Extended IP ACL) 221
 PIM-DM
 ip pim dense-mode 1041
 PIM-SM
 clear ip pim rp-mapping 1044
 clear ip pim snooping tib 1044
 clear ip pim tib 1044
 debug ip pim 1045
 ip pim dr-priority 1047, 1049
 ip pim query-interval 1049, 1050
 ip pim rp-address 1050, 1068
 ip pim snooping 1051
 ip pim sparse-mode 1052
 ip pim sparse-mode sg-expiry-timer 1053
 no ip pim snooping dr-flood 1054
 show ip pim bsr-router 1054
 show ip pim interface 1055
 show ip pim neighbor 1056
 show ip pim rp 1057

- show ip pim snooping interface 1058
- show ip pim snooping neighbor 1058
- show ip pim summary 1061
- show ip pim tib 1059, 1062
- show running-config pim 1063
- ping 96
- policy (FTSA) 491
- Policy based Routing
 - ip redirect-group 1034
 - ip redirect-list 1034
 - redirect 1036
 - seq 1037
- policy-action-list 492
- policy-aggregate 1130
- policy-map-input 1131
- policy-map-output 1132
- policy-test-list 492
- Port Channel
 - audit egress port table 93
 - channel-member 594
 - interface port-channel 596
 - minimum-links 597
 - minimum-links command 597
 - show interfaces port-channel 598
- port-channel failover-group 597
- port-channel mode 832
- port-channel-protocol lacp 833
- portmode hybrid 565
- port-shutdown 1316
- power budget 1079
- power inline 1080
- power inline priority 1080
- power-{off | on} sfm 1413, 1457
- power-off 99
- power-on 99
- power-reset cycle 100
- Prefix list
 - clear ip prefix-list 243
 - deny 243
 - ip prefix-list 244
 - permit 245
 - seq 245
 - show config 246
 - show ip prefix-list detail 246
 - show ip prefix-list summary 247
- private-vlan mapping secondary-vlan 1094
- private-vlan mode 1093
- pr-number 493
- protocol frrp (FRRP) 471
- protocol gvrp 510
- protocol lldp (Configuration) 868
- protocol lldp (Interface) 869
- protocol spanning-tree (STP) 1349
- protocol spanning-tree mstp 906

- protocol spanning-tree pvst 1103
- protocol spanning-tree rstp 1201
- protocol-tunnel enable 1269
- protocol-tunnel rate-limit 1270
- protocol-tunnel stp 1268
- PVST
 - description 1102
- pwd 42

Q

- QoS
 - bandwidth-percentage 1123
 - class-map 1124
 - match ip access-group 1125
 - match ip dscp 1127
 - match ip precedence 1128
 - policy-aggregate 1130
 - policy-map-input 1131
 - policy-map-output 1132
 - qos-policy-output 1134
 - rate limit 1115
 - rate shape 1117
 - rate-police 1137
 - rate-shape 1138
 - service-class dynamic dot1p 1118
 - service-policy input 1139
 - service-policy output 1139
 - service-queue 1140
 - show interfaces rate 1119
 - show qos class-map 1144
 - show qos policy-map 1145
 - show qos policy-map-input 1146
 - show qos policy-map-output 1147
 - show qos qos-policy-input 1148
 - show qos qos-policy-output 1148
 - show qos statistics 1149
 - strict-priority queue 1121
 - threshold 1154
 - trust dffserv 1154
 - wred 1156
 - wred-profile 1156
- qos 1134
 - qos-policy-input 1133
 - qos-policy-output 1134
- queue backplane 1134
- queue backplane ignore-backpressure 1134
- queue egress multicast linecard (policy QoS) 1135
- queue ingress multicast (policy QoS) 1136

