




SFTOS Command Reference



Force10

Notes, Cautions, and Warnings

-  NOTE: A NOTE indicates important information that helps you make better use of your computer.
-  CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instruction are not followed.
-  WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

© 2010 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.

New Features

SFTOS 2.5.3 adds improved SFTOS internals, but no changed CLI.

SFTOS 2.5.2 adds:

- A substantial Technical Support interface that is not accessible through the standard CLI modes and is not publicly documented
- Support for new S-Series platforms, including the S50N, S50N-DC, S25P, and S25P-DC

Other Changes to the Document

This edition contains only minor edits, with no changes to syntax.

Changes in the previous edition include:

Unsupported Features: The major change was to note features that were at least partially implemented in SFTOS 2.5.2, but not supported by Dell Force10, because they were not sufficiently tested. The Release Notes document for SFTOS 2.5.2.2 contains a list of those features, including DSCP options in QoS commands, DVMRP, GARP, GVRP, IP subnet-based VLANs, MAC-based VLANs, PIM-DM, protocol-based VLANs, VLAN-Stacking, and the Web UI.

The SFTOS Web User Interface (Web UI) chapter is removed from this book, and the Command History fields of commands supporting those unsupported features are updated in this edition with the following statement:

Version 2.5.2 Unsupported: not tested in 2.5.2

The ACL chapter now states that both MAC and IP ACLs can be applied to the same interface. See [Chapter 21, “ACL Commands,” on page 379](#).

The `show classofservice` commands (global and interface) are added to the DHCP Server Commands chapter. See [DHCP Server Commands on page 231](#).

Corrections to existing commands include `show classofservice` (see [igmp enable \(interface\) on page 274](#)) and `show classofservice` (see [classofservice trust on page 329](#)).

Changes to the previous edition of this guide for SFTOS 2.5.2 include:

- The previously separate VLAN section in the System Configuration chapter, and the GARP (including GMRP and GVRP) and VLAN-Stacking chapters are combined into a separate VLAN chapter.
- The `show classofservice ip-dscp-mapping` on page 332 command from an earlier release is added to the book.
- Command options from an earlier release for `show diffserv service` on page 360 added to the book
- Descriptions of `monitor session` on page 95 and `show monitor session` on page 101 modified
- Updated features list in [SFTOS Features on page 13](#).
- **SNTP chapter:** More details added

Multicast SNTP servers is removed as an SNTP option. See [Time Commands on page 243](#).

- **System Configuration chapter:** Added details to `show process cpu` and to `show memory` commands
- **Security chapter:**
 - Deprecated `single-connection` command
 - Revised `show tacacs` command output
 - Noted for `ip ssh server enable` command that offline key generation no longer required.

System Management chapter: The list of outputs of the `show tech-support` command is corrected. See [show tech-support on page 68](#).

ACL chapter:

- The `access-list` command now states that the `mirror` and `redirect` options require that the source, destination, and monitor/redirect ports must be in the same VLAN. See [access-list on page 379](#).
- The sequence of the parameters in the `mac access-group` command are corrected. See [mac access-group on page 387](#).

Table of Contents

New Features	3
Other Changes to the Document	3
1 About This Guide	9
Objectives	9
Audience	10
How to Use this Guide	10
Related Documents and Sources of Additional Information	10
Products and Services Liability	11
Contact Information	11
Documentation Feedback	11
Technical Support	12
The iSupport Website	12
2 SFTOS Overview	13
Switch Management Options	13
SFTOS Features	13
Layer 2 Package Features	14
Layer 3 Package Features	16
3 Quick Start	17
Quick Starting the Switch	17
System Info and System Setup	18
Physical Port Data	18
User Account Management	18
Management IP Address	19
Uploading from the Switch through XMODEM	20
Downloading to the Switch through XMODEM	21
Downloading from a TFTP Server	21
Resetting to Factory Defaults	22
4 Using the Command Line Interface	23
Command Syntax Conventions	23
Command Format	24
Command Parameters	24
“No” Form of a Command	24
Common Command Parameters	25
Addresses	25
Annotations	26

Keyboard Shortcuts	26
Obtaining Help at the Command Line	27
Using Command Modes	28
Mode-based Topology	29
Mode-based Command Hierarchy	31
Flow of CLI Operation	33
5 System Management Commands	35
General System Management and Information Commands	35
Telnet Commands	71
Serial Commands	75
SNMP Management Commands	77
6 System Configuration Commands	87
System Configuration Commands	87
System Utility Commands	105
PoE Commands	114
Dual Image Management Commands	119
Configuration Scripting	122
7 VLAN Commands	125
Virtual LAN (VLAN) Commands	125
Protected-Port (PVLAN) Commands	147
VLAN-Stacking Commands	150
8 Link Layer Discovery Protocol (LLDP) Commands	157
LLDP Overview	157
LLDP Commands	158
9 System Logs	169
10 User Account Commands	179
11 Security Commands	183
Port Security Commands	183
Port-Based Network Access (IEEE 802.1X) Commands	187
RADIUS Commands	199
TACACS+ Commands	205
Secure Shell (SSH) Commands	209
Hypertext Transfer Protocol (HTTP) Commands	212

12 Stacking Commands	217
Stacking	217
Slot and Card Commands	226
13 DHCP Server Commands	231
14 Time Commands	243
System Clock Commands	243
SNTP Commands	244
15 GARP Commands	251
GARP Commands	251
GARP VLAN Registration Protocol (GVRP) Commands	254
GARP Multicast Registration Protocol (GMRP) Commands	257
16 RMON Commands	261
17 IGMP Snooping Commands	273
18 LAG/Port Channel Commands	287
19 Spanning Tree (STP) Commands	309
20 Quality of Service (QoS) Commands	327
Class of Service (CoS) Commands	327
Differentiated Services (DiffServ) Commands	335
Class Commands	337
Policy Commands	346
Service Commands	357
Show Commands	358
Buffer Carving	367
21 ACL Commands	379
IP Access Control List (IP ACL) Commands	379
MAC Access Control List (ACL) Commands	384
Broadcast Storm Control Commands	389
22 Routing Commands	391
Address Resolution Protocol (ARP) Commands	391
IP Routing	397

Bootp/DHCP Relay Commands	407
Router Discovery Protocol Commands	410
Virtual LAN Routing Commands	413
Virtual Router Redundancy Protocol (VRRP) Commands	414
23 OSPF Commands	423
24 RIP Commands	449
25 IP Multicast Commands	457
Basic IP Multicast Commands	457
Distance Vector Multicast Routing Protocol (DVMRP)	465
IGMP Commands	471
26 PIM Commands	485
PIM-DM Commands	485
PIM-SM Commands	488
Index	499

About This Guide

This guide describes configuration commands for SFTOS software. The commands can be accessed from the SFTOS Command Line Interface (CLI), accessed through the console port or through a Telnet connection, and from the Node Manager component of Dell Force10 Management System (FTMS).

This chapter covers the following topics:

- Objectives
- Audience on page 10
- How to Use this Guide on page 10
- Related Documents and Sources of Additional Information on page 10
- Products and Services Liability on page 11
- Contact Information on page 11
- Documentation Feedback on page 11
- Technical Support on page 12



Note: Please note that BGP and bandwidth allocation are not supported in this release, but may appear in the command output examples in this document.

Objectives

This document is intended as a reference guide for users of the SFTOS 2.5.2 command line interface (CLI) used for the following S-Series switches:

- S50
- S50V
- S50N, S50N-DC
- S25P, S25P-DC



Note: For S2410 documentation, see the S2410 Documentation CD-ROM.

The CLI command statements list syntax information for constructing command input at the SFTOS command line interface (CLI). Also, in some cases, “screenshot” examples are provided.

Commands that generate reports are called “show commands”, because they all begin with the keyword “nieA”. The syntax statements for those commands in this guide contain a description of the fields in their reports, and, in some cases, with examples.

This document includes information on the protocols and features found in SFTOS. Background on networking protocols is included primarily to describe the capabilities of SFTOS. For more complete information on protocols, refer to other documentation and IETF RFCs.

Audience

This guide assumes you are knowledgeable in Layer 2 and Layer 3 networking technologies, that you have an understanding of the SFTOS software base and have read the appropriate specification for the relevant switch platform.

This document is primarily for system administrators configuring and operating a system using SFTOS software. It is intended to provide an understanding of the configuration options of SFTOS software.

In addition, software engineers who will be integrating SFTOS software into their router or switch product can benefit from a description of the configuration options.

How to Use this Guide

This guide is structured so that you can look up not only command syntax, but also how commands are related. Related commands are generally grouped together, and, in addition, some command statements contain links to descriptions of related commands.

While you can infer a lot about the use of a command from its syntax statement, you are better served to see if the *SFTOS Configuration Guide* uses the command, because you can learn more about the context of its use.

Regarding RFCs and MIBs (management information base files) supported in S-Series systems, syntax statements in this guide and related instructions in the *SFTOS Configuration Guide* cite the relevant RFCs. Also, an appendix in that guide contains a list of the RFCs and MIBs.

This guide is structured in this sequence:

- [New Features on page 3](#) is a quick way to access new and changed commands.
- [Chapter 2, SFTOS Overview](#) briefly introduce the S-Series hardware and SFTOS software.
- [Chapter 3, Quick Start](#) is an introduction to how to start and configure the S-Series using SFTOS software.
- Information on how this guide presents the CLI modes, syntax, conventions, and terminology is in [Chapter 4, “Using the Command Line Interface,” on page 23](#).
- The CLI command syntax statements begin in [Chapter 5, System Management Commands](#). Chapters 6 through 11 describe commands that manage the system, while the later chapters describe commands specific to particular networking protocols. Beginning with Release 2.3, the CLI syntax statements that are new or changed include a Command History table.

Related Documents and Sources of Additional Information

The following documents provide information on using Dell Force10 S-Series switches and SFTOS software. All of the documents are available on the Documents tab of iSupport (the Dell Force10 support website): <http://www.force10networks.com/support>:

- *SFTOS Command Reference*
- *SFTOS Configuration Guide*
- *SFTOS and S-Series Release Notes*

- *Quick Reference* (also included as a printed booklet with the system)
- Hardware installation guides
- MIBs files
- *S-Series Tech Tips and FAQ*

Except for the Tech Tips and FAQ documents, all of the documents listed above are also on the S-Series CD-ROM. Training slides are also on the S-Series CD-ROM.

Currently, access to user documentation on iSupport is available without a customer account. However, in the future, if you need to request an account for access, you can do so through that website.

Products and Services Liability

References in this publication to Dell Force10 products, programs, or services do not imply that Dell Force10 intends to make these available in all countries in which Dell Force10 operates. Any reference to a Dell Force10 product, program, or service is not intended to state or imply that only Dell Force10's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any of Dell Force10's intellectual property rights may be used instead of the Dell Force10 product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by Dell Force10, are the user's responsibility.

Contact Information

For technical support, see [Technical Support on page 12](#). For other questions, contact Dell Force10 using the following address:

Dell Force10
350 Holger Way
San Jose, CA 95134
USA

Documentation Feedback

techpubs@Force10Networks.com

If appropriate, please include the following information with your comments:

- Document name
- Document part number (from the front cover)
- Page number
- Software release version (from the front cover)

Technical Support

The iSupport Website

Dell Force10 iSupport provides a range of support programs to assist you with effectively using Dell Force10 equipment and mitigating the impact of network outages. Through iSupport you can obtain technical information regarding Dell Force10 products, access to software upgrades and patches, and open and manage your Technical Assistance Center (TAC) cases. Dell Force10 iSupport provides integrated, secure access to these services.

Accessing iSupport Services

The URL for iSupport is www.force10networks.com/support/. To access iSupport services you must have a userid and password. If you do not have one, you can request one at the website:

- 1 On the Dell Force10 iSupport page, click the **Account Request** link.
- 2 Fill out the User Account Request form and click **Send**. You will receive your userid and password by email.
- 3 To access iSupport services, click the **Log in** link, and enter your userid and password.

Contacting the Technical Assistance Center

How to Contact Dell Force10 TAC	Log in to iSupport at www.force10networks.com/support/ , and select the Service Request tab.
Information to Submit When Opening a Support Case	<ul style="list-style-type: none"> • Your name, company name, phone number, and email address • Preferred method of contact • Model number • Software version number • Symptom description • Screen shots illustrating the symptom, including any error messages
Managing Your Case	Log in to iSupport, and select the Service Request tab to view all open cases and RMAs.
Downloading Software Updates	Log in to iSupport, and select the Software Center tab.
Technical Documentation	Log in to iSupport, and select the Documents tab. This page can be accessed without logging in via the Documentation link on the iSupport page.
Contact Information	<p>E-mail: support@force10networks.com</p> <p>Web: www.force10networks.com/support/</p> <p>Telephone:</p> <p>US and Canada: 866.965.5800</p> <p>International: 408.965.5800</p>


SFTOS Overview

The SFTOS software loaded in every S-Series switch has two purposes:

- Assist attached hardware in switching frames, based on Layer 2, 3, or 4 information contained in the frames.
- Provide a complete device management portfolio to the network administrator.

Switch Management Options

SFTOS provides the network administrator with a choice of management methods:

- **VT100 interface:** You can access the SFTOS command line interface (CLI) through either the console port on the switch or through the management IP address. This book focuses on CLI syntax.
-  **Note:** When configuring a device by use of a configuration file, the maximum number of configuration file command lines is 2000.
- **Simple Network Management Protocol (SNMP):** Dell Force10 provides Force10 Management System (FTMS), a graphical network management software product that provides a global view of your complete Dell Force10 network. FTMS includes Node Manager, which not only provides GUI-based device management, it also includes the ability to execute CLI commands, either individually from Node Manager or by having Node Manager open a Telnet window to the device.

SFTOS Features

The SFTOS software is available in two packages—the “Layer 2 Package” (“Switching”) and the “Layer 3 Package” (“Routing”). The Layer 2 Package is the standard core software package shipped on all S-Series switches. The Layer 3 Package includes both the core software and software that supports Layer 3 of the OSI 7-Layer model.

Layer 2 Package Features

The core SFTOS software provides the following features.

Basic Routing and Switching Support

- 10 GigE (IEEE 802.3ae)
- 1000 Base-T (IEEE 802.3ab)
- 16k MAC Address Table
- BootP (RFC951, 1542)
- BootP/DHCP Relay and Server (RFC 2131)
- IEEE 802.3ad
- IEEE 802.1ab – Link-level discovery
- Flow Control (IEEE 802.3x)
- Host Requirements (RFC 1122)
- IP (RFC 791)
- ICMP (RFC 792)
- Jumbo Frame Support
- MSTP (IEEE 802.1s)
- Rapid Spanning Tree (IEEE 802.1w)
- STP (Spanning Tree Protocol) (IEEE 802.1D)
- TCP (RFC 793)
- UDP (RFC 768)

QoS

- 802.1p Priority Marking
- ACL Entries (L2 + L3)
- Bandwidth-based Rate Limiting
- Layer 2 Classification
- Layer 3 DSCP
- Priority Queues
- VTY ACLs
- Wirespeed ACLs (L2/L3/L4)

VLAN

- Frame Extensions (IEEE 802.3ac)
- GVRP, GARP, GMRP
- IEEE 802.1q Support
- IP Subnet-based VLANs
- MAC-based VLANs
- Port-based VLANs
- Private VLAN– Edge
- Protocol-based VLANs
- Supported Number of VLANs

Multicast Protocols

- IGMP Snooping
- Layer 2 Multicast Forwarding

Security and Packet Control Features

- Access Profiles on Routing Protocols
- DOS Protection
- IEEE 802.1x
- Ingress Rate Limiting
- Login Access Control
- MAC-based Port Security
- Port Mirroring
- RADIUS
- SSH2 Server Support

Management

- Dual Image Support
- External Redundant Power System
- HTML-based Management
- HTTPS/SSL
- RMON Groups
- SNMP v1/v2c
- SNMP
- SSHv2
- Syslog, with Specification of Facility
- Telnet (RFC 854)
- TFTP (RFC 783)

Stacking

- Auto Configuration
- Auto Master Election
- Hot Insertion and Removal of Units in a Stack
- LAG across Units in a Stack
- Stacking Multiple Units

Layer 3 Package Features

The Layer 3 Package (“Routing”) of SFTOS includes all of the features listed above, along with the following features:

Extended Routing and Switching Support

- 4k IPv4 Routing Table Entry
- ARP (RFC 826)
- CIDR (RFC 1519)
- IGMP Proxy
- IPv4 (RFC 1812)
- IPv4 Router Discovery (RFC 1256)
- OSPF (RFC 2328, 1587, 1765, 2370)
- Proxy ARP (RFC 1027)
- RIPv1/v2
- Routing Protocol Support
- Static Routes
- VRRP (RFC 2338)

Multicast Protocols

- DVMRP
- IGMP v1/v2 (RFC 1112, 2236)
- IGMP v3 (RFC 3376)
- PIM-SM-edge
- PIM-DM

Management

- ECMP

Quick Start

This chapter summarizes the procedures to start and operate S-Series switches. For more detail, see the Getting Started chapter in the *SFTOS Configuration Guide* (and the rest of that guide) or the *Quick Reference* for your switch model.

This chapter covers the following topics:

- [Quick Starting the Switch on page 17](#)
- [System Info and System Setup on page 18](#)
- [Physical Port Data on page 18](#)
- [User Account Management on page 18](#)
- [Management IP Address on page 19](#)
- [Uploading from the Switch through XMODEM on page 20](#)
- [Downloading to the Switch through XMODEM on page 21](#)
- [Downloading from a TFTP Server on page 21](#)
- [Resetting to Factory Defaults on page 22](#)

Quick Starting the Switch

You can access the SFTOS software in the switch locally or from a remote workstation. For remote access, the switch must be configured with an IP address, subnet mask, and default gateway:

1. Turn the Power ON.
2. From a console connection, allow the switch to load the software until the login prompt appears. The device initial state is called the default mode.
3. When the prompt asks for operator login, execute the following steps:
 - 1 Type the word `admin` in the login area. Do not enter a password because there is no password in the default mode.
 - 2 Press ENTER two times. The prompt of the User Exec mode of the CLI is displayed.
 - 3 Enter `enable` to switch to the Privileged Exec mode. You can run all “show” commands from this mode, while some “show” commands do not run from User Exec mode.
 - 4 Enter `configure` to access the Global Config mode to enter configuration commands.
 - 5 Enter `exit` if you need to return to any previous mode.

System Info and System Setup

To get information on the software version, use the **show hardware** command:

Command Syntax	Command Mode	Purpose
show hardware	Privileged Exec	Displays the serial number, software version the device contains, burned-in MAC address, and other device information. Information is listed for all units in the stack.

Physical Port Data

To get information on the physical port, use the **show port all** command:

Command Syntax	Command Mode	Purpose
show port all	Privileged Exec	<p>Displays the ports in <i>unit/slot/port</i> format and the following data for each port:</p> <ul style="list-style-type: none"> Type - Indicates if the port is a special type of port Admin Mode - Selects the Port Control Administration State Physical Mode - Selects the desired port speed and duplex mode Physical Status - Indicates the port speed and duplex mode Link Status - Indicates whether the link is up or down Link Trap - Determines whether or not to send a trap when link status changes LACP Mode - Displays whether LACP is enabled or disabled on this port.

User Account Management

To configure account management, use the following commands:

Command Syntax	Command Mode	Purpose
show users	Privileged Exec	<p>Displays all of the users that are allowed to access the switch</p> <p>Access Mode - Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only).</p> <p>As a factory default, the 'admin' user has Read/Write access. There can only be one Read/Write user and up to five Read Only users.</p>
show login session	Privileged Exec	Displays all of the login session information

Command Syntax	Command Mode	Purpose
[no] username <i>user</i> passwd <i>password</i>	Global Config	<p>This command adds a new user (account) if space permits, along with the user's password. The user name and password can each be up to eight alphanumeric characters in length.</p> <p>To remove a user, use the no username <i>user</i> command.</p> <p>To delete or change a password, remove and reenter the user with the new password.</p> <p>Passwords can include special characters. As of SFTOS 2.5.1.3, the following characters are supported: , . { } . (period, comma, open bracket, close bracket, bar)</p>
copy system:running-config nvram:startup-config	Privileged Exec	<p>This will save passwords and all other changes to the device.</p> <p>If you do not save the configuration by doing this command, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset.</p> <p>In a stacking environment, the running configuration is saved in all units of the stack.</p>
logout	User Exec and Privileged Exec	Logs the user out of the switch.

Management IP Address

To view and manage network parameters, you set up the management IP address (see below) so that you can use the following management methods:

- Simple Network Management Protocol (SNMP)
- SSH
- Telnet



Note: Helpful Hint: After configuring the network parameters, enter **write** (same effect as executing the **copy system:running-config nvram:startup-config** command), in Privileged Exec mode, so that the management configuration changes are not lost.

To configure the management IP address, use the following commands:

Command Syntax	Command Mode	Purpose
show interface managementethernet	Privileged Exec	Displays the Network Configurations IP Address: IP Address of the interface. Default IP is 0.0.0.0 Subnet Mask: IP Subnet Mask for the interface. Default is 0.0.0.0 Default Gateway: The default Gateway for this interface. Default value is 0.0.0.0 Burned in MAC Address: The Burned in MAC Address used for in-band connectivity Locally Administered MAC Address: Can be configured to allow a locally administered MAC address MAC Address Type: Specifies which MAC address should be used for in-band connectivity Network Configurations Protocol Current: Indicates which network protocol is being used. Default is none. Management VLAN Id - Specifies VLAN id Web Mode: Indicates whether HTTP/Web is enabled. Java Mode: Indicates whether Java mode is enabled.
interface managementethernet	Global Config	Invokes the (Config-if-ma)# prompt, at which you can execute the ip address command.
ip address <i>ipaddr</i> <i>netmask</i>	Interface Config	Configure the management IP address and subnet mask: IP Address range from 0.0.0.0 to 255.255.255.255 Subnet Mask range from 0.0.0.0 to 255.255.255.255
management route default <i>gateway</i>	Global Config	Set the default gateway. Gateway Address range from 0.0.0.0 to 255.255.255.255

For details on command syntax for the commands listed above, see [General System Management and Information Commands on page 35](#).

Uploading from the Switch through XMODEM

To copy to a PC from the switch console port with XMODEM, use the following commands.

Command Syntax	Command Mode	Purpose
copy {nvram:startup-config nvram:errorlog nvram:log nvram:traplog} xmodem:// <i>filepath/</i> <i>filename</i> See copy on page 106 and the Getting Started chapter of the <i>SFTOS Configuration</i> <i>Guide</i> .	Privileged Exec	The file types are: startup-config — configuration file errorlog — Event log log — System log traplog — trap log This starts the upload and also displays the mode of uploading and the type of upload it is and confirms the upload is taking place. If you are using HyperTerminal, specify which file is to be sent to the switch.



Note: Keywords and parameters that are shown within braces in syntax statements must be entered in the CLI. Keywords and parameters that are shown separated by a bar in syntax statements indicate that you choose only one. For details, see [Command Syntax Conventions on page 23](#).

Downloading to the Switch through XMODEM

To download through the switch console port from a PC, use the following command:

Command Syntax	Command Mode	Purpose
<pre>copy xmodem://filepath/ filename {nvram:startup-config image1 image2} See copy on page 106.</pre>	Privileged Exec	<p>Sets the destination (download) data type to be an image (image1 or image2) or a configuration file (nvram:startup-config).</p> <p>If you are using HyperTerminal, specify which file is to be sent to the switch.</p> <p>The switch will restart automatically after the code has been downloaded.</p> <p>Note: The software download option was expressed before SFTOS 2.5.1 as <code>copy xmodem://filepath/filename system:image</code>.</p>

Downloading from a TFTP Server

Before starting a TFTP server download, complete the Quick Start-up for the IP Address.

To download from a TFTP server, use the following command:

Command Syntax	Command Mode	Purpose
<pre>copy tftp://ipaddress/filepath {nvram:startup-config image1 image2} See copy on page 106.</pre> <p>The software download option was expressed before SFTOS 2.5.1 as <code>system:image</code>.</p>	Privileged Exec	<p>Sets the destination (download) datatype to be a software image (image1 or image2) or a configuration file (nvram:startup-config).</p> <p>The URL must be specified as: <code>tftp://ipaddress/filepath</code> (where <i>filepath</i> includes the filename, such as <code>s50/s50software.bin</code>)</p> <p>The <code>nvram:startup-config</code> option downloads the configuration file.</p> <p>The <code>copy tftp://ipaddress/filepath image1</code> option downloads the code to the image1 storage location in the switch.</p>

Resetting to Factory Defaults

To help configure factory defaults, use one of the following commands:

Command Syntax	Command Mode	Purpose
clear config	Privileged Exec	Enter yes when the prompt pops up to clear all the configurations made to the switch. This option replaces the current running-config with the most recent startup configuration file. However, if the startup configuration file has been modified from the factory default settings, this command does not restore the system to factory defaults.
reload (or cold boot of the switch)	Privileged Exec	Enter yes when the prompt pops up that asks if you want to reset the system. Choose to reset the switch or cold boot the switch—both work effectively. See reload on page 111 , and see the Getting Started chapter of the <i>SFTOS Configuration Guide</i> .

Using the Command Line Interface

The command line interface (CLI) for SFTOS is the primary way to manage S-Series switches, and is the focus of this book.

This chapter covers the following topics:

- [Command Syntax Conventions on page 23](#)
- [Keyboard Shortcuts on page 26](#)
- [Obtaining Help at the Command Line on page 27](#)
- [Using Command Modes on page 28](#)
- [Mode-based Topology on page 29](#)
- [Mode-based Command Hierarchy on page 31](#)
- [Flow of CLI Operation on page 33](#)

Command Syntax Conventions

This guide uses the following conventions to describe command syntax:

Convention	Description
REIAEs.	Keywords are in bold and must be entered in the CLI as listed.
<i>parameter</i>	Parameters (variables) are in italics and require a number or word to be entered in the CLI. The CLI online help shows parameters in brackets: <i><parameter></i>
{X}	Keywords and parameters that are shown within braces in syntax statements must be entered in the CLI.
[X]	Keywords and parameters that are shown within brackets in syntax statements are optional.
x y	Keywords and parameters that are shown separated by a bar in syntax statements require you to choose one.

The following conventions apply to the command name:

- The command name is displayed in bold font. It must be entered exactly as shown.
- When you have entered enough letters of a command name to uniquely identify the command, you can press the **space bar** or **Tab** key to cause the system to complete the word. For more keyboard shortcuts (speedkeys), see [Keyboard Shortcuts on page 26](#).

Command Format

Some commands, such as `clear vlan`, do not require parameters. Other commands have parameters for which you must supply a value. Parameters are positional — you must enter the values in the correct order. Optional parameters follow required parameters. For example:

`snmp-server location loc`

- `snmp-server location` is the command name.
- `loc` is a parameter—a placeholder for a required value.

`ip address ipaddr subnetmask`

- `ip address` is the command name.
- `ipaddr` and `subnetmask` are two required parameters —placeholders for two required values.

`mtrace sourceipaddr [destination] [group]`

- `mtrace` is the command name.
- `sourceipaddr` is a required parameter
- The parameters `destination` and `group` are in brackets to indicate that they are optional parameters, and being in separate brackets indicates that they are not mutually exclusive.

`mac-type {local | burnedin}`

- `mac-type` is the command name.
- The keywords `local` and `burnedin` are in curly braces and separated by a vertical bar to indicate that you must one. If, instead of curly braces, brackets were used, a keyword would be optional.

Command Parameters

- Parameters are order-dependent.
- Parameters are displayed in this document in italic font, which must be replaced with a name or number.
- To use spaces as part of a name parameter, enclose it in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces.
- Parameters may be mandatory values, optional values, choices, or a combination.

Words in italics (also sometimes shown in brackets: `<parameter>`) indicate that a mandatory parameter must be entered in place of the brackets and text inside them.

[parameter]—square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.

choice1 | choice2—pipe indicates that only one of the parameters should be entered.

{parameter}—curly braces indicate that a parameter must be chosen from the list of choices.

“No” Form of a Command

“No” is a specific form of an existing command and does not represent a new or distinct command. Only the configuration commands are available in the “no” form. The behavior and the support details of the “no” form is captured as part of the mapping sheets.

Almost every configuration command has a “no” form. In general, use the “no” form to reverse the action of a command or reset a value to the default. For example, the `no shutdown` command reverses the shutdown of an interface. Use the command without the keyword `no` to re-enable a disabled feature or to enable a feature that is disabled by default.

Common Command Parameters

`ipaddr`—This parameter is a valid IP address. Presently, the IP address can be entered in these formats:

- a (32 bits)
- a.b (8.24 bits)
- a.b.c (8.8.16 bits)
- a.b.c.d (8.8.8.8)

In addition to these formats, decimal, hexadecimal, and octal formats are supported through the following input formats (where n is any valid hexadecimal, octal, or decimal number):

- 0xn (CLI assumes hexadecimal format)
- 0n (CLI assumes octal format with leading zeros)
- n (CLI assumes decimal format)

`macaddr`—The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

`areaid`—Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network number of the sub-netted network may be used for the area ID.

`routerid`—The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

`unit/slot/port`—Valid slot and port number separated by forward slashes. For example, `0/1` represents slot number 0 and port number 1.

`logical unit/slot/port`—Logical unit, slot and port number. This is applicable in the case of a port-channel (LAG). The operator can use the *logical unit/slot/port* to configure the port-channel.

`character strings`—Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

Addresses

Network addresses are used to define a link to a remote host, workstation or network. Network addresses are shown using the following syntax:

Table 4-1. Network Address Syntax

Address Type	Format	Range
<code>ipaddr</code>	192.165.11.110	0.0.0.0 to 255.255.255.255 (decimal)
<code>macaddr</code>	A7:C9:89:DD:A9:B3	hexadecimal digit pairs

Double quotation marks such as “System Name with Spaces” set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings are not valid user-defined strings.

Command completion finishes spelling the command when enough letters of a command are entered to uniquely identify the command word. The command may be executed by pressing **ENTER** (command abbreviation) or the command word may be completed by pressing the Tab key or Spacebar (command completion).

The value 'Err' designates that the requested value was not internally accessible. This should never happen and indicates that there is a case in the software that is not handled correctly.

The value of '-----' designates that the value is unknown.

Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character ‘!’ is recognized as a comment line and ignored by the parser.

Some examples are shown here:

! Script file for displaying the ip interface

! Display information about interfaces

show ip interface 0/1 !Displays the information about the first interface

! Display information about the next interface

show ip interface 0/2

```
! End of the script file! Script file for displaying the ip interface
! Display information about interfaces
show ip interface 1/0/1 !Displays the information about the first interface
! Display information about the next interface
show ip interface 1/0/2
! End of the script file
```

Keyboard Shortcuts

The following key combinations (speedkeys, special characters) speed up use of the CLI:

Backspace—delete previous character

Ctrl-A—go to beginning of line

Ctrl-B—go backward one character

Ctrl-D—delete current character

Ctrl-E—go to end of line
Ctrl-F—go forward one character
Ctrl-H—display command history or retrieve a command
Ctrl-I—complete a keyword
Ctrl-K—delete to end of line
Ctrl-N—go to next line in history buffer
Ctrl-P—go to previous line in history buffer
Ctrl-T—transpose previous character
Ctrl-U, X—delete to beginning of line
Ctrl-W—delete previous word
Ctrl-Z—return to root command prompt
Delete key—delete next character
Tab key or space bar—keyword completion in command line
Exit—go to next lower command prompt

Obtaining Help at the Command Line

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

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

Figure 4-1 illustrates the results of entering ? to get a list of possible keywords.

Figure 4-1. Partial Keyword Example

```

(Force10) #show ?

access-lists          Display Access List information.
arp                   Display Address Resolution Protocol cache.
authentication        Display ordered methods for authentication lists
bootpdhcprelay        Display the value of BOOTP/DHCP relay parameters.
class-map              Display DiffServ Class information.
classofservice         Display class of service information.
diffserv              Display DiffServ information.
dot1q-tunnel           Display double VLAN Tunneling configuration.
dot1x                  Display dot1x information.
dvlan-tunnel           Display double VLAN Tunneling configuration.
forwardingdb          Display Forwarding Database aging time.
garp                   Display Generic Attribute Registration Protocol
                      information.
gmrp                   Display GMRP interface information.
gvrp                   Display GARP VLAN Registration Protocol parameters.
hardware               Display vital product data.
igmpsnoothing         Display IGMP Snooping information.
interface              Display summary statistics for a specific port or for
                      the entire switch.

interfaces            Display Interfaces Information.
ip                     Display IP information.
logging                Display logging and eventlog parameters.
--More-- or (q)uit

(Force10) #show terminal
Command not found / Incomplete command. Use ? to list commands.

(Force10) #show terminal ?
length                 Display terminal length.

(Force10) #show terminal length ?
<cr>                   Press Enter to execute the command.

```

Using Command Modes

The CLI of SFTOS follows the industry convention of mode-based access to functionality, grouping all of the CLI commands in appropriate modes according to the nature of the commands. In other words, each of the command modes supports specific, related SFTOS software commands. You specify through CLI commands which mode you want to access, and then, in that mode, you enter commands that are specific to that mode. For example, if you want to configure a VLAN, you would first enter the Interface VLAN mode by entering the command `interface vlan vlanid` at a prompt in the Global Config mode.

The following command-mode tree diagram provides an overview of the names of the modes and how they relate to each other. The User Exec mode at the top of the tree is the mode you enter when you access the CLI.