R

- RADIUS

- debug radius 1226
- ip radius source-interface 1226
- radius-server deadtime 1227
- radius-server host 1227
- radius-server key 1229
- radius-server retransmit 1229
- radius-server timeout 1230
- rate limit (QoS) 1115
- rate police (QoS) 1116
- rate shape (QoS) 1117
- rate-interval 566
- rate-police 1137
- recipient 493
- redistribute (BGP IPv6) 773
- redistribute (BGP) 341
- redistribute (MBGP) 387
- redistribute (OSPF IPv6) 1024
- redistribute bgp 984
- redistribute isis (BGP) 342
- redistribute ospf
 - BGP 343, 747
- redistribute ospf (BGP) 343
- redistribute ospf (MBGP) 388
- Redundancy
 - redundancy primary 519
 - redundancy protocol 519
 - show redundancy 523, 1331
- redundancy auto-failover-limit 517
- redundancy disable-auto-reboot 517, 1329
- redundancy force-failover 518
- redundancy force-failover rpm 518
- redundancy primary rpm 519
- redundancy protocol lacp 519
- redundancy protocol xstp 519
- redundancy reset-counter 520
- redundancy sfm standby 520
- redundancy synchronize 521
- reload 70, 100
- remark 188
- rename 43, 71
- resequence access-list 197
- resequence access-list (Extended IP ACL) 223
- resequence prefix-list ipv4 198
- resequence prefix-list ipv4 (Extended IP ACL) 224
- reset 100
- reset hard 100
- reset linecard 100
- reset rpm 100
- reset sfm 101, 1416, 1460
- reset stack-unit 1330
- restore factory-defaults 71
- revision (MSTP) 907
- RIP
 - auto-summary 1168
 - clear ip rip 1168
 - debug ip rip 1169
 - default-information originate 1169
 - default-metric 1170
 - description 1171
 - distance 1171
 - distribute-list in 1172
 - distribute-list out 1172
 - ip poison-reverse 1173
 - ip rip receive version 1174
 - ip rip send version 1174
 - ip split-horizon 1175
 - maximum-paths 1175
 - neighbor 1176
 - network 1176
 - offset-list 1177
 - output-delay 1177
 - passive-interface 1178
 - redistribute 1179
 - redistribute isis 1179
 - redistribute ospf 1180
 - router rip 1180
 - show config 1181
 - show ip rip database 1181
 - show running-config rip 1182
 - timers basic 1183
 - version 1184
- rmon alarm 1186
- rmon collection history 1187
- rmon collection statistic 1187
- rmon collection statistics 1187
- RMON Commands 1185
- rmon event 1188
- rmon hc-alarm 1188
- Route map
 - match as-path 251
 - match community 252
 - match interface 252
 - match ip address 253
 - match ip next-hop 254
 - match ip route-source 254
 - match metric 255
 - match origin 255
 - match route-type 256
 - match tag 256
 - route-map 257
 - set as-path 258
 - set automatic-tag 258
 - set comm-list delete 259
 - set community 260
 - set level 261
 - set local-preference 261
 - set metric 262
 - set metric-type 262

- set next-hop 263
- set origin 264
- set tag 264
- set weight 265
- show route-map 266
- route-map 682
- route-map (Route Map) 257
- router bgp (BGP) 344
- router-id 985
- router-id (OSPF IPv6) 1024
- RSTP
 - bridge-priority 1198
 - debug spanning-tree rstp 1198
 - disable 1199
 - forward-delay 1200
 - hello-time 1200
 - max-age 1201
 - protocol spanning-tree rstp 1201
 - show config 1202
 - show spanning-tree rstp 1202
 - spanning-tree rstp 1204
- run-cpu 494

S

- sample-rate 494
- SCP
 - ip scp topdir 1244
- scramble-atm (SONET) 1323
- Security
 - aaa authentication login 1216
 - enable password 1218
 - enable restricted 1219
 - login authentication 1220
 - password 1221
 - privilege level 1213
 - service password-encryption 1222
 - show privilege 1223
 - show users 1223
 - timeout login response 1224
 - username 1225
- send 102
- seq 674
 - IP ACL (standard) 198
 - MAC Access list (extended) 241
 - MAC ACL (standard) 236
 - Prefix list 245
- seq (Extended IP ACL) 228
- seq arp (Extended IP ACL) 225
- seq ether-type (Extended IP ACL) 227
- server 495
- service power-off 96
- service timestamps 102