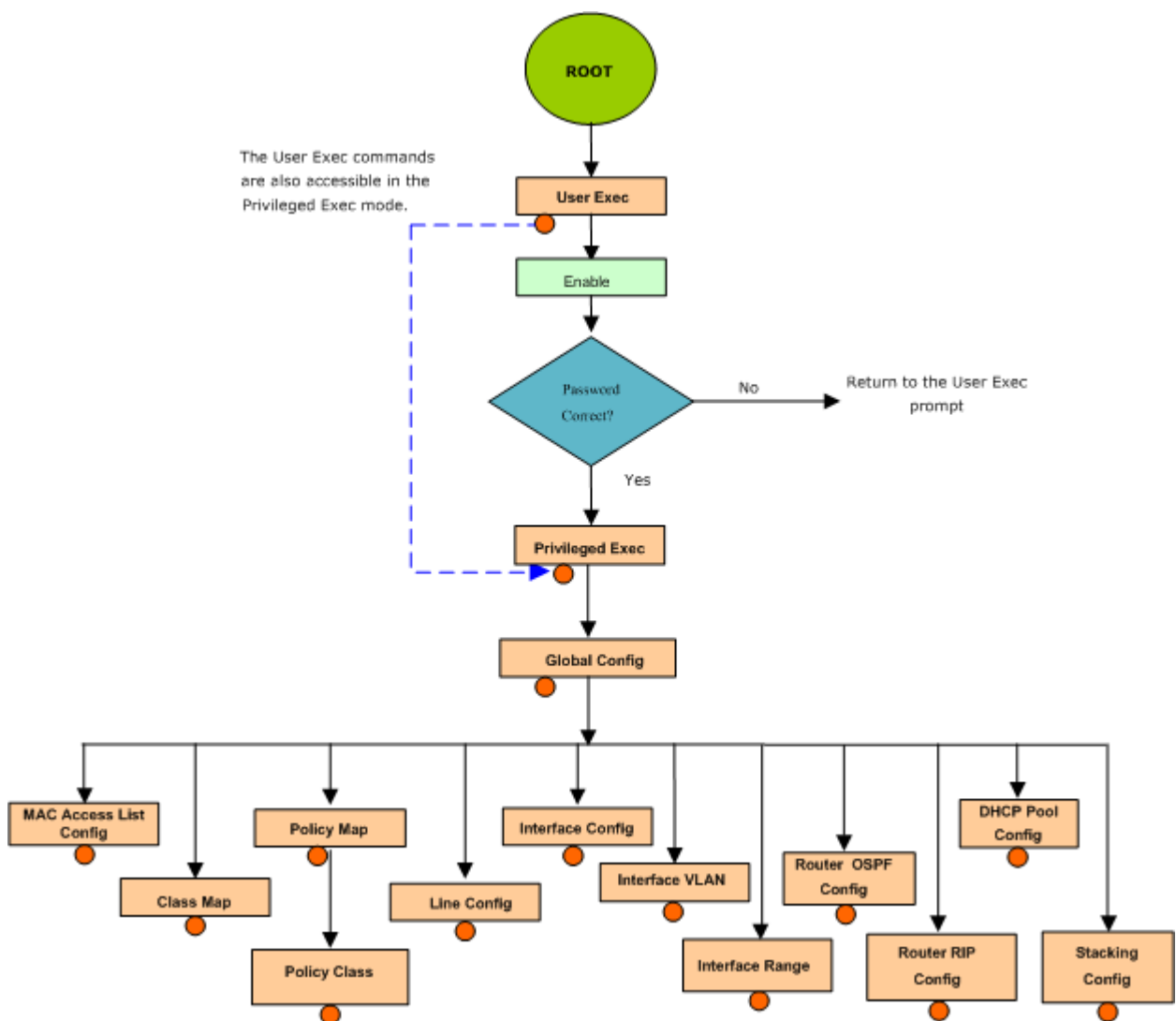
Mode-based Topology

As detailed above, the CLI is built on a mode concept, where related commands are grouped together within modes that you access with particular mode-access commands. The mode-access commands are listed in [Table 4-2 on page 30](#). Access to the modes is depicted in a tree format in [Figure 4-2](#).

Note: Except for the Interface Range mode or its child modes—Ethernet Range mode, Port Channel mode, and VLAN Range mode—and the TACACS Config mode, the diagram shows modes that are in the Layer 2 Package of SFTOS or the Layer 3 Package of SFTOS. Those in the Layer 3 Package include the various “Router” modes.

The S2410 does not use the Layer 3 modes, nor the Stacking mode.

Figure 4-2. CLI Mode Diagram





Note: Previous to Release 2.3, the VLAN mode was accessed from the Privileged Exec mode with the command `vlan database`. Starting in Release 2.3, you access the mode from the Global Config mode with the command `interface vlan vlanid`.

Note: Some modes may be unavailable, depending on the installed SFTOS image.

Access to all commands beyond the User Exec mode can be restricted through the `enable` password, which you set with the `enable passwd` command. See [enable passwd](#) on page 110.

The following table shows the relationship of the command mode names to the prompts visible in the mode and the exit method from that mode. The first three rows in the table are organized in the sequence in which you would access the child modes. Beyond the Global Config mode, the modes are either accessed from the Global Config mode or from the mode listed in the row above.

The *hostname* in the Prompt column is a placeholder for the prompt name that you create using the `hostname` command. For example, if you use “Speedy”, the User Exec prompt is `Speedy>`, the Privileged Exec prompt is `Speedy#`, and the Global Config prompt is `Speedy (Config)#`. For details, see [Figure 4-2](#) on page 29 and [Mode-based Command Hierarchy](#) on page 31.

Table 4-2. Command Modes

Command Mode	Mode Access Method	Prompt	Exit or Access Previous Mode
User Exec	This is the first level of access. Perform basic tasks and list system information.	<i>hostname</i> >	Enter <code>logout</code> .
Privileged Exec	In the User Exec mode, enter the <code>enable</code> command.	<i>hostname</i> #	To exit to the User Exec mode, enter <code>exit</code> or press Ctrl-Z.
Global Config	In the Privileged Exec mode, enter the <code>configure</code> command.	<i>hostname</i> (Config)#	To exit to the Privileged Exec mode, enter the <code>exit</code> command, or press Ctrl-Z to switch to the User Exec mode.
Class Map	In the Global Config mode, enter the <code>class-map</code> command	<i>hostname</i> (Config-classmap)#	To exit to the Global Config mode, enter the <code>exit</code> command. To return to the User Exec mode, enter Ctrl-Z.
DHCP Pool Config	In the Global Config mode, enter the <code>ip dhcp pool <i>pool-name</i></code> command.	<i>hostname</i> (Config-dhcp-pool)#	To exit to the Global Config mode, enter the <code>exit</code> command. To return to the User Exec mode, enter Ctrl-Z
Interface Config	In the Global Config mode, enter the <code>interface <i>unit/slot/port</i><<i>slot/port</i>></code> command.	<i>hostname</i> (Interface " <i>if number</i> ")#	To exit to the Global Config mode, enter the <code>exit</code> command. To return to the User Exec mode, enter Ctrl-Z.
Interface Port Channel Config	In the Global Config mode, enter the <code>interface port channel <<i>slot/port</i>></code> command.	<i>hostname</i> (Interface " <i>if-port number</i> ")#	To exit to the Global Config mode, enter the <code>exit</code> command. To return to the User Exec mode, enter Ctrl-Z.
Interface Range	In the Global Config mode, enter the <code>interface range <i>range</i> <<i>slot/port</i>></code> command.	<i>hostname</i> (conf-if-range- <i>range</i>)#, where <i>range</i> consists of the specified interface range. For example, for VLANs 100–200, the prompt is <i>hostname</i> (conf-if-range-vl-100-200)#	To exit to the Global Config mode, enter the <code>exit</code> command. To return to the User Exec mode, enter Ctrl-Z. The Ethernet Range mode, Port Channel mode, and VLAN Range mode are the three child modes of the Interface Range mode. The <code>exit</code> command returns you to the Interface Range mode.

Table 4-2. Command Modes

Command Mode	Mode Access Method	Prompt	Exit or Access Previous Mode
Interface VLAN	In the Global Config mode, enter the command interface vlan <i>vlanid</i> .	<i>hostname</i> (conf-if-vl-vlan-id) #	To exit to the Global Config mode, enter the exit command, or press Ctrl-Z to switch to the User Exec mode.
Line Config Mode	In the Global Config mode, enter the lineconfig command	<i>hostname</i> (line) #	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
Mac Access List Config	In the Global Config mode, enter the mac access-list extended command	<i>hostname</i> (Mac-Access-List Config)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
Interface ManagementEthernet	In the Global Config mode, enter the interface managementethernet command	<i>hostname</i> (Config-if-ma)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
Policy Map	In the Global Config mode, enter the policy-map command	<i>hostname</i> (Config-policy-map)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
Policy Class	In the Policy Map mode enter the class command	<i>hostname</i> (Config-policy-classmap)#	To exit to the Policy Map mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
Router OSPF Config	In the Global Config mode, enter the router ospf command	<i>hostname</i> (Config-router)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
Router RIP Config	In the Global Config mode, enter the router rip command	<i>hostname</i> (Config-router)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
Bwprovisioning - bwallocation Config Mode	From the Bwprovisioning mode, enter the bwallocation command.	Switch (Config-bwp-bwallocation) #	To exit to the Bwprovisioning mode, enter exit . To return to the User Exec mode, enter ctrl-Z .
Stacking Config	In the Global Config mode, enter the stack command.	<i>hostname</i> (Config-stack)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
TACACS Config	In the Global Config mode, enter the tacacs-server host <i>ip-address</i> command.	<i>hostname</i> (Tacacs)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.

Mode-based Command Hierarchy

As introduced above, the CLI is divided into various modes. Commands in a particular mode are not available until the operator switches to that mode, with the exception of the User Exec mode commands. The User Exec mode commands may also be executed in the Privileged Exec mode.

The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt displays a list of the available commands, along with descriptions of the commands.

The CLI provides the following modes:

User Exec Mode. When the operator logs into the CLI, the User Exec mode is the initial mode. The User Exec mode contains a limited set of commands.

Command Prompt: *hostname >*



Note: The *hostname* here is a placeholder for the prompt that you create using the *hostname* command. See [hostname on page 37](#).

Privileged Exec Mode. To have access to the full suite of commands, you must enter the Privileged Exec mode. The Privileged Exec mode requires password authentication. In Privileged Exec mode, you can issue any User Exec mode command or enter the Global Config mode. **Command Prompt:** *hostname #*

Global Config Mode. This mode permits you to make general modifications to the running configuration. From the Global Configuration mode, you can enter all of the configuration-specific modes listed below. **Command Prompt:** *hostname (Config)#*

From the Global Config mode, you may enter the following configuration modes:

Interface Port Channel Config Mode. This mode, introduced in SFTOS Version 2.5.1, groups commands pertaining to port channels.

Interface Config Mode. Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface.

In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to the router interface configuration commands. **Command Prompt:** *hostname (Interface <unit/slot/port><slot/port>)#*

The resulting prompt sequence for the interface configuration command entered in the Global Configuration mode is shown here:

```
hostname (Config)# interface 1/0/1
hostname (Interface 1/0/1)#
```

DHCP Pool Config Mode. Use the *ip dhcp pool pool-name* command to access the DHCP Pool Config. The mode is used for configuring the switch as a DHCP server.

Line Config Mode. Use this mode to configure the console interface. You may configure the interface from the directly connected console or the virtual terminal used with Telnet. **Command Prompt:** *hostname (Line)#*

Policy Map Mode. Use the *policy-map <policy-name>* command to access the QoS policy map configuration mode to configure the QoS policy map. The prompt sequence is:

```
hostname (Config)# policy map <policy name>
hostname (Config-policy-map)#
```

Policy Class Mode. Use the *class <class-name>* command to access the QoS policy-classmap mode to attach/remove a diffserv class to a policy and to configure the QoS policy class. The prompt sequence is:

```
hostname (Config policy-map)# class <class name>
```


hostname (Config-policy-classmap)#

Class Map Mode: This mode consists of class creation/deletion and matching commands. The class match commands specify Layer 2, Layer 3 and general match criteria. Use the `class-map` `class-map-name` commands to access the QoS class map configuration mode to configure QoS class maps. The prompt sequence is:

hostname (Config)# class-map <class-map-name>

hostname (Config class-map)#

Router OSPF Config Mode: In this mode, you can access the router OSPF configuration commands. The prompt sequence is:

hostname (Config)# router ospf

hostname (Config router)#

Router RIP Config Mode: In this mode, you can access the router RIP configuration commands. The prompt sequence is:

hostname (Config)# router rip

hostname (Config router)#

MAC Access List Config Mode. Use the MAC Access-List Config mode to create a MAC access-List and to enter the mode containing mac access-list configuration commands. The prompt sequence is:

hostname (Config)#mac-access-list extended name

hostname (Config-mac-access-list)#

TACACS Config Mode. Use this mode to configure the connection parameters to a TACACS+ user authentication server.

Stack Config Mode. Use the `nC O` command to access the Stack Config mode for stacking S50 switches.

VLAN Mode. (formally called the Interface Vlan Config mode, or more simply, the Interface Vlan mode) This mode groups all the commands pertaining to VLANs.

Command Prompt: *hostname (conf-if-vl-vlan-id)#*



Note: Before Release 2.3, the VLAN mode was accessed from the Privileged Exec mode. With Release 2.3, the mode is accessed from the Global Config mode by entering the command `interface vlan vlanid`.

Flow of CLI Operation

1. You log into the CLI session and enter the User Exec mode. In the User Exec mode, the “*hostname >*” prompt is displayed on the screen.

The parsing process is initiated whenever you type a command and press **ENTER**. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins. For instance, the Privileged Exec mode has the command `show arp brief`. If you attempt to execute the command, but you enter an extra “p” in “`arpp`”, then the

output message displays the ^ marker under the extra “p”, followed by “*Invalid input detected at '^' marker.*”

Another typical case when an error message appears is when you have entered an invalid input parameter in the command. The ^ marker shows where in the command the first character of invalid input was detected.

After all the mandatory parameters are entered, any additional parameters entered are treated as optional parameters. If any of the parameters are not recognized, a syntax error message will be displayed.

2. After the command is successfully parsed and validated, the control of execution goes to the corresponding CLI callback function.
3. For mandatory parameters, the command tree extends until the mandatory parameters make the leaf of the branch. The callback function is only invoked when all the mandatory parameters are provided. For optional parameters, the command tree extends till the mandatory parameters and the optional parameters make the leaf of the branch. However, the callback function is associated with the node where the mandatory parameters are fetched. The callback function then takes care of the optional parameters.
4. Once the control has reached the callback function, the callback function has complete information about the parameters entered.

System Management Commands

The commands in this chapter either manage the switch in general, configure management interfaces, or show current management settings. For every configuration command, there is a `show` command that displays the configuration setting.

This chapter contains the following major sections:

- [General System Management and Information Commands](#) on page 35
- [Telnet Commands](#) on page 71
- [remotecon maxsessions](#) on page 73
- [SNMP Management Commands](#) on page 77



Note: See also Chapter 6, “System Configuration Commands,” on page 87 and Chapter 9, “System Logs,” on page 169.

General System Management and Information Commands

This section describes the following commands:

- [cx4-cable-length](#) on page 36
- [dir](#) on page 37
- [hostname](#) on page 37
- [interface managementethernet](#) on page 38
- [ip address \(management\)](#) on page 38
- [mac-address](#) on page 39
- [mac-type](#) on page 39
- [management route default](#) on page 40
- [network mac-address](#) on page 41
- [network mac-type](#) on page 41
- [network parms](#) on page 41
- [network protocol](#) on page 41
- [protocol](#) on page 41
- [show arp switch](#) on page 42
- [show cx4-cable-length](#) on page 43
- [show ethernet](#)
- [show hardware](#) on page 46
- [show interface](#) on page 47
- [show interface ethernet](#) on page 50
- [show interface managementethernet](#) on page 57
- [show interface switchport](#) on page 59

- [show interfaces on page 59](#)
- [show logging on page 60](#)
- [show mac-addr-table on page 61](#)
- [show memory on page 63](#)
- [show msglog on page 63](#)
- [show network on page 64](#)
- [show process cpu on page 64](#)
- [show running-config on page 65](#)
- [show sysinfo on page 66](#)
- [show version on page 69](#)
- [show tech-support on page 68](#)

See also the **show** commands in the logging chapter, [System Logs on page 169](#).

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	<hr/> <table> <tr> <td>long medium short</td> <td>Enter the keyword that matches the cable length to be used at the selected port: short = 60cm, 1m, and 3m medium = 5m long = 10m, 15m</td> </tr> </table> <hr/>	long medium short	Enter the keyword that matches the cable length to be used at the selected port: short = 60cm, 1m, and 3m medium = 5m long = 10m, 15m
long medium short	Enter the keyword that matches the cable length to be used at the selected port: short = 60cm, 1m, and 3m medium = 5m long = 10m, 15m		
Default	medium		
Mode	Interface Config		
Command History	<hr/> <table> <tr> <td>Version 2.5.1</td> <td>Introduced</td> </tr> </table> <hr/>	Version 2.5.1	Introduced
Version 2.5.1	Introduced		

Example **Figure 5-3. Example of CX4 Cable Length Configuration**

```

Force10 #config
Force10 Config#interface config 1/0/49
Force10 (Interface 1/0/49)# cx4-cable-length long
Force10 (Interface 1/0/49)#exit
Force10 Config#interface config 1/0/50
Force10 (Interface 1/0/50)#no cx4-cable-length
Force10 (Interface 1/0/50)#exit
Force10 Config#exit
Force10 #show cx4-cable-length

Interface      CX4 Cable Length Setting
-----
1/0/49         long
1/0/50         medium

Force10 #

```

**Related
Commands**

show cx4-cable-length	Displays CX4 cable lengths connected to the system.
---------------------------------------	---

dir

This command displays the directory structure and files stored in NVRAM.

Syntax dir nvram

Default none

Mode Privileged Exec

**Command
History**

Version 2.3	Introduced
-------------	------------

Example **Figure 5-4. Example of dir nvram Command Output**

```
Force10 #dir nvram
RamDiskVol:filesystem>
.
..
sslt.rnd                               1024
dhcpLeases.cfg                         85088
startup-config                         6392

Filesystem size 4179968
Bytes used      92504
Bytes free     4087464

CodeStorVol:>

log2.bin                               131040
slog0.txt                               0
olog0.txt                               0
mrt.log                                 0
--More-- or (q)uit

Filesystem size 20022272
Bytes used      131040
Bytes free     19891232

Force10#
```

hostname

Change the text that appears as part of the CLI prompt.

Syntax hostname *hostname*

Parameters

<i>hostname</i>	Enter the desired text for the prompt, up to 64 alphanumeric characters.
-----------------	--

Default Force10 (For example, the User Exec prompt appears as “Force10-S50 >”.)

Mode	Global Config	
Command History	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.
	Version 2.2	Replaced set prompt command.

interface managementethernet

This command invokes the Interface ManagementEthernet mode (uses the `(Config-if-ma)#` prompt), where you can set up a management IP interface. For details on management interfaces, see the Management chapter of the *SFTOS Configuration Guide*.

Syntax	interface managementethernet	
Mode	Global Config	
Command History	Version 2.3	Introduced
Usage Information	This command provides access to the following network configuration command groups:	

Table 5-3. Interface ManagementEthernet Mode Command Families

ip	Configure network parameters of the switch.
mac-address	Configure MAC Address.
mac-type	Select the locally administered or burnedin MAC address.
vlan	Configure the Management VLAN ID of the switch.
protocol	Select DHCP, BootP, or None as the network config protocol

Related Commands	ip address (management)	Configures the IP address of the management interface.
	mac-address	Configure the MAC address of the management interface.
	mac-type	Configure the MAC type of the management interface.
	management route default	Set the IP gateway of the switch
	protocol	Set the network protocol of the management interface.
	show interface	Display a summary of statistics for a specific port, including the management port, or a count of all CPU traffic based upon the argument.
	vlan participation (management VLAN only)	Set the VLAN ID of the management interface.

ip address (management)

This command configures the IP address of the management interface.

Syntax ip address *ipaddr subnetmask*

The value for *ipaddr* is the IP Address of the management interface.

The value for *subnetmask* is a 4-digit dotted-decimal number which represents the subnet mask of the interface.

Enter **no ip address** to remove the IP Address and subnet mask.

Mode	Interface ManagementEthernet — (Config-if-ma)# prompt within the Global Config mode	
Command History	Version 2.3	Introduced: Replaces the network parms command for the IP address and subnet mask components of the management address.
Related Commands	management route default	Sets the IP gateway of the switch.
	interface managementethernet	Invokes the Interface ManagementEthernet mode.
	ip address (routed)	Configures an IP address on a routed interface.
	show interface	Displays a summary of statistics for a specific port, including the management port, or a count of all CPU traffic based upon the argument.

mac-address

Configure the MAC address to be used for the management VLAN.

Syntax	<code>mac-address mac-address</code>	
Default	None	
Mode	Interface ManagementEthernet	
Command History	Version 2.3	Introduced. Replaces the network mac-address command.
Related Commands	management route default	Sets the IP gateway of the switch.
	interface managementethernet	Invokes the Interface ManagementEthernet mode, the (Config-if-ma)# prompt.

mac-type

Configure the MAC address to be used for the management VLAN.

Syntax	<code>mac-type {local burnedin}</code>
Default	None
Mode	Interface ManagementEthernet

Command History	Version 2.3	Introduced. Replaces the network mac-type command.
Related Commands	interface managementethernet	Invokes the Interface ManagementEthernet mode, the (Config-if-ma)# prompt.

management route default

This command sets the IP gateway of the switch. The management IP address (configured with the [ip address](#), above) and the gateway must be on the same subnet.

Syntax	management route default <i>gateway</i>	
Parameters	<i>gateway</i>	Valid IP address
	Use no management route default to remove the gateway.	
Mode	Global Config	
Command History	Version 2.3	Introduced: Replaces the network parms command for the gateway part of the management address.

Usage Information Use this command along with the [ip address](#) command to configure the management address of the switch. Execute the [interface managementethernet](#) command from Global Config mode to access the [ip address](#) command, as shown in the following example.



Note: The IP Address and the gateway must be on the same subnet.

Example **Figure 5-5. Example of Configuring Management Address**

```
(s50-1) (Config)#management route default 10.10.1.254
(s50-1) (Config)#interface managementethernet
(Config-if-ma)#ip address 10.10.1.251 255.255.255.0
(Config-if-ma)#exit
(s50-1) (Config)#ip http server enable
(s50-1) (Config)#exit
(s50-1) #
(s50-1) #show interface managementethernet

IP Address..... 10.10.1.151
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.10.1.254
Burned In MAC Address..... 00:01:E8:D5:A0:39
Locally Administered MAC Address..... 00:00:00:00:00:00
MAC Address Type..... Burned In
Network Configuration Protocol Current..... None
Management VLAN ID..... 1
Web Mode..... Enable
Java Mode..... Disable
```


**Related
Commands**

interface managementethernet	Invokes the (Config-if-ma)# prompt, where you can set up a management IP interface (the ip address command; see next).
ip address (management)	Configures the IP address of the management interface.
show interface	Displays a summary of statistics for a specific port, including the management port, or a count of all CPU traffic based upon the argument.

network mac-address

This command is replaced by the [mac-address](#) command in Version 2.3.

Mode Privileged Exec

**Command
History**

Version 2.3	Introduced. Replaced by the mac-address command.
-------------	--

network mac-type

This command is replaced by the [mac-type](#) command in Version 2.3.

Mode Privileged Exec

**Command
History**

Version 2.3	Introduced. Replaced by the mac-type command.
-------------	---

network parms

**Command
History**

Version 2.3	Deprecated: Replaced, in part, by management route default for the gateway part of the management address. Replaced, in part, by interface managementethernet and ip address (management) .
-------------	---

network protocol

**Command
History**

Version 2.3	Replaced by the protocol command.
-------------	---

protocol

This command specifies the network configuration protocol to be used for the management VLAN.

Syntax protocol {bootp | dhcp | none}

Parameters	bootp	Set BootP as the network configuration protocol. This keyword has the switch periodically send requests to a Bootstrap Protocol (BootP) server until a response is received.
	dhcp	Set DHCP as the network configuration protocol. This keyword has the switch periodically send requests to a DHCP server until a response is received.
	none	This keyword indicates that the switch should be manually configured with IP information.
Default	none	
Mode	Interface ManagementEthernet	
Command History	Version 2.3	Introduced. Replaces the network protocol command.
Related Commands	management route default	Sets the IP gateway of the switch.
	interface managementethernet	Invokes the (Config-if-ma)# prompt.

show arp switch

This command displays connectivity between the switch and other devices. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations communicating with the switch.

Syntax show arp switch

Mode Privileged Exec

Example **Figure 5-6. show arp switch Command Example**

```
(Force10) #show arp switch
MAC Address          IP Address          Interface
-----
```

Report Fields **MAC Address**—A unicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB

IP Address—The IP address assigned to each interface

Interface—Ports, displayed as *unit/slot/port*

Related Commands	show arp	Displays the Address Resolution Protocol (ARP) cache, all the ARP entries learned through the routing engine.
-------------------------	--------------------------	---

show cx4-cable-length

Display the cable lengths of the cables connected to CX4 cards in the system.

Syntax	show cx4-cable-length		
Default	none		
Mode	EXEC Privilege		
Command History	<hr/> <table><tr><td>Version 2.5.1</td><td>Introduced</td></tr></table> <hr/>	Version 2.5.1	Introduced
Version 2.5.1	Introduced		
Usage	See Figure 5-3 on page 36 .		
Related Commands	<hr/> <table><tr><td>cx4-cable-length</td><td>Set the cable length of the cable connected to the CX4 card at the port.</td></tr></table> <hr/>	cx4-cable-length	Set the cable length of the cable connected to the CX4 card at the port.
cx4-cable-length	Set the cable length of the cable connected to the CX4 card at the port.		

show ethernet

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

Syntax	show ethernet {switchport <i>unit/slot/port</i> 1-3965}						
Parameters	<hr/> <table><tr><td>switchport</td><td>Display statistics for the entire switch. See the example output in Figure 5-7, below.</td></tr><tr><td><i>unit/slot/port</i></td><td>Enter interface in unit/slot/port format. See the example output in Figure 5-8 on page 45.</td></tr><tr><td>1-3965</td><td>Enter a VLAN ID.</td></tr></table> <hr/>	switchport	Display statistics for the entire switch. See the example output in Figure 5-7 , below.	<i>unit/slot/port</i>	Enter interface in unit/slot/port format. See the example output in Figure 5-8 on page 45 .	1-3965	Enter a VLAN ID.
switchport	Display statistics for the entire switch. See the example output in Figure 5-7 , below.						
<i>unit/slot/port</i>	Enter interface in unit/slot/port format. See the example output in Figure 5-8 on page 45 .						
1-3965	Enter a VLAN ID.						
Mode	Privileged Exec						
	<hr/> <table><tr><td>show interface ethernet</td><td>Displays detailed statistics for a specific port or for all CPU traffic based upon the argument.</td></tr><tr><td>show tech-support</td><td>Displays a compilation of many “show” commands</td></tr></table> <hr/>	show interface ethernet	Displays detailed statistics for a specific port or for all CPU traffic based upon the argument.	show tech-support	Displays a compilation of many “show” commands		
show interface ethernet	Displays detailed statistics for a specific port or for all CPU traffic based upon the argument.						
show tech-support	Displays a compilation of many “show” commands						

Example 1 **Figure 5-7. Example of show ethernet switchport Output**

```
(Force10) #show ethernet switchport
Total Packets Received (Octets)..... 0
Unicast Packets Received..... 0
Multicast Packets Received..... 0
Broadcast Packets Received..... 0

Octets Transmitted..... 0
Unicast Packets Transmitted..... 0
Multicast Packets Transmitted..... 0
Broadcast Packets Transmitted..... 0
Most Address Entries Ever Used..... 1
Address Entries Currently in Use..... 1

Maximum VLAN Entries..... 3965
Most VLAN Entries Ever Used..... 1
Static VLAN Entries..... 1
Dynamic VLAN Entries..... 0
VLAN Deletes..... 0
Time Since Counters Last Cleared..... 0 day 0 hr 11 min 7 sec
```

Example 2 Figure 5-8. Example of show ethernet unit/slot/port Output

```
(Forcel0) #show ethernet 1/0/1
Type..... Normal
Admin Mode..... Disable
Physical Mode..... Auto
Physical Status..... Down
Speed..... 0 - None
Duplex..... N/A
Link Status..... Down
MAC Address..... 0001.E8D5.BBDE
Native Vlan..... 1

Total Packets Received (Octets)..... 0
Packets Received > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 0
Packets RX and TX 65-127 Octets..... 0
Packets RX and TX 128-255 Octets..... 0
Packets RX and TX 256-511 Octets..... 0
Packets RX and TX 512-1023 Octets..... 0
Packets RX and TX 1024-1518 Octets..... 0
Packets RX and TX 1519-1522 Octets..... 0
Packets RX and TX 1523-2047 Octets..... 0
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0
Total Packets Received Without Errors..... 0
Unicast Packets Received..... 0
Multicast Packets Received..... 0
Broadcast Packets Received..... 0
Jabbers Received..... 0
Fragments Received..... 0
Undersize Received..... 0
Alignment Errors..... 0
FCS Errors..... 0
Overruns..... 0

Total Received Packets Not Forwarded..... 0
Local Traffic Frames..... 0
802.3x Pause Frames Received..... 0
Unacceptable Frame Type..... 0
Multicast Tree Viable Discards..... 0
Reserved Address Discards..... 0
Broadcast Storm Recovery..... 0
CFI Discards..... 0
Upstream Threshold..... 0

Total Packets Transmitted (Octets)..... 0
Max Frame Size..... 1518
Unicast Packets Transmitted..... 0
Multicast Packets Transmitted..... 0
Broadcast Packets Transmitted..... 0
FCS Errors..... 0
Tx Oversized..... 0
Underrun Errors..... 0
Single Collision Frames..... 0
Multiple Collision Frames..... 0
Excessive Collision Frames..... 0
Port Membership Discards..... 0

802.3x Pause Frames Transmitted..... 0
GVRP PDUs received..... 0
GVRP PDUs Transmitted..... 0
GVRP Failed Registrations..... 0
GMRP PDUs Received..... 0
GMRP PDUs Transmitted..... 0
GMRP Failed Registrations..... 0

STP BPDUs Transmitted..... 0
STP BPDUs Received..... 0
RSTP BPDUs Transmitted..... 0
RSTP BPDUs Received..... 0
--More-- or (q)uit
MSTP BPDUs Transmitted..... 0
MSTP BPDUs Received..... 0

EAPOL Frames Transmitted..... 0
EAPOL Start Frames Received..... 0
Time Since Counters Last Cleared..... 0 day 0 hr 11 min 1 sec
```

show hardware

This command displays inventory information for the switch.

Syntax	show hardware
Mode	Privileged Exec
Command History	Version 2.5.1 Modified to include information about XFP/SFPs plugged into the system.

Example **Figure 5-9. Example of Using show hardware Command**

```
(Force10#show hardware
Switch: 1
System Description..... Force10 48GE 4TENGIG L3 Stackable
switch
Vendor ID..... 07
Plant ID..... 01
Country Code..... 04
Date Code.....
Serial Number..... 3232322
Part Number.....
Revision.....
Catalog Number..... SA-01-GE-48T
Burned In MAC Address..... 00:02:03:04:05:06
Software Version..... 0.0.0.0

Additional Packages..... Force10 QOS
Force10 Stacking

Additional XFP/SFP Modules
Vendor Name..... FINISAR CORP.
Serial Number..... P11LY41
Part Number..... FTRJ-8519-7D

Vendor Name..... FINISAR CORP.
Serial Number..... P6D15NC
Part Number..... FTRJ1319P1BTL
```

Table 5-4. Fields in the Output of the show hardware Command

Field	Description
Switch Description	Text used to identify the product name of this switch
Vendor ID	Number used to identify the manufacturer of the device
Plant ID	
Country Code	
Date Code	Month and year of manufacture of the switch
Serial Number	The unique box serial number for this switch
Part Number	Manufacturing part number
Revision	
Catalog Number	The catalog number of the switch
Burned in MAC Address	Universally assigned network address
Software Version	The version of the SFTOS software currently running on the switch, expressed as base.release.version.revision.
Additional Packages	The software modules that are incorporated into this version of SFTOS

Related Commands

show cx4-cable-length	Displays CX4 cable lengths connected to the system.
show tech-support	Displays the output of many show commands, including this one.

show interface

This command displays a summary of statistics for a specific port or for the entire switch, depending on the argument.

Syntax `show interface { unit/slot/port | ethernet { switchport | unit/slot/port | 1-3965 } | loopback | managementethernet | switchport }`

Parameters

<i>unit/slot/port</i>	Enter the port number of a particular port to query, where unit is the stack member, slot is always 0 (zero), and port is the port number. The display parameters are shown below.
ethernet { <i>switchport</i> <i>unit/slot/port</i> 1-3965 }	See show interface ethernet on page 50 .
loopback	See show interface loopback on page 99 .
managementethernet	See show interface managementethernet on page 57 .
switchport	Enter the keyword to display a summary of statistics on Layer 2 interfaces. See show interface switchport on page 59 .

Mode Privileged Exec

Command History

Version 2.5.1	Modified: Added port channel options and Native VLAN information to VLAN output. Many report fields changed.
---------------	--

Usage Information

Figure 5-10 shows an example of the `show interface unit/slot/port` report on the S50 model. Table 5-5 contains an explanation of the report fields. Figure 5-11 on page 49 shows an example of the report on the S50 model. Table 5-6 on page 49 contains the report fields.

See the links above or in the Related Commands section, below, for details on the other options.

Example**Figure 5-10. S50: Output of the show interface unit/slot/port Command**

```
Forcel0#show interface 1/0/2
Packets Received Without Error..... 0
Packets Received With Error..... 0
Broadcast Packets Received..... 0
Packets Transmitted Without Errors..... 579
Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 0 day 0 hr 18 min 58 sec
Native Vlan..... 1
```

The display parameters of the `show interface` command for the S50 model, when the argument is `unit/slot/port`, are as follows:

Table 5-5. Fields in Output of show interface unit/slot/port Command

Field	Description
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received on the interface.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The number of packet collisions
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

Figure 5-11. S50V: Output of the show interface unit/slot/port Command

```
Force10-S50V#show interface 1/0/1

Packets Received Without Error..... 1555
Packets Received With Error..... 0
Broadcast Packets Received..... 642
Packets Transmitted Without Errors..... 0
Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 3 day 20 hr 59 min 6 sec
Native Vlan..... 1

Rate Info (interval 300 seconds):
Packets Rx Rate Mbits/sec..... 00.00
Packets Tx Rate Mbits/sec..... 00.00
Packets Rx Rate packets/sec..... 00.00
Packets Tx Rate packets/sec..... 00.00
Packets Rx Line Rate..... 0.00%
Packets Tx Line Rate..... 0.00%

Force10-S50V#
```

When the show interface *unit/slot/port* command is run on the S50V, the following second group of fields is also displayed (these fields are displayed by the show interface ethernet *unit/slot/port* command.):

Table 5-6. Fields in Output of show interface *unit/slot/port* Command

Field	Description
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received on the interface.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The number of packet collisions
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

Related Commands

ip address (management)	Configures the IP address of the management interface.
show ethernet	Displays detailed statistics for a specific port or summary information for all CPU traffic, based upon the argument.
show interface ethernet	Displays detailed statistics for a specific port or for all CPU traffic based upon the argument.
show interface switchport	Displays a summary of statistics on Layer 2 interfaces.