- service-policy-input 1139, 1150, 1151
- service-policy-output 1139
- service-queue 1140
- set (policy QoS) 1141
 - set as-path (Route Map) 258
 - set automatic-tag (Route Map) 258
 - set comm-list delete (Route Map) 259
 - set community (Route Map) 260
 - set extcommunity rt (BGP) 404
 - set extcommunity soo (BGP) 404
 - set ipv6 next-hop 682
 - set level (Route Map) 261
 - set local-preference (Route Map) 261
 - set metric (Route Map) 262
 - set metric-type (Route Map) 262
 - set next-hop (Route Map) 263
 - set origin (Route Map) 264
 - set tag (Route Map) 264
 - set weight (Route Map) 265
- sflow collector 1274
- sflow enable (Global) 1275
- sflow enable (Interface) 1276
- sflow extended-gateway enable 1276
- sflow extended-router 1277
- sflow extended-switch enable 1278
- sflow polling-interval (Global) 1278
- sflow polling-interval (Interface) 1279
- sflow sample-rate (Global) 1279
- sflow sample-rate (Interface) 1280
- show accounting 1210
- show acl-vlan-group 277
- show acl-vlan-group detail 278
- show bfd counters 288
- show bfd neighbors 289, 291
- show boot selection 72
- show bootflash 72
- show bootvar 44, 73
- show calendar 1366
- show cam ipv4flow 427
- show cam layer2-qos (policy QoS) 1141
- show cam layer3-qos (policy QoS) 1142
- show cam mac linecard (count) 843
- show cam mac linecard (dynamic or static) 845
- show cam mac stack-unit 847
- show cam maccheck linecard 844
- show cam-acl 419, 675
- show cam-ipv4flow 1422, 1466
- show cam-l2acl 430
- show cam-profile 412, 420, 1422, 1466
- show cam-usage 422
- show capture bgp-pdu neighbor (ipv4) 344
- show chassis 104, 1422, 1467
- show clock 1367, 1422, 1467
- show command-history 1414, 1458

show config 437, 676, 683
 AS-PATH ACL 269
 Community-list 272
 Prefix list 246
show config (ACL VLAN group) 279
show config (ACL) 189
show config (from INTERFACE RANGE mode) 567
show config (GVRP) 510
show config (LAG) 598
show config (MSTP) 908
show config (port monitor) 1088
show config (Route Map) 265
show config (RSTP) 1202
show config (STP) 856, 1349
show config (VLAN) 856
show configuration 496
show console lp 107, 1415, 1459
show controllers (SONET) 1323
show control-traffic 1430
show control-traffic ingress 1430
show cpu-interface-stats 1431, 1432, 1444, 1445, 1474
show cpu-traffic-stats 108
show crypto 1250
show crypto ipsec policy 1025, 1027
show crypto ipsec sa ipv6 1027
show debugging 496
show default-gateway 73
show diag 1426, 1470
show diag sfm 1417, 1461
show dot1x cos-mapping interface 182
show dot1x interface 183, 1241
show environment 110, 111, 1422, 1467
show fefd 464
show file 45
show file-system 1422, 1467
show file-systems 46
show frpr 472
show garp timers 510
show gvrp 511
show gvrp statistics 512
show hardware btm 1434, 1476
show hardware linecard fpc forward 1435, 1477
show hardware linecard fpc lookup detail 1438, 1479
show hardware rpm cp 1480
show hardware rpm mac counters 1440, 1482
show hardware rpm rp1/rp2 1483
show hosts 634
show interface 1422, 1467
show interfaces 568
show interfaces configured 574
show interfaces dampening 575
show interfaces debounce 576
show interfaces description 576
show interfaces gigabitethernet phy 579, 1442
show interfaces gigabitethernet transceiver 584, 1443
show interfaces link-status 1441
show interfaces management ethernet 74
show interfaces police (QoS) 1121
show interfaces port-channel 598
show interfaces private-vlan 1095
show interfaces rate 1119
show interfaces stack-unit 581
show interfaces status 582
show interfaces tenGigabitEthernet link-status 1483
show inventory 113, 1422, 1467
show inventory (S-Series) 116
show ip accounting access-list 192
show ip as-path-access-lists 269
show ip bgp 346
show ip bgp ipv4 extcommunity-list 405
show ip bgp ipv4 multicast 392, 774
show ip bgp ipv6 unicast dampened-paths 751
show ip bgp ipv6 unicast detail 777
show ip bgp regexp 367
show ip cam linecard 635
show ip cam stack-unit 638
show ip community-lists 273
show ip extcommunity-list 407
show ip fib linecard 639
show ip fib stack-unit 640
show ip flow 641
show ip interface 642
show ip management-route 644, 1422, 1467
show ip mroute 526, 527, 528, 529, 530, 531, 532, 533, 916, 920, 921, 923, 926
show ip ospf asbr 988
show ip prefix-list detail 246
show ip prefix-list summary 247
show ip protocols 645, 1422, 1467
show ip route 646
show ip route list 648
show ip route summary 649, 1422, 1467
show ip ssh client-pub-keys 1251
show ip ssh rsa-authentication 1252
show ip traffic 650
show ip udp-helper 606
show ip vrf 1388
show ipv6 fib linecard 693
show ipv6 interface 694
show ipv6 ospf database 1029
show ipv6 ospf neighbor 1031
show ipv6 pim bsr-router 1070
show ipv6 pim interface 1071
show ipv6 pim neighbor 1071
show ipv6 pim rp 1072
show ipv6 pim tib 1073
show isis traffic 825
show keys 497