<code>show interface managementethernet</code>	Displays information about the management interface to the switch.
<code>show interfaces port-channel</code>	Displays detailed statistics for a specific LAG or summary information for all LAGs, based upon the argument.
<code>show ip interface</code>	Displays summary information about IP configuration settings for all ports in the router.
<code>show interfaces</code>	Displays information about a selected interface or VLAN

show interface ethernet

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

Syntax `show interface ethernet {switchport | unit/slot/port | 1-3965}`

Parameters

<code>switchport</code>	The display parameters for when <code>switchport</code> is entered, are shown below the list for <i>unit/slot/port</i> .
<i>unit/slot/port</i>	Valid unit, slot and, port number, separated by forward slashes. The display parameters are shown below.
<code>1-3965</code>	VLAN ID

Mode Privileged Exec

Command History

Version 2.5.1 Modified: Many report fields changed

Usage Information

This command displays distinctly different reports, depending on the entered parameter.

[Figure 5-12](#) shows an example of the `show interface ethernet` report when the keyword `switchport` is added. [Table 5-7 on page 51](#) contains an explanation of the report fields.

[Figure 5-13](#) shows an example of the `show interface ethernet` report when the argument is *unit/slot/port*. [Table 5-8 on page 52](#) contains an explanation of the report fields.

Example 1 Figure 5-12. Example of show interface ethernet switchport Output

```
(Forcel0) #show interface ethernet switchport
Total Packets Received (Octets)..... 40648140
Unicast Packets Received..... 324
Multicast Packets Received..... 307772
Broadcast Packets Received..... 3
Receive Packets Discarded..... 0

Octets Transmitted..... 42855160
Packets Transmitted Without Errors..... 319879
Unicast Packets Transmitted..... 327
Multicast Packets Transmitted..... 307916
Broadcast Packets Transmitted..... 11636
Transmit Packets Discarded..... 0
Most Address Entries Ever Used..... 5
Address Entries Currently in Use..... 2

Maximum VLAN Entries..... 1024
Most VLAN Entries Ever Used..... 2
Static VLAN Entries..... 2
Dynamic VLAN Entries..... 0
VLAN Deletes..... 0
Time Since Counters Last Cleared..... 2 day 16 hr 9 min 26 sec
```

The display fields of `show interface ethernet`, when the keyword `switchport` is added, are as follows:

Table 5-7. Fields in Output of show interface ethernet switchport Command

Field	Description
Total Packets Received (Octets)	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters
Packets Transmitted without Errors	The total number of packets transmitted out of the interface
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent

Table 5-7. Fields in Output of show interface ethernet switchport Command

Field	Description
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot
Address Entries Currently in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared

Example 2 Figure 5-13. Example of show interface ethernet unit/slot/port Output (truncated)

```
(Forcel0) #show interface ethernet 1/0/1
Type..... Normal
Admin Mode..... Enable
Physical Mode..... Auto
Physical Status..... Up
Speed..... 1 Gig
Link Status..... Up
MAC Address..... 0001.E8D5.A0F8
Total Packets Received (Octets)..... 15508603844
Packets Received > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 0
Packets RX and TX 65-127 Octets..... 216200946
Packets RX and TX 128-255 Octets..... 2441
{More}
```

The show interface ethernet display fields, when the argument is *unit/slot/port*, are as follows:

Table 5-8. Fields in Output of show interface ethernet unit/slot/port Command

Field	Description
Packets Received	
Type	Indicates current type of use of the port, such as “PC Mbr” to indicate port channel member, “Mirror” to indicate source port for port-mirroring, “Probe” to indicate destination port for mirroring, and, most commonly, “Normal”.
Admin Mode	Whether the port is administratively enabled or disabled
Physical Mode	Whether the port is physically up or down

Table 5-8. Fields in Output of show interface ethernet *unit/slot/port* Command

Field	Description
Physical Status	Whether the port is physically connected or disconnected
Speed	The port speed setting
Duplex	
Link Status	Whether the link is up or down.
MAC Address	MAC address of the port
Native Vlan	
Total Packets Received (Octets)	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received 1024-1518 Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.
Packets Received > 1522 Octets	The total number of packets (including bad packets) received that were greater than 1522 octets in length (excluding framing bits but including FCS octets).
(The following fields appear in the output in this sequence: Packets RX and TX 64 Octets Packets RX and TX 65-127 Octets Packets RX and TX 128-255 Octets Packets RX and TX 256-511 Octets Packets RX and TX 512-1023 Octets Packets RX and TX 1024-1518 Octets Packets RX and TX 1519-1522 Octets Packets RX and TX 1523-2047 Octets Packets RX and TX 2048-4095 Octets Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received and sent that were within the range of octets in length (excluding framing bits but including FCS octets) specified by the field label Note: The 1519-1522 frame counter is incremented only for VLAN-tagged frames. Untagged frames with that size increment the >1522 counter (“Packets Received > 1522 Octets”).
Rate Info (interval 300 seconds):	
Packets Rx Rate Mbits/sec	
Packets Tx Rate Mbits/sec	
Packets Rx Rate packets/sec	
Packets Tx Rate packets/sec	
Packets Rx Line Rate	
Packets Tx Line Rate	
Packets Received Successfully	
Total Packets Received Without Errors	The total number of packets received that were without errors
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol

Table 5-8. Fields in Output of show interface ethernet unit/slot/port Command

Field	Description
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Undersize Received	
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow
Received Packets not forwarded	
Total Received Packets Not Forwarded	A count of valid frames received which were discarded (i.e. filtered) by the forwarding process
Local Traffic Frames	The total number of frames dropped in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type. An entry in this field does not necessarily indicate that the interface is receiving error packets. This field is incremented when packets are dropped due to an ACL filtering them out, when tagged packets are received on an untagged port, or when untagged packets are received on a tagged port. This field does not increment when the following packets are received: CRC error packets, non-IP packets, giants.
Multicast Tree Viable Discards	The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.

Table 5-8. Fields in Output of show interface ethernet *unit/slot/port* Command

Field	Description
Reserved Address Discards	The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.
Broadcast Storm Recovery	The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled
CFI Discards	The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.
Upstream Threshold	The number of frames discarded due to lack of cell descriptors available for that packet's priority level.
Packets Transmitted Octets	
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets)
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 1519-1522 Octets	The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets)
Max Frame Size	The maximum size of the Info (non-MAC) field that this port will receive or transmit
Packets Transmitted Successfully	
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent

Table 5-8. Fields in Output of show interface ethernet *unit/slot/port* Command

Field	Description
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent
Transmit Errors	
Total Transmit Errors	The sum of Single, Multiple, and Excessive Collisions
FCS Errors	The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Tx Oversized	The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions
Port Membership Discards	The number of frames discarded on egress for this port due to egress filtering being enabled
Protocol Statistics	
BPDUs received	The count of BPDUs (Bridge Protocol Data Units) received in the spanning tree layer
BPDUs Transmitted	The count of BPDUs (Bridge Protocol Data Units) transmitted from the spanning tree layer
802.3x Pause Frames Transmitted	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDUs received	The count of GVRP PDUs received in the GARP layer
GVRP PDUs Transmitted	The count of GVRP PDUs transmitted from the GARP layer
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed
GMRP PDUs received	The count of GMRP PDU's received in the GARP layer
GMRP PDUs Transmitted	The count of GMRP PDU's transmitted from the GARP layer
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received

Table 5-8. Fields in Output of show interface ethernet unit/slot/port Command

Field	Description
RST BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received
Dot1x Statistics	
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared

Related Commands

ip address (management)	Configures the IP address of the management interface.
show interface	Displays statistics for a specific port.
show interface switchport	Displays a summary of statistics on Layer 2 interfaces.
show interfaces	Displays information about a selected interface or VLAN

show interface managementethernet

This command displays information about the management address of the switch.

Syntax show interface managementethernet

Mode Privileged Exec

Command History

Version 2.3	Modified: Added the keyword managementethernet to show interface to provide the information that had been available through the show network command.
-------------	--

Usage Information

The display parameters of the **show interface** command, when the keyword is **managementethernet**, are as follows:

Table 5-9. Fields in Output of show interface managementethernet command

Field	Description
IP Address	The IP address of the interface. The factory default value is 0.0.0.0
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0
Burned In MAC Address	The burned in MAC address used for in-band connectivity

Table 5-9. Fields in Output of show interface management ethernet command

Field	Description
Java Mode	Enable or Disable. Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is disabled.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	Specifies which MAC address should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Management VLAN ID	Specifies the management VLAN ID.
Network Configuration Protocol Current	Indicates which network protocol is being used. The options are bootp dhcp none.
Web Mode	Enable or Disable

Related Commands

ip address (management)	Configures the IP address of the management interface.
show ethernet	Displays statistics for a specific port or for the switch.
show interface	Displays statistics for a specific port.
show interface switchport	Displays a summary of statistics on Layer 2 interfaces.
show interface ethernet	Displays detailed statistics for a specific ethernet port or for all CPU traffic based upon the argument.
show interfaces	Displays information about a selected interface or VLAN

show interface switchport

This command displays a summary of statistics on Layer 2 interfaces.

Syntax show interface switchport

Mode Privileged Exec

Usage Information The display parameters of show interface, when the argument is switchport, are as follows:

Table 5-10. Fields in Output of show interface switchport Command

Field	Description
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

Related Commands

ip address (management)	Configures the IP address of the management interface.
show interface	Displays statistics for a specific port.
show interface managementethernet	Displays information about the management interface.
show interface ethernet	Displays detailed statistics for a specific ethernet port or for all CPU traffic based upon the argument.
show interfaces	Displays information about a selected interface or VLAN

show interfaces

This command displays information about a selected interface or VLAN.

Syntax	show interfaces {cos-queue [<i>unit/slot/port</i>] description { <i>unit/slot/port</i> 1-3965} port-channel { 1-128 brief} switchport <i>unit/slot/port</i> 0-2}	
Parameters	cos-queue [<i>unit/slot/port</i>]	(OPTIONAL) For details on this option, see show interfaces cos-queue on page 334 .
	description { <i>unit/slot/port</i> 1-3965}	(OPTIONAL) Enter the keyword description followed by the interface in the form <i>unit/slot/port</i> . Alternatively, enter a VLAN ID to display information for that VLAN (must be a VLAN enabled for routing).
	port-channel { 1-128 brief}	See show interfaces port-channel on page 303 .
	switchport <i>unit/slot/port</i> 0-2	(OPTIONAL) Enter the interface ID and an integer between 0–2, identifying the protected port group. See show port-channel brief on page 304 .
Mode	Privileged Exec	
Command History	Version 2.3	Modified: Added description [<i>unit/slot/port</i>] parameter.
Usage Information	The following example shows sample output of the show interfaces description command with an interface specified in the <i>unit/slot/port</i> form:	
Example	<p>Figure 5-14. Output of the show interfaces description Command</p> <pre> Forcel0#show interfaces description 1/0/1 Interface.....1/0/1 IfIndex.....1 Description....1/0/1 is access port MAC Address....00:01:E8:D5:BA:C0 Bit Offset Val..1 </pre>	
Related Commands	show interface	Displays statistics for a specific port or port channel (LAG).
	show interfaces cos-queue	Displays the class-of-service queue configuration for the specified interface.
	show ip interface	Displays summary information about IP configuration settings for all ports in the router.

show logging



Note: See the various versions of the show logging command in the Syslog chapter, as linked, below

Related Commands	show logging eventlog	Displays a combination of the system log and event log (buffered log).
	show logging	Displays buffered logging (the System log)
	show logging hosts	Displays configured logging hosts (syslog servers).

<code>show logging traplogs</code>	Displays trap summaries (number of traps since last reset and last view) and trap details.
<code>show tech-support</code>	Displays the output of many show commands, including <code>show logging</code> .

show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. the same as entering the optional `all` parameter. Alternatively, you can enter a MAC address to display the table entry for that address and all entries following it.

Syntax `show mac-addr-table [macaddr | all] [interface unit/slot/port | vlan VLAN_ID | count]`


Parameters	<code>macaddr</code>	(OPTIONAL) Enter a 6-byte MAC address.
	<code>all</code>	(OPTIONAL) Enter <code>all</code> to get results for all interfaces.
	<code>interface unit/slot/port</code>	(OPTIONAL) To show MAC addresses on a particular interface, enter the keyword <code>interface</code> followed by the interface unit, slot, and port. This can be a physical or logical interface.
	<code>vlan VLAN_ID</code>	(OPTIONAL) To show MAC addresses in a particular VLAN, enter the keyword <code>vlan</code> followed by the VLAN ID.
	<code>count</code>	(OPTIONAL) Display Multicast Forwarding Database (MFDB) count.

Mode Privileged Exec


Example **Figure 5-15. Example of Output from the show mac-addr-table all Command**

```
(S50-TAC-8) #show mac-addr-table all
-----
      Mac Address      Interface  IfIndex  Status
-----
00:01:00:01:E8:D5:A1:51  0/3/1     401      Management
00:01:00:03:6C:13:91:31  1/0/30    30       Learned
00:01:00:D0:01:97:2C:0A  1/0/30    30       Learned
00:04:00:01:E8:D5:9E:D2  VLAN 4    434      Management
```

Field Descriptions: **Mac Address**—A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system, the MAC address is displayed as 8 bytes. In an SVL system, this will display the system's address aging timeout value in seconds.

 **Note:** IVL (Independent VLAN Learning) allows unicast address-to-port mappings to be created based on a MAC address in conjunction with a VLAN ID. In an IVL system, the MAC address is displayed as 8 bytes.

Interface—The Unit/Slot/Port at which this address was learned.

 **Note:** The “0/3/1” in the Interface column references the CPU. See [Figure 5-15](#) and [Figure 5-17](#).

IfIndex—This object indicates the IfIndex of the interface table entry associated with this port. It is a reserved ID that the switch assigns to physical, logical, and VLAN interfaces for the switch to transmit data across the ports within a switch.

In the S50 switch running SFTOS 2.5.1, the IfIndex ID ranges are:

- Physical ports—1 to 400 (stack of 8 units x 50 ports per unit = 400 upper limit)
- Management port—401 (The next ID available after the physical ports)
- LAGs (port channels)—402 to 529 (32 LAGs possible)
- Layer 3 VLAN interfaces—530 to 657 (128 possible Layer 3 VLANs)

In the S50 switch running SFTOS 2.3 and before, the IfIndex ID ranges are:

- Physical ports—1 to 400 (stack of 8 units x 50 ports per unit = 400 upper limit)
- Management port—401 (The next ID available after the physical ports)
- LAGs (port channels)—402 to 433 (32 LAGs possible)
- Layer 3 VLAN interfaces—434 to 561 (128 possible Layer 3 VLANs)

The S50V and S25P have an extra expansion slot for an additional 10G module with another two ports (51 & 52), which makes the ifIndex count as 52 ports per unit in the S50V (versus 50 in the S50). So, the range allocation in the S50V (and S25P) is:

- Physical ports—1 to 416 (stack of 8 units x 52 ports per unit = 416 upper limit)
- Management port—417 (The next ID available after the physical ports)
- LAGs (port channels)—418 to 545 (128 LAGs possible)
- Layer 3 VLAN interfaces—546 to 673 (128 possible Layer 3 VLANs)

Status—The status of this entry. The meanings of the values are:

Static—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned.

Learned—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.

Management—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1 and is currently used when enabling VLANs for routing.

GMRP Learned—The value of the corresponding was learned via GMRP and applies to Multicast.

Other—The value of the corresponding instance does not fall into one of the other categories.

Example Figure 5-16. Example of Output from the show mac-addr-table count Command

```
Forcel0 #show mac-addr-table count
Dynamic Address count..... 0
Static Address (User-defined) count..... 0
Total MAC Addresses in use..... 0
Total MAC Addresses available..... 16384
```

Example Figure 5-17. Example of Output from the show mac-addr-table vlan Command

```
(S50-TAC-8) #show mac-addr-table vlan 1
Mac Address      Interface      Status
-----
00:01:E8:D5:A2:19  0/3/1         Management
```

Related Commands

show mac-address-table	Depending on selected display parameters, displays various Multicast Forwarding Database (MFDB) information, including GMRP or IGMP Snooping entries in the table.
--	--

show memory

The output from this command displays current memory usage in bytes, in tabular format.

Syntax show memory

Mode Privileged Exec

Example **Figure 5-18. Example of Output from the show memory Command**

```
(Force10) #show memory
Total Memory (b)    Used Memory (b)    Free Memory (b)
31326208           12738560           18587648
```

Usage This command shows the entire system memory usage, including tasks created by the operating system and the application layer (SFTOS). In contrast, **show process cpu** shows only memory used by application tasks.