show lacp 833
 show linecard 47, 118
 show linecard boot-information 120
 show lldp neighbors 869
 show lldp statistics 870
 show logging 1309
 show logging driverlog 1447, 1484
 show mac accounting access-list 192, 232
 show mac accounting destination 850
 show mac cam 851
 show mac learning-limit 851
 show mac-address-table 848
 show mac-address-table aging-time 849
 show memory 122
 show memory (S-Series) 123
 show monitor session 1088
 show os-version 47
 show port-channel-flow 600
 show power detail 1081
 show power inline 1082
 show power supply 1083
 show processes cpu 124, 1422, 1467
 show processes cpu (S-Series) 126
 show processes ipc 1418, 1462
 show processes ipc flow-control 129, 1419, 1463
 show processes memory 132, 135, 1422, 1467
 show processes switch-utilization 137
 show protocol-tunnel 1271
 show qos class-map 1144
 show qos policy-map 1145
 show qos policy-map-input 698, 1146
 show qos policy-map-output 1147
 show qos qos-policy-input 1148
 show qos qos-policy-output 1148
 show qos statistics 1149
 show qos wred-profile 1152
 show queue statistics egress (QoS) 1158
 show queue statistics ingress (QoS) 1162
 show range 588
 show redundancy 1331, 1422, 1467
 show revision 1421, 1465
 show rmon 1189
 show rmon alarms 1190
 show rmon events 1191
 show rmon hc-alarm 1192
 show rmon history 1193
 show rmon log 1194
 show rmon statistics 1194
 show route-map 683
 show route-map (Route Map) 266
 show rpm 138, 1422, 1467
 show running config acl-vlan-group 279
 show running-conf 1422, 1467
 show running-config 49
 show running-config bgp 371
 show running-config extcommunity-list 407
 show running-config hardware-monitor 1485
 show running-config lldp 870
 show running-config monitor session 1089
 show sflow 1281
 show sflow linecard 1282
 show sfm 51, 1422, 1467
 show snmp 1284
 show snmp engineID 1285
 show snmp group 1285
 show snmp user 1286
 show software ifm 140
 show spanning-tree 0 (STP) 1350
 show spanning-tree mst configuration 908
 show spanning-tree msti 909
 show spanning-tree pvst 1104
 show spanning-tree rstp 1202
 show startup-config 52
 show storm-control broadcast 1338, 1339
 show storm-control unknown-unicast 1339
 show switch links 141
 show system (S-Series) 142
 show system stack-ports 1332
 show tcp statistics 654
 show tdr 603
 show tech-support 33, 40, 41, 45, 46, 63, 64, 65, 67, 68, 69, 70, 71, 72, 73, 74, 144, 160, 1422, 1466
 show tech-support stack-unit 147
 show util-threshold cpu 149
 show util-threshold mem 150
 show version 53, 1422, 1467
 show vlan 857
 show vlan private-vlan 1096
 show vlan private-vlan mapping 1098
 shutdown (port, LAG, VLAN) 589
 smtp 497
 SNMP
 show snmp 1284, 1285
 show snmp user 1286
 snmp trap link-status 1299
 snmp-server community 1288
 snmp-server contact 1289
 snmp-server enable traps 1290
 snmp-server host 1293
 snmp-server location 1295, 1296
 snmp-server trap-source 1296
 snmp ifmib ifalias long 1287
 snmp-server engineID 1291
 snmp-server group 1292
 snmp-server user 1297
 snmp-server view 1299
 SONET
 ais-shut 1312

- alarm-report 1312
 - clock source 1313
 - debug ppp 1313
 - delay triggers 1314
 - down-when-looped 1315
 - encap 1315
 - flag 1315
 - framing 1316
 - hardware monitor 1316
 - interface sonet 1316
 - loopback 1317
 - ppp authentication 1318
 - ppp chap hostname 1319
 - ppp chap password 1319
 - ppp chap rem-hostname 1320
 - ppp chap rem-password 1320
 - ppp next-hop 1321
 - ppp pap hostname 1321
 - ppp pap password 1321
 - ppp pap rem-hostname 1322
 - ppp pap rem-password 1322
 - scramble-atm 1323
 - show controllers 1323
 - show interfaces sonet 1325
 - speed 1328
 - source (port monitoring) 1090
 - Spanning Tree
 - bridge-priority 1345
 - debug spanning-tree 1346
 - description 902, 1199, 1347
 - disable 1102, 1347
 - forward-delay 1347
 - hello-time 1348
 - max-age 1348
 - protocol spanning-tree 1349
 - show config 856, 1349
 - show spanning-tree 0 1350
 - spanning-tree 1353
 - spanning-tree (MSTP) 911
 - spanning-tree (STP) 1353
 - spanning-tree msti 911
 - spanning-tree mstp edge-port 912
 - spanning-tree pvst 1107
 - spanning-tree rstp 1204
 - speed
 - 10/100/1000 Base-T Ethernet Interfaces 590
 - Management interface 591
 - S-Series-only commands
 - redundancy disable-auto-reboot 1329
 - reset stack-unit 1330
 - show redundancy 1331
 - show system stack-ports 1332
 - stack-unit priority 1334
 - stack-unit provision 1334
 - stack-unit renumber 1335
 - upgrade system stack-unit 1336
 - SSH
 - show ip ssh 1251
 - ssh 1252
 - ssh-peer-rpm 150
 - stack-unit priority 1334
 - stack-unit provision 1334
 - stack-unit renumber 1335
 - startup-config 68
 - start-vlan-id 1389
 - storm-control broadcast 1340, 1341, 1342
 - storm-control unknown-unicast 1343, 1344
 - strict-priority queue 1121
 - switchport 591
 - switchport backup interface 591
 - switchport mode private-vlan 1099
- ## T
- TACACS
 - ip tacacs source-interface 1231
 - tc-flush-standard 1109, 1206
 - tc-flush-standard (MSTP) 913
 - tdr-cable-test 603
 - Telnet
 - ip telnet server enable 91
 - ip telnet source-interface 92
 - telnet 151
 - telnet-peer-rpm 152
 - terminal length 152
 - terminal monitor 1310
 - terminal xml 153
 - test cam-usage 424, 678
 - test-condition (comparing FTSA samples) 498
 - test-limit 502
 - test-list (FTSA) 503
 - TFTP
 - ip tftp source-interface 93
 - threshold 1154
 - Time Domain Reflectometer
 - show tdr 603
 - tdr-cable-test 603
 - timer (FRRP) 473
 - Trace list
 - clear counters ip trace-group 1253
 - deny 1254
 - deny udp 1255
 - ip trace-group 1256
 - ip trace-list 1257
 - permit tcp 1258
 - seq 1260
 - show config 1261

- show ip accounting trace-lists 1261
- traceroute 153
- track ip 860
- trust diffserv 1154

U

- undebug all 155
- upgrade 54, 55
- upgrade (S-Series management unit) 57
- upgrade all 55, 56
- upgrade boot 57
- upgrade booted 56
- upgrade bootflash-image 54, 55
- upgrade bootselector-image 54, 55
- upgrade fpga-image 60
- upgrade ftp 57
- upgrade linecard 55, 56
- upgrade rpm 55, 56
- upgrade scp 57
- upgrade sfm-fpga 58
- upgrade system 57
- upgrade system stack-unit (S-Series stack member) 1336
- upgrade system-image 55, 56
- upgrade tftp 57
- upload trace-log 155
- util-threshold cpu (C- and E-Series) 156
- util-threshold cpu (S-Series) 157
- util-threshold mem (C- and E-Series) 158
- util-threshold mem (S-Series) 159

V

- virtual-ip 159
- VLAN
 - default vlan-id 854
 - description 853, 967
 - interface vlan 558
 - show vlan 857
 - tagged 859
 - untagged 861
 - vrrp-group 1401, 1406
- vlan bridge-priority (PVST+) 1109
- vlan forward-delay 1110
- vlan hello-time (PVST+) 1110
- vlan max-age (PVST+) 1111
- vlan-stack access 1375
- vlan-stack compatible 1375
- vlan-stack protocol-type 1377
- vlan-stack trunk 1378
- VRRP
 - advertise-interval 1392
 - authentication-type 1392

- clear vrrp counters 1393, 1403
- debug vrrp 1393, 1404
- description 1394
- disable 1394
- hold-time 1395
- preempt 1395
- priority 1396
- show config 1396
- show vrrp 1397, 1404
- track 1400
- virtual-address 1401

W

- wanport 592
- wred 1140, 1156
- wred-profile 1156
- write 160
- write memory 41