Command History

Version 2.5.1	Introduced
---------------	------------

Related Commands

show process cpu	Displays current CPU usage in percentage and a list of all currently running tasks, along with their individual CPU usage.
show tech-support	Displays the output of many show commands, including this one.

show msglog

Command History

Version 2.3	Deprecated: The keyword traplogs in the command show logging provides the information that had been available through this command.
-------------	---

Related Commands

show logging traplogs	Displays the SNMP trap log maintained by the switch.
show logging eventlog	Displays a combination of the system log and event log (buffered log).
show logging	Displays buffered logging (the System log)
show logging hosts	Displays configured logging hosts (syslog servers).

show network

Command History

Version 2.3 Deprecated: The keyword `managementethernet` in the command `show interface` provides the information that had been available through this command.

Related Commands

[show interface](#) Displays information about the management address of the switch.
[managementethernet](#)

show process cpu

The output from this command displays current switch memory used by application, in percentage form and in a list of all currently running tasks, along with their individual usage.

Syntax `show process cpu`

Mode Privileged Exec

Command History

Version 2.5.1 Introduced
 Note also that the `show tech-support` command now includes the output of this command.

Example

Figure 5-19. Example of Output from the `show process cpu` Command

```
(Force10) #show process cpu
Memory Utilization Report
status      bytes
-----
free       95145000
alloc     109810976
Task Utilization Report
Task                               Utilization
-----
osapiTimer                          5.00%
bcmCNTR.0                            0.20%
bcmCNTR.1                            0.40%
bcmL2X.2                             0.60%
bcmCNTR.2                             0.60%
bcmL2X.3                             0.60%
bcmCNTR.3                             0.20%
bcmL2X.4                             0.60%
bcmCNTR.4                             0.40%
bcmRX                                0.50%
SNMPCfgTask                          0.10%
RMONTask                              0.10%
```

Usage This command shows only memory used by application tasks. In contrast, `show memory` shows the entire system memory usage, including tasks created by the operating system and the application layer (SFTOS).

Related Commands

[show memory](#) Displays current memory usage in bytes in tabular format.
[show tech-support](#) Displays the output of several `SHOW` commands.

show running-config

This command is used to display/capture the current setting of different protocol packages supported on the switch. This command displays/captures only commands with settings/configurations with values that differ from the default value. The output is displayed in script format, which can be used to configure another switch with the same configuration.

Syntax show running-config [all] [*scriptname*]

The option **all** adds the display/capture of default values. When a script name is provided for the *scriptname* variable, the output is redirected to a configuration script. If the variable includes a file name extension of “.scr”, the output will be redirected to a script file.

Mode Privileged Exec

If [port-channel staticcapability](#) is enabled, the device has static capability enabled.

Example **Figure 5-20. Using the show running-config command**

```
(S50-5) #show running-config all
!Current Configuration:
!
configure

!System Description "Force10 S50"
!System Description 2.3.1.5
hostname "S50-5"
no dvlan-tunnel l2pdu-forwarding enable
  no dvlan-tunnel l2pdu-forwarding mac-address
  no gmrp adminmode enable
  no gvrp adminmode enable
no ip ssh server enable
sshcon maxsessions 5
sshcon timeout 5
no ip http javamode enable
no ip http secure-server enable
ip http secure-server enable
ip http secure-protocol TLS1 SSL3
ip http secure-port 443
no ip http server enable
ip http server enable
snmp unicast client poll-interval 6
  snmp unicast client poll-retry 1
  snmp unicast client poll-timeout 5
snmp broadcast client poll-interval 6
snmp client port 123
stack
  member 1 1
exit
logging buffered
logging buffered wrap
no logging console
logging facility local7
```



Note: This sample of the output is just a small part of the many thousands of lines that can be generated by this command.

Command History

Version 2.5.1 Modified: Output is indented in outline form.

Usage Information

Starting with Release 2.3, **show running-config startup-config** provides the user the opportunity to capture the running-config data to the startup-config file as a text file. If a startup-config file is already present, the system will prompt the user to overwrite it.

Related Commands

copy	Downloads files to the switch and uploads files from the switch. Copies files within the system and between switches.
script apply	Applies the commands in the designated script to the switch.
script list	Lists all scripts present on the switch as well as the total number of files present.
script show	Displays the contents of a designated script file.
show tech-support	Displays the output of many SHOW commands, including this one.

show sysinfo

This command displays switch information.

Syntax show sysinfo

Mode Privileged Exec

Example Figure 5-21. Using the show sysinfo command

```
(Force10) #show sysinfo

System Description..... Force10-S50 48GE 2TENGIG L3
                          Stackable switch
System Name.....
System Location.....
System Contact.....
System Object ID..... force10
System Up Time..... 0 days 0 hrs 26 mins 39 secs
Current SNTP Synchronized Time..... Not Synchronized

MIBs Supported:

RFC 1907 - SNMPv2-MIB          The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB           Remote Network Monitoring Management
                              Information Base
FORCE10-REF-MIB               Forcel10 Reference
SNMP-COMMUNITY-MIB           This MIB module defines objects to help
                              support coexistence between SNMPv1, SNMPv2,
                              and SNMPv3.
SNMP-FRAMEWORK-MIB           The SNMP Management Architecture MIB
SNMP-MPD-MIB                  The MIB for Message Processing and
                              Dispatching
SNMP-NOTIFICATION-MIB        The Notification MIB Module
SNMP-TARGET-MIB              The Target MIB Module
SNMP-USER-BASED-SM-MIB       The management information definitions for
                              the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB      The management information definitions for
                              the View-based Access Control Model for SNMP.
                              SNMP Research, Inc.
USM-TARGET-TAG-MIB           Forcel10 Power Ethernet Extensions MIB
F100S-POWER-ETHERNET-MIB     Power Ethernet MIB
POWER-ETHERNET-MIB           The Link Aggregation module for managing
LAG-MIB                        IEEE 802.3ad
RFC 1213 - RFC1213-MIB       Management Information Base for Network
RFC 1493 - BRIDGE-MIB        Management of TCP/IP-based internets: MIB-II
                              Definitions of Managed Objects for Bridges
                              (dot1d)
RFC 2674 - P-BRIDGE-MIB      The Bridge MIB Extension module for managing
                              Priority and Multicast Filtering, defined by
                              IEEE 802.1D-1998.
RFC 2674 - Q-BRIDGE-MIB      The VLAN Bridge MIB module for managing
                              Virtual Bridged Local Area Networks
RFC 2737 - ENTITY-MIB        Entity MIB (Version 2)
RFC 2863 - IF-MIB            The Interfaces Group MIB using SMiv2
RFC 3635 - Etherlike-MIB     Definitions of Managed Objects for the
                              Ethernet-like Interface Types
F100S-SWITCHING-MIB          Forcel10 Switching - Layer 2
F100S-INVENTORY-MIB          Unit and Slot configuration.
F100S-PORTSECURITY-PRIVATE-MIB Port Security MIB.
IEEE8021-PAE-MIB             Port Access Entity module for managing IEEE
                              802.1X.
F100S-RADIUS-AUTH-CLIENT-MIB Forcel10 Radius MIB
RADIUS-ACC-CLIENT-MIB        RADIUS Accounting Client MIB
RADIUS-AUTH-CLIENT-MIB       RADIUS Authentication Client MIB
FASTPATH-MGMT-SECURITY-MIB   The LVL7 Private MIB for FastPath Mgmt
                              Security
IANA-ADDRESS-FAMILY-NUMBERS-MIB The MIB module defines the
                              AddressFamilyNumbers textual convention.
RFC 1724 - RIPv2-MIB         RIP Version 2 MIB Extension
RFC 1850 - OSPF-MIB          OSPF Version 2 Management Information Base
!-----output truncated-----!
```

Table 5-11. Fields in Output of show sysinfo Command

Field	Description
Switch Description	Text used to identify this switch
System Name	Name used to identify the switch
System Location	Text used to identify the location of the switch. May be up to 31 alpha-numeric characters. The factory default is blank

Table 5-11. Fields in Output of show sysinfo Command (continued)

Field	Description
System Contact	Text used to identify a contact person for this switch. May be up to 31 alpha-numeric characters. The factory default is blank
System ObjectID	The base object ID for the switch's enterprise MIB
System Up Time	The time in days, hours and minutes since the last switch reboot
Current SNTP Synchronized Time	The current time reported by the SNTP server, if configured.
	A list of MIBs supported by SFTOS on this switch

show tech-support

This command displays the output of the commands `show eventlog`, `show logging`, `show memory`, `show port all`, `show process cpu`, `show running-config`, and `show version`. The output for each is separated by a header, as exemplified here:

```
----- show version -----
```

[The output fields are displayed in “[Fields in Output of show version Command](#)” on page 69.]

```
-----show logging -----
```

[The output fields are displayed in [show logging on page 174](#).]

Syntax `show tech-support [non-paged]`

When the command is entered without the optional `non-paged` keyword, the result is a multi-page presentation based upon the setting entered in the `terminal length` command. When the `non-paged` keyword is used, the report is displayed without interruption.

Mode Privileged Exec

Command History

Version 2.5.1	Modified: Output now also includes output of the <code>show process cpu</code> and <code>show memory</code> . The <code>non-paged</code> keyword option is added.
---------------	---

Related Commands

show logging eventlog	Event log (persistent log, error log) for the switch
show logging	Trap log maintained by the switch, and event log, containing error messages from the system
show memory	Total switch memory usage, in bytes, in tabular format.
show port	Port information
show process cpu	Current memory usage of applications in switch
show running-config	Updated configuration maintained by the switch.
show version	Details of the software/hardware present on the system

show version

This command displays version details of the software/hardware present on the system, which would be used for trouble-shooting. This command provides the details shown with the `show hardware` and `show sysinfo` commands, along with interface information, the u-boot version number, and the system image file version.

Syntax show version

Mode Privileged Exec

Example **Figure 5-22. Using the show version Command**

```
(Forcel0) #show version
Switch: 1

System Description..... Force10-S50 48GE 2TENGIG L3
                          Stackable switch
Vendor ID..... 07
Plant ID..... 01
Country Code..... 04
Date Code..... 102005
Serial Number..... DE4541040
Part Number..... 759-00001-00
Revision..... 0A
Catalog Number..... SA-01-GE-48T
Burned In MAC Address..... 0001.E8D5.BBDC
Software Version..... 2.5.1

Additional Packages..... Force10 Multicast
                          Force10 Stacking
                          Force10 Routing

10/100 Ethernet/802.3 interface(s)..... 0
Gig Ethernet/802.3 interface(s)..... 0
10Gig Ethernet/802.3 interface(s)..... 0
Virtual Ethernet/802.3 interface(s)..... 0
System Name.....

System Location.....
System Contact.....
System Object ID..... force10
System Up Time..... 0 days 0 hrs 26 mins 47 secs
```

Table 5-12. Fields in Output of show version Command

Headings	Explanation
Switch Description	Text used to identify the product name of this switch
Vendor ID	Number used to identify the manufacturer of the device
Plant ID	
Country Code	
Date Code	Month and year of manufacture of the device
Serial Number	The unique box serial number for this switch
Part Number	Manufacturing part number
Revision	
Catalog Number	
Burned in MAC Address	Universally assigned network address

Table 5-12. Fields in Output of show version Command (continued)

Headings	Explanation
Software Version	The release.version.revision number of the code currently running on the switch
Additional Packages	This displays the additional packages that are incorporated into this system, such as Dell Force10 Multicast.
10/100 Ethernet/802.3 interface(s)	Copper ports running at 10/100 speed reporting link UP
Gig Ethernet/802.3 interface(s)	Copper/fiber ports running at 1Gb speed reporting link UP
10Gig Ethernet/802.3 interface(s)	10Gb optional module
Virtual Ethernet/802.3 interface(s)	Layer 3 VLAN interfaces
System Name	
System Location	
System Contact	
System Object ID	
System Up Time	

Related Commands

show hardware	Inventory information for the switch
show sysinfo	Switch information, including list of supported MIBs
show tech-support	Displays the output of many show commands, including this one.

vlan participation (management VLAN only)

This command assigns the management VLAN of the switch.

Syntax [no] vlan participation *vlan_id*

The value for *vlan_id* is the VLAN that you want to use for the management interface (By default, VLAN 1 is used.)

Mode Interface ManagementEthernet. Uses the (Config-if-ma)# prompt, accessed by [interface managementethernet](#).

Default VLAN 1 (default management VLAN; all enabled ports are on VLAN 1 by default, so all ports are capable, by default, of being management ports.)

Command History

Version 2.3	Introduced: Replaces the command network mgmt_vlan on page 131 .
-------------	--

Related Commands

management route default	Sets the IP gateway of the switch.
interface managementethernet	Invokes the Interface ManagementEthernet mode, the (Config-if-ma)# prompt.

ip address (routed)	Configures an IP address on a routed interface.
show interface	Displays a summary of statistics for a specific port, including the management port, or a count of all CPU traffic based upon the argument.

Telnet Commands

This section describes the following SFTOS Telnet commands:

- [ip telnet maxsessions on page 71](#)
- [ip telnet timeout on page 71](#)
- [session-limit on page 72](#)
- [session-timeout on page 72](#)
- [show telnet on page 73](#)
- [telnet on page 73](#)
- [telnetcon maxsessions on page 73](#)
- [telnetcon timeout on page 73](#)

ip telnet maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established.

Syntax `ip telnet maxsessions 0-5`

A value of 0 indicates that no Telnet connection can be established. The range is 0 to 5.

The command `no telnet maxsessions` sets the maximum number of Telnet connection sessions that can be established to the default value.

Default 5

Mode Global Config

Command History

Version 2.3	Changed from <code>telnetcon maxsessions</code> and moved from Privileged Exec mode to Global Config.
-------------	---

ip telnet timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set.



Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Syntax `ip telnet timeout 1-160`

The time is a decimal value from 1 to 160.

The `no ip telnet timeout` command sets the Telnet connection session timeout value, in minutes, to the default.

Default 5 (minutes)

Mode Global Config

Command History

Version 2.3	Changed from <code>telnetcon timeout</code> and moved from Privileged Exec mode to Global Config.
-------------	---

ip telnet server enable

Enable or disable Telnet services.

Syntax `[no] telnet server enable`

Mode Global Config

Command History

Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.
-------------	--

Related Commands

ip ssh server enable	Enable/disable SSH services.
--------------------------------------	------------------------------

session-limit

This command specifies the maximum number of simultaneous outbound telnet sessions. A value of 0 indicates that no outbound telnet session can be established.

Syntax `session-limit 0-5`

Use `no session-limit` to set the maximum number of simultaneous outbound telnet sessions to the default value.

Default 5

Mode Line Config

session-timeout

This command sets the outbound Telnet session timeout value.

Syntax `[no] session-timeout 1-160`

The timeout value unit of time is minutes.

The `no` version of this command sets the outbound Telnet session timeout value to the default.

Default	1 (minute)
Mode	Line Config

show telnet

This command displays the current outbound telnet settings.

Syntax show telnet

Modes Privileged Exec and User Exec

Outbound Telnet Login Timeout (in minutes)—Indicates the number of minutes an outbound telnet session is allowed to remain inactive before being logged off. A value of 0, which is the default, results in no timeout.

Maximum Number of Outbound Telnet Sessions—Indicates the number of simultaneous outbound telnet connections allowed.

Allow New Outbound Telnet Sessions—Indicates whether outbound telnet sessions will be allowed.

telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If *[debug]* is used, the current telnet options enabled is displayed. The optional *line* parameter sets the outbound telnet operational mode as ‘linemode’, where by default, the operational mode is ‘character mode’. The *noecho* option disables local echo.

Syntax telnet *host* [*port*] [*debug*] [*line*] [*noecho*]

Modes Privileged Exec and User Exec

telnetcon timeout

Command History	Version 2.3	Modified: Changed to ip telnet timeout .
	<hr/>	

telnetcon maxsessions

Command History	Version 2.3	Modified: Changed to ip telnet maxsessions
	<hr/>	

remotecon maxsessions

This command specifies the maximum number of remote connection sessions that can be established. A value of 0 indicates that no remote connection can be established. The range is 0 to 5.

The **oe** version of this command sets the maximum number of remote connection sessions that can be established to the default value.

Default	5
Syntax	remotecon maxsessions <i>0-5</i> no remotecon maxsessions
Mode	Privileged EXEC

remotecon timeout

This command sets the remote connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. A value of 0 indicates that a session remains active indefinitely. The time is a decimal value from 0 to 160.

The **no** version of this command sets the remote connection session timeout value, in minutes, to the default.



Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Default	5
Syntax	remotecon timeout <i>0-160</i> no remotecon timeout
Mode	Privileged EXEC

Serial Commands

This section describes the following SFTOS system management commands pertaining to console port connections (serial connections, EIA-232):

- [lineconfig on page 75](#)
- [serial baudrate on page 75](#)
- [serial timeout on page 76](#)
- [show serial on page 76](#)

lineconfig

This command accesses the Line Config mode from the Global Config mode.

Syntax	lineconfig
Mode	Global Config
Usage Information	Users executing this command enter the Line Config mode.

For details on modes, see [Chapter 4, “Using the Command Line Interface,” on page 23](#).

Example **Figure 5-23. lineconfig Command Example**

```
(S50) #configure
(S50) (Config)#lineconfig
(S50) (Line)#
```

Related Commands	configure	Accesses the Global Config mode, which is the mode in which you can execute this lineconfig command.
-------------------------	---------------------------	---

serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Syntax	serial baudrate {1200 2400 4800 9600 19200 38400 57600 115200}
	The no serial baudrate command sets the communication rate of the terminal interface to the 9600 default.
Default	9600
Mode	Line Config

serial timeout

This command specifies the maximum connect time (in minutes) without console activity.

Syntax serial timeout *0-160*

A value of 0 means no console timeout. The range is 0 to 160 minutes.

The `no serial timeout` command sets the maximum connect time (in minutes) without console activity to the 5-minute default.

Default 5

Mode Line Config

show serial

This command displays serial communication settings for the switch.

Syntax show serial

Mode Privileged Exec and User Exec

Example **Figure 5-24. Sample Output of show serial Command**

```
(Force10 S50) #show serial
Serial Port Login Timeout (minutes)..... 20
Baud Rate (bps)..... 9600
Character Size (bits)..... 8
Flow Control..... Disable
Stop Bits..... 1
Parity..... none
```

Table 5-13. Fields of show serial Command Output

Field	Description
Serial Port Login Timeout (minutes)	Specifies the time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout
Baud Rate	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud (bps). The factory default is 9600
Character Size	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether hardware flow control is enabled or disabled. It is always disabled.

Table 5-13. Fields of show serial Command Output (continued)

Field	Description
Stop Bits	The number of stop bits per character. The number of stop bits is always 1.
Parity	The parity method used on the serial port. The parity method is always None.

SNMP Management Commands

This section describes the SNMP system management commands supported by SFTOS:

- [show snmpcommunity on page 78](#)
- [show snmptrap on page 78](#)
- [show trapflags on page 79](#)
- [snmp-server on page 79](#)
- [snmp-server community on page 80](#)
- [snmp-server community ipaddr on page 80](#)
- [snmp-server community ipmask on page 80](#)
- [snmp-server community mode on page 81](#)
- [snmp-server community ro on page 81](#)
- [snmp-server community rw on page 81](#)
- [snmp-server enable traps bcaststorm on page 81](#)
- [snmp-server enable traps linkmode on page 82](#)
- [snmp-server enable traps multiusers on page 82](#)
- [snmp-server enable traps stpmode on page 82](#)
- [snmp-server enable trap violation on page 83](#)
- [snmp-server traps enable on page 83](#)
- [snmptrap on page 83](#)
- [snmptrap ipaddr on page 84](#)
- [snmptrap mode on page 84](#)
- [snmp trap link-status \(interface\) on page 84](#)
- [snmp trap link-status all on page 85](#)
- [snmptrap snmpversion on page 85](#)



Note: The Layer 3 Routing Package of SFTOS also contains these SNMP traps:

In Global Config mode:

- `[no] ip dvmrp trapflags`: Sets the DVMRP (Distance Vector Multicast Routing Protocol) traps flag (disabled by default). See the Multicast chapter.
- `[no] ip pim-trapflags`: Sets the PIM traps flag (disabled by default). See the PIM chapter.

In Router OSPF Config mode:

- `[no] trapflags`: Sets the OSPF traps flag. See the OSPF chapter (enabled by default).

For information on configuring SNMP, see the Management chapter in the *SFTOS Configuration Guide*.

show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Version 1 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Syntax show snmpcommunity

Mode Privileged Exec

Table 5-14. Fields of show snmpcommunity Command Output

Field	Description
SNMP Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
Client IP Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address. Note: that if the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
Client IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string
Status	The status of this community access entry

show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Syntax show snmptrap

Mode Privileged Exec

Table 5-15. Fields of show snmptrap Command Report

Field	Description
SNMP Trap Name	The community string of the SNMP trap packet sent to the trap manager. This may be up to 16 alphanumeric characters. This string is case sensitive.
IP Address	The IP address to receive SNMP traps from this device. Enter four numbers between 0 and 255 separated by periods.
Status	Indicates the receiver's status (enabled or disabled)

show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold start traps are always generated and cannot be disabled.

 **Note:** The DVMRP, OSPF, and PIM traps are not supported in the L2 image.

Syntax show trapflags

Mode Privileged Exec

Table 5-16. Fields of show trapflags Command Report

Field	Description
Authentication Flag	May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	May be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either via telnet or serial port).
Spanning Tree Flag	May be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps will be sent.
DVMRP Traps	May be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps will be sent.
OSPF Traps	May be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps will be sent.
PIM Traps	May be enabled or disabled. The factory default is disabled. Indicates whether PIM traps will be sent.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for name, location, and contact is from 1 to 31 alphanumeric characters.

Syntax snmp-server {sysname *name* | location *loc* | contact *con*}

Default None

Mode Global Config

snmp-server community

This command adds (and names) a new SNMP community. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of name can be up to 16 case-sensitive characters.



Note: Community names in the SNMP community table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Syntax snmp-server community *name*

The no snmp-server community *name* command removes the specified community name from the SNMP community table.

Default None

Mode Global Config

snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet-sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Syntax snmp-server community ipaddr *ipaddr name*

Use no snmp-server community ipaddr *name* to reset a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Default 0.0.0.0

Mode Global Config

snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP Address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Syntax snmp-server community ipmask *ipmask name*

Use no snmp-server community ipmask *name* to reset a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Default 0.0.0.0
Mode Global Config

snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case, the SNMP manager associated with this community cannot manage the switch until the status is changed back to Enable. The **no** version of this command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Syntax [no] snmp-server community mode *name*
Default Enable
Mode Global Config

snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Syntax snmp-server community ro *name*
Mode Global Config

snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Syntax snmp-server community rw *name*
Mode Global Config


snmp-server enable traps bcstorm

This command enables sending Broadcast Storm traps.

Syntax [no] snmp-server enable traps bcstorm

The **no** version of this command disables the sending of Broadcast Storm traps.

Default enabled

Mode	Global Config
Command History	Version 2.3 Introduced
	Note: The CLI indicates successful execution of this command, and the show trapflags report shows successful execution of the command, but this trap is not currently supported.

snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see ‘snmp trap link-status’ command).

Syntax [no] snmp-server enable traps linkmode

The no version of this command disables Link Up/Down traps for the entire switch.

Default enabled

Mode Global Config

snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or telnet) and there is an existing terminal interface session.

Syntax [no] snmp-server enable traps multiusers

The no version of this command disables Multiple User traps.

Default enabled

Mode Global Config

snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Syntax [no] snmp-server enable traps stpmode

The no version of this command disables the sending of new root traps and topology change notification traps.

Default enabled

Mode Global Config

snmp-server enable trap violation

This command enables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Syntax [no] snmp-server enable trap violation

The **no** version of this command disables the sending of new violation traps.

Default Disabled

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.1	Added Interface Port Channel Config mode
---------------	--

Version 2.3	Added Interface Range mode.
-------------	-----------------------------

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

interface	Identifies an interface and enters the Interface Config mode.
---------------------------	---

snmp-server traps enable

This command enables the Authentication traps.

Syntax [no] snmp-server traps enable

The **no** version of this command disables the Authentication traps.

Default enabled

Mode Global Config

Command History

Version 2.3	Corrected from snmp-server enable traps
-------------	--

snmptrap

This command adds an SNMP trap receiver name and trap receiver IP address. The maximum name length is 16 case-sensitive alphanumeric characters.

Syntax [no] snmptrap *name ipaddr*

The **no** version of this command deletes the specified trap receiver from the community.

Default The default name for the six undefined community names is Delete.

Mode Global Config

snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum name length is 16 case-sensitive alphanumeric characters.



Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Syntax `snmptrap ipaddr name ipaddroid ipaddrnew`

Mode Global Config

snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Syntax `[no] snmptrap mode name ipaddr`

The `no` version of this command deactivates an SNMP trap. Disabled trap receivers are inactive (not able to receive traps).

Mode Global Config

snmp trap link-status (interface)

This command enables link status traps by interface.

Syntax `[no] snmp trap link-status`

The `no` version of this command disables link status traps by interface.



Note: This command is valid only when the Link Up/Down Flag is enabled. See [no, d6nEsbEsuEo rgEuCs dnugaORnd](#).

Mode Interface Config (including Interface Loopback Config); Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.1	Added Interface Loopback Config mode.
Version 2.3	Added Interface Range mode.

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface	Identifies an interface and enters the Interface Config mode.
snmp trap link-status (port channel)	enables link status traps for the selected port channel

snmp trap link-status all

This command enables link status traps for all interfaces.

Syntax [no] snmp trap link-status all

The **no** version of this command disables link status traps for all interfaces.



Note: This command is valid only when the Link Up/Down Flag is enabled. See `snmp-server enable traps linkmode`.

Mode Global Config

snmptrap snmpversion

This command selects between SNMP version 1 and version 2 traps to be sent for the selected SNMP trap name.

Syntax snmptrap snmpversion *name ipaddr* {snmpv1|snmpv2}

Mode Global Config

System Configuration Commands

This chapter provides a detailed explanation of the system configuration commands in the following major sections:

- [System Configuration Commands on page 87](#)
- [System Utility Commands on page 105](#)
- [PoE Commands on page 114](#)
- [Dual Image Management Commands on page 119](#)
- [Configuration Scripting on page 122](#)

**Note:**

See also [Chapter 5, “System Management Commands,” on page 35](#) and [Chapter 9, “System Logs,” on page 169](#).

For VLAN commands, see the chapter [LAG/Port Channel Commands on page 287](#).

For port channel (LAG) commands, see the chapter [LAG/Port Channel Commands on page 287](#).

For port security commands, also known as port MAC locking, see the section [Port Security Commands on page 183](#) in the chapter [Security Commands on page 183](#)

System Configuration Commands

This section describes the following system configuration commands:

- [auto-negotiate on page 88](#)
- [auto-negotiate all on page 89](#)
- [bridge aging-time on page 89](#)
- [configure on page 90](#)
- [enable on page 90](#)
- [interface on page 91](#)
- [interface range on page 91](#)
- [interface loopback on page 95](#)
- [monitor session on page 95](#)
- [monitor session 1 mode on page 96](#)
- [mtu \(port\) on page 97](#)
- [no monitor on page 97](#)
- [no monitor session 1 on page 98](#)

- [rate-interval on page 98](#)
- [show forwardingdb agetime on page 98](#)
- [show interface loopback on page 99](#)
- [show mac-address-table on page 99](#)
- [show mac-address-table multicast on page 100](#)
- [show mac-address-table stats on page 100](#)
- [show monitor session on page 101](#)
- [show port on page 101](#)
- [show port protocol on page 103](#)
- [shutdown \(port\) on page 103](#)
- [shutdown all \(port\) on page 103](#)
- [speed on page 104](#)
- [speed all on page 104](#)



Note: Broadcast storm control commands are in the ACL chapter, in the section [Broadcast Storm Control Commands on page 389](#).

Interface routing commands are in the section [IP Routing on page 397 in Chapter 22, Routing Commands](#).

MAC Database Commands

Among the commands in this section are the following four commands that you use to configure and view information about the MAC address database:

- [bridge aging-time on page 89](#)
- [show forwardingdb agetime on page 98](#)
- [show mac-address-table multicast on page 100](#)
- [show mac-address-table stats on page 100](#)

cablestatus

This command tests the status of the cable attached to an interface.

Syntax `show cablestatus [slot/port]`

Mode Privileged EXEC

auto-negotiate

This command enables automatic speed negotiation on a port.



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

Syntax `speed [enable|disable]`

The default value is enable.

The **no** version of this command disables automatic speed negotiation on a port.

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	speed	Manually set the port speed.

auto-negotiate all

This command enables automatic speed negotiation on all ports. The default value is enable.

The **no** version of this command disables automatic speed negotiation on all ports.

Syntax	[no] auto-negotiate all	
Mode	Global Config	
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	speed all	Manually set the same port speed for all ports.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Syntax	bridge aging-time <i>seconds</i>	
	The command no bridge aging-time sets the forwarding database address aging timeout to the default of 300 seconds. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.	
Parameters	<i>seconds</i>	In place of <i>seconds</i> , enter a number between 10 and 1,000,000 to indicate the number of seconds before the timeout.
Default	300	
Mode	Global Config In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.	
Command History	Version 2.3	Modified: Removed parameters and statements relating to IVL.

configure

This command enables the user to enter the Global Config mode from the Privileged Exec mode.

Syntax configure

Command Modes Privileged Exec

Usage Information Users executing this command enter the Global Config mode, which provides access to many commands within that mode. Also, this mode is a gateway to all other more protocol-specific modes except the VLAN mode.

For details on modes, see [Chapter 4, “Using the Command Line Interface,”](#) on page 23.

Example **Figure 6-25. configure Command Example**

```
(S50) #configure
(S50) (Config)#
```

Related Commands

[enable](#) The enable command accesses the Privileged Exec mode.

enable

This command accesses the Privileged Exec mode from the User Exec mode. If the enable password is set, you must enter the password to gain access to the Privileged Exec mode.



Note: In a stack, only the management unit (stack manager) provides access to CLI commands. Other member units display the prompt “(Unit [unit number])”.

Syntax enable

Defaults none

Mode User Exec

Usage Information Users who execute this command enter the Privileged Exec mode, gaining access to the commands available in this mode, as well as being able to directly access the Global Config mode and the VLAN mode. After accessing the Global Config mode, users can access all modes to which the Global Config mode provides a gateway.

To protect against unauthorized access, use the command [enable passwd](#) to configure a password for the command.

Example **Figure 6-26. enable Command Example**

```
(S50)>enable
Password:
(S50)#
```

Related Commands

[enable passwd](#) Configure a password for the enable command.

[configure](#) Use this command to access the Global Config mode from the Exec Privilege mode.

interface

This command accesses the Interface Config mode for a designated logical or physical interface. The Interface Config mode provides access to configuration commands for the specified interface.

Syntax `interface unit/slot/port`

The *unit/slot/port* is a valid physical or logical port number. Physical ports are numbered #/0/1 through #/0/50. In contrast, logical port numbers contain a number in the slot position and are defined by the system. The number in the slot position is a 1 when you create a LAG (port channel).

The `no` version of this command deletes the selected logical port.

Default None

Mode Global Config

Related Commands

interface range	Groups a set of individual interfaces, a range of interfaces, or more than one range of interfaces, to which subsequent configuration commands can be applied (bulk configuration)
ip address (VLAN)	Assigns an IP address and subnet mask to the selected VLAN to support Layer 3 routing.
interface vlan	Creates a new VLAN, or selects one based on ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
routing	Enables routing for the selected interface
show ip interface	Displays summary information about IP configuration settings for all ports in the router

interface range

This command groups a set of individual interfaces, a range of interfaces, or more than one range of interfaces, to which subsequent configuration commands can be applied (bulk configuration).

Syntax `interface range {ethernet range,range,... | port-channel range,range,... | vlan range,range,...}`

Parameters

<code>ethernet <i>range,range,...</i></code>	Enter the keyword <code>ethernet</code> and one or more ports separated by hyphens and commas in this form: <code><i>unit/slot/port-unit/slot/port,unit/slot/port-unit/slot/port</i></code> Spaces are not allowed around commas or hyphens. You can enter up to six comma-separated ranges. Example: <code>ethernet 1/0/1-1/0/10,1/0/40-1/0/45</code>
--	--

<code>port-channel range,range,...</code>	Enter the keyword <code>port-channel</code> and one or more port channel IDs separated by commas or grouped in a range, as above: For example: port-channel 3-5 (In this example, you previously assigned IDs 3, 4, and 5 to three port channels.)
<code>vlan range,range,...</code>	Enter the keyword <code>vlan</code> and one or more VLAN numbers, from 1 to 3965, separated by commas or grouped in a range in this form: vlan 10,33-50 As above, spaces are not allowed around commas or hyphens, and you can enter up to six comma-separated ranges.

Defaults This command has no default behavior or values.

Mode Global Config

Command History

Version 2.3	Introduced
-------------	------------

Usage Information

The `interface range` command invokes the Interface Range mode, more specifically, one of three versions of it—Ethernet Range, Port Channel Range, or VLAN Range. Here, you can execute commands that modify the selected interface or set of interfaces. These commands have the same effect as they do when they are used within the Interface VLAN or Interface Config modes (see [interface](#) on page 91 and [interface vlan](#) on page 129).

Important things to remember:

- You can only modify, not create, interfaces (ethernet ports, LAGs, and VLANs) using the `interface range` command.
- A range command can include only one type of interface—VLAN, physical, or LAG. You can use the `show running-config` command to note VLAN and LAG (port channel) interfaces that are available to be used with the `interface range` command.
- Bulk configuration is created if at least one interface is valid, automatically excluding non-existing interfaces from the bulk configuration and generating a warning message.
- 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).
- The resulting interface range prompt includes interface types with slot/port information for valid interfaces, for example: `(conf-if-range-et-1/0/10-1/0/11)#`. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- If 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.

The VLAN Range mode commands appear in [Figure 6-27](#).

Figure 6-27. Commands Available in VLAN Range Mode

```
(s50-1) (conf-if-range-vl-10,20)#?  
encapsulation      Configure interface link layer encapsulation type.  
exit               To exit from the mode.  
igmp               Configure IGMP Snooping parameters for the Vlan  
ip                 Configure IP parameters.  
makestatic         Change the VLAN type from 'Dynamic' to 'Static'.  
mtu                Sets the default MTU size.  
name               Configure an optional VLAN Name.  
protocol           Configure the Protocols associated with particular  
                   Group Ids.  
shutdown           Enable/Disable a port.  
tagged             Configure tagging for a specific VLAN port.
```

The Port Channel Range mode commands (LAG commands) appear in [Figure 6-28](#).

Figure 6-28. Commands Available in Port Channel Range Mode

```
(s50-1)(Config)#interface range port-channel 1,3  
(s50-1)(conf-if-range-po-1,3)#?  
classofservice     Configure Class of Service parameters.  
cos-queue          Configure the Cos Queue Parameters.  
description        Add Description to the interface  
dot1p-priority     Configure the priority for untagged frames.  
exit               To exit from the mode.  
gmrp               Set GARP Multicast Registration Protocol parameters.  
gvrp               Set GARP VLAN Registration Protocol parameters.  
igmp               Enable/Disable IGMP Snooping on a selected interface  
ip                 Configure IP parameters.  
mac                Configure MAC Access List group parameters.  
mode               Configure the double VLAN tunnel mode for this  
                   interface.  
mtu                Sets the default MTU size.  
port-security      Enable/Disable Port MAC Locking/Security for  
                   interface.  
protocol           Configure protocol type for port-channel.  
rate-interval      Sets the traffic monitoring rate interval  
service-policy     Configure DiffServ Service.  
set                Configure switch options and settings.  
shutdown           Enable/Disable a port.  
snmp               Configure SNMP options.  
snmp-server        Enable/Disable SNMP violation traps interface.  
spanning-tree      Set the spanning tree operational mode.  
vlan               Configure VLAN parameters.
```

The command families available from the Ethernet Range prompt (for configuring all physical ports) are displayed in [Figure 6-29](#).

Figure 6-29. Commands Available in Interface Range Mode

```
(s50-1) (conf-if-range-et-1/0/10-1/0/22)#?
addport          Add this port to a port-channel.
auto-negotiate   Enables/Disables automatic negotiation on a port.
classofservice   Configure Class of Service parameters.
cos-queue        Configure the Cos Queue Parameters.
deleteport       Delete this port from a port-channel.
description      Add Description to the interface
dot1x            Configure Dot1x interface commands.
exit             To exit from the mode.
gmrp             Set GARP Multicast Registration Protocol parameters.
gvrp             Set GARP VLAN Registration Protocol parameters.
igmpp            Enable/Disable IGMP Snooping on a selected interface
ip              Configure IP parameters.
mac             Configure MAC Access List group parameters.
mode            Configure the double VLAN tunnel mode for this interface.
mtu             Sets the default MTU size.
port            Configure a physical port.
port-channel     Enable/Disable the port-channel's administrative mode.
port-security    Enable/Disable Port MAC Locking/Security for interface.
protocol        Configure the Protocol Based VLAN parameters.
service-policy   Configure DiffServ Service.
set             Configure switch options and settings.
shutdown        Enable/Disable a port.
snmp            Configure SNMP options.
snmp-server     Enable/Disable SNMP violation traps interface.
spanning-tree   Set the spanning tree operational mode.
speed           Sets the speed and duplex setting for the interface.
traffic-shape    Configure the maximum transmission bandwidth limit.
vlan            Configure VLAN parameters.

(s50-1) (conf-if-range-et-1/0/10-1/0/22)#ip ?
access-group    Add Access List to the Group.
address         Create an IP Address and subnet for an interface.
dvmrp          Configure DVMRP parameters.
igmp           Configure IGMP parameters.
igmp-proxy     Configure IGMP Proxy parameters.
irdp           Enables Router Discovery on an interface. Use no
               command to disable.
multicast       Configure multicast routing parameters.
netdirbcast    Enables net directed broadcasts. Use no command to
               disable.
ospf           Configure Open Shortest Path First parameters.
pimdm          Configure PIM-DM parameters.
pimsm          Configure PIM-SM parameters.
proxy-arp      Enables or disables Proxy ARP on an interface.
rip            Configure Router Interface Protocol settings in the
               router.
vrrp           Configure Virtual Router Redundancy Protocol
               parameters.

(s50-1) (conf-if-range-et-1/0/10-1/0/21)#mode ?
dvlan-tunnel   Configure double VLAN tunneling for a specific port.
dot1q-tunnel   Configure double VLAN tunneling for a specific port.

(s50-1) (conf-if-range-et-1/0/10-1/0/21)#vlan ?
priority       Configure the priority for untagged frames.
```

Figure 6-30. Multiple Ranges Selected for Configuration for Physical Ports

```
Forcel0(config)#interface range ethernet 5/0/1-5/0/23,1/0/49-1/0/50,2/0/10-2/0/12
Forcel0(config-if-range)#no shutdown
Forcel0(config-if-range)#
```

Note in [Figure 6-30](#) that port ranges in separate stack members have been selected.

For more on VLAN commands, see [VLAN Commands on page 125](#).

For more on LAG commands, see [LAG/Port Channel Commands on page 287](#).

For more on bulk configuration, see the Bulk Configuration section in the Interfaces chapter of the *SFTOS Configuration Guide*.

Related Commands

interface	Accesses the Interface Config mode for a designated logical or physical interface.
ip address (VLAN)	Assigns an IP address and subnet mask to the selected VLAN to support Layer 3 routing.
interface vlan	Creates a new VLAN and accesses the Interface VLAN mode for it, or selects an existing VLAN and accesses the Interface VLAN mode for it.
tagged	Adds ports or port channels to the selected VLAN as tagged interfaces.

interface loopback

Configure a loopback interface, and access Interface Loopback Config mode (the prompt is (Interface loopback 0)#).

Syntax interface loopback 0

Use `no interface loopback 0` to remove the interface.

Modes Global Config

Command History

Version 2.5.1	Introduced
---------------	------------

Usage A loopback interface is a virtual interface in which the software emulates an interface. Basically, the loopback interface is a handle controlling access to the CPU interface.

The prompt provides access to IP commands — `ip access-group`, `ip address`, and `ip ospf` — along with `port enable/disable (shutdown)` and `SNMP` commands. This command in combination with an ACL rule, often called a management VTY ACL, protects access to switch management. For more, see “Applying an ACL to Loopback” in the QoS chapter of the *SFTOS Configuration Guide*.

Related Commands

access-list	Creates an IP access control list
ip access-group (Interface)	Attaches a specified access control list to an interface
ip address (routed)	Configures an IP address on a routed interface
ip ospf	Enables OSPF on a router interface
show interface loopback	Displays the configured loopback interface.
snmp trap link-status (interface)	Enables link status traps by interface

monitor session

This command adds a mirrored port (source port) or probe port (destination port) to a session identified with the session ID of 1. In all released versions of SFTOS, the session is always 1.

Syntax [no] monitor session 1 {destination interface *unit/slot/port* | source interface *unit/slot/port* | mode}

Parameters	destination interface <i>unit/slot/port</i>	Specify the probe port (target port). The probe port cannot be a VLAN member.
	source interface <i>unit/slot/port</i>	Specify the source interface (mirrored port). The port can be a part of any VLAN.
	mode	Enable/disable the port mirroring session. See monitor session 1 mode on page 96 .
	To remove the destination port, use no monitor session 1 destination interface .	
	To remove a source port, use no monitor session 1 source interface <i>unit/slot/port</i> .	
	In other words, removing the source interface requires specifying the port to be removed, but removing the destination port does not require specifying the destination port, since there can be only one destination port.	
Default	None	
Mode	Global Config	
Usage Information	In an S-Series stack, destination and source ports can be on separate stack members. A stack has a limit of one port mirroring session and one destination port. Remove an existing source or destination port before replacing it with another. For more on configuring port monitoring (port mirroring), see the Port Mirroring chapter of the <i>SFTOS Configuration Guide</i> .	
Related Commands	monitor session 1 mode	Sets the monitor session (port monitoring) mode to enabled.
	mtu (port)	Removes the destination port and all source ports from the mirroring configuration.
	show monitor session	Shows the mirroring configuration.

monitor session 1 mode

This command sets the monitor session (port monitoring) mode to enabled. The probe and monitored ports must be configured before port monitoring can be enabled. When enabled, the probe port monitors all traffic received and transmitted on the physical monitored port. It is not necessary to disable port monitoring before modifying the probe and monitored ports.

A session is operationally active if and only if both a destination port and at least one source port is configured. If neither is true, the session is inactive.

A port configured as a destination port acts as a mirroring port when the session is operationally active. If it is not, the port acts as a normal port and participates in all normal operation with respect to transmitting traffic.

Syntax [no] monitor session 1 mode

The **no** version of this command sets the monitor session (port monitoring) mode to disabled.

Default disabled

Mode Global Config

Related Commands	monitor session	Adds a mirrored port (source port) or mirroring port (destination port) to a session identified with the session ID of 1.
	mtu (port)	Removes the destination port and all source ports from the mirroring configuration.
	show monitor session	Shows the mirroring configuration.

mtu (port)

This command sets the maximum transmission unit (MTU) size (in bytes) for the selected port.

Syntax [no] mtu 1518-9216

For the standard implementation, the range is a valid integer between 1518–9216.

Enter `no mtu` to set the MTU for the interface to the default.

Default 1518

Note: The hardware on the 1-Gigabit ports automatically compensates for the tags on tagged packets. For a 1-Gigabit port, the default setting of 1518 allows 1518-byte untagged and 1522-byte tagged packets. Likewise, set to the maximum, a setting of 9216 will allow for tagged packets up to 9220 bytes.

The 10-Gigabit ports do not automatically allow for the length of a tag. For 10-Gigabit ports, the default setting of 1518 means 1518 untagged or tagged. The maximum is 9216 bytes.

Mode Interface Config

Related Commands	mtu (LAG)	Sets the MTU for a selected port channel
	ip mtu	Sets the MTU on a routing interface (Interface Config or VLAN mode)
	mtu (VLAN)	Sets the MTU for a selected VLAN (VLAN mode)

no monitor

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

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

Default enabled

Syntax no monitor

Mode Global Config

no monitor session 1

This command removes all the source ports and a destination port of the mirroring session and restore the default value for mirroring session mode.

The 1 or *session-id* parameter is an integer value used to identify the session. In the current version of the software, the *session-id* parameter is always 1.

This is a stand-alone “no” command. This command does not have a “normal” form. This command can be issued without regard for the session status (enabled or disabled).

Syntax	no monitor session 1
Default	enabled
Mode	Global Config

rate-interval

This command sets the traffic monitoring rate interval in seconds.

Syntax	rate-interval 15-300
Default	299 seconds
Mode	Interface Config; Interface Port Channel Config; Interface Range Ethernet; Interface Range Port Channel

Command History	Version 2.5.1	Introduced
------------------------	---------------	------------

show forwardingdb agetime

This command displays the timeout for address aging. In an SVL system, the [fdbid | all] parameter is not used and will be ignored if entered.

Syntax	show forwardingdb agetime
Mode	Privileged Exec

Example **Figure 6-31. Example of show forwardingdb agetime Command Output**

```
Force10 #show forwardingdb agetime
Address Aging Timeout:300
Force10#
```

Command History	Version 2.3	Modified: Removed parameters and statements relating to IVL.
------------------------	-------------	--

show interface loopback

Display loopback interface configuration.

Syntax	show interface loopback 0							
Modes	Privileged Exec; User Exec							
Command History	<hr/> <table><tr><td>Version 2.5.1</td><td>Introduced</td></tr></table> <hr/>		Version 2.5.1	Introduced				
Version 2.5.1	Introduced							
Related Commands	<hr/> <table><tr><td>access-list</td><td>Creates an IP access control list.</td></tr><tr><td>interface loopback</td><td>Configures loopback interface 0.</td></tr><tr><td>ip access-group (Interface)</td><td>Attaches a specified access control list to an interface.</td></tr></table> <hr/>		access-list	Creates an IP access control list.	interface loopback	Configures loopback interface 0.	ip access-group (Interface)	Attaches a specified access control list to an interface.
access-list	Creates an IP access control list.							
interface loopback	Configures loopback interface 0.							
ip access-group (Interface)	Attaches a specified access control list to an interface.							

show mac-address-table

This command displays the Multicast Forwarding Database (MFDB) statistics.

Syntax	show mac-address-table {gmrp igmpsnooping multicast stats}											
	gmrp—Display GMRP entries in the MFDB table.											
	igmpsnooping—Display IGMP Snooping entries in the MFDB table.											
	multicast—Display Multicast Forwarding Database Table information.											
	stats—Display MFDB statistics.											
Mode	Privileged Exec											
	The output field descriptions are:											
	Total Entries—This displays the total number of entries that can possibly be in the Multicast Forwarding Database table.											
	Most MFDB Entries Ever Used—This displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.											
	Current Entries—This displays the current number of entries in the Multicast Forwarding Database table.											
Related Commands	<hr/> <table><tr><td>show mac-address-table multicast</td><td>Displays Multicast Forwarding Database (MFDB) information</td></tr><tr><td>show mac-address-table stats</td><td>Displays Multicast Forwarding Database (MFDB) statistics</td></tr><tr><td>show mac-address-table gmrp</td><td>Displays GARP Multicast Registration Protocol (GMRP) entries in the MFDB table</td></tr><tr><td>show mac-address-table igmpsnooping</td><td>Displays IGMP Snooping entries in the MFDB table</td></tr><tr><td>show mac-addr-table</td><td>Displays forwarding database entries</td></tr></table> <hr/>		show mac-address-table multicast	Displays Multicast Forwarding Database (MFDB) information	show mac-address-table stats	Displays Multicast Forwarding Database (MFDB) statistics	show mac-address-table gmrp	Displays GARP Multicast Registration Protocol (GMRP) entries in the MFDB table	show mac-address-table igmpsnooping	Displays IGMP Snooping entries in the MFDB table	show mac-addr-table	Displays forwarding database entries
show mac-address-table multicast	Displays Multicast Forwarding Database (MFDB) information											
show mac-address-table stats	Displays Multicast Forwarding Database (MFDB) statistics											
show mac-address-table gmrp	Displays GARP Multicast Registration Protocol (GMRP) entries in the MFDB table											
show mac-address-table igmpsnooping	Displays IGMP Snooping entries in the MFDB table											
show mac-addr-table	Displays forwarding database entries											

show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional **all** parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Syntax show mac-address-table multicast { *macaddr* [1-3965] }

(OPTIONAL) For *macaddr*, enter a 6-byte MAC address.

(OPTIONAL) For 1-3965, enter a valid VLAN ID.

Mode Privileged Exec

Report Fields MAC Address—A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In a system, the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes.

Type—This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Component—The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.

Description—The text description of this multicast table entry

Interfaces—The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Forwarding Interfaces—The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

Related Commands

show mac-address-table	Displays Multicast Forwarding Database (MFDB) statistics
show mac-address-table stats	Displays Multicast Forwarding Database (MFDB) statistics

show mac-address-table stats

This command displays Multicast Forwarding Database (MFDB) statistics.

Syntax show mac-address-table stats

Mode Privileged Exec

Report Fields Max MFDB Table Entries — Displays the total number of entries that can possibly be in the Multicast Forwarding Database table.

Most MFDB Entries Ever Since Last Reset — Displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.

Current Entries — Displays the current number of entries in the MFDB.

Example **Figure 6-32. Command Example: show mac-address-table stats**

```
Force10 #show mac-address-table stats
Max MFDB Table Entries..... 256
Most MFDB Entries Since Last Reset..... 0
Current Entries..... 0
```

Related Commands	show mac-address-table multicast	Displays the Multicast Forwarding Database (MFDB) information
-------------------------	---	---

show monitor session

This command displays the port monitoring information for the system.

Syntax show monitor session 1

Mode Privileged Exec

Example **Figure 6-33. Command Example: show monitor session 1**

```
Force10 #show monitor session 1
Session ID   Admin Mode   Probe Port   Mirrored Port
-----
1            Enable       2/0/26       1/0/1
```

Report Fields Session ID—In all released versions of SFTOS, the session is always 1.

Admin Mode—Indicates whether the Port Mirroring feature is enabled or disabled. The possible values are Enable and Disable.

Probe Port *unit/slot/port*—The *unit/slot/port* configured as the probe port (destination port for mirroring). If this value has not been configured, 'Not Configured' will be displayed.

Mirrored Port *unit/slot/port*—The *unit/slot/port* configured as the monitored port (source port, mirrored port). If this value has not been configured, 'Not Configured' will be displayed.

Related Commands	monitor session	Adds a mirrored port (source port) or probe port (destination port) to a session identified with the session ID of 1.
	monitor session 1 mode	Sets the monitor session (port monitoring) mode to enabled.

show port

This command displays port information for a selected port or for all ports.

Syntax show port {*unit/slot/port* | all}

Mode Privileged Exec

Command History

Version 2.3 Modified: Revised to include VLAN interface IDs in the Interface column of the report.

Example

Figure 6-34. Command Example: show port

```
(Forcel0_S50) #show port 1/0/1
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode
1/0/1		Enable	Auto	100 Full	Up	Enable	Enable

```
(Forcel0_S50) #show port all
```

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode
1/0/1		Enable	Auto		Down	Enable	Enable
1/0/2		Enable	Auto	1000 Full	Up	Enable	Enable
1/0/3		Disable	Auto		Down	Enable	Enable
1/0/4		Disable	Auto		Down	Enable	Enable
1/0/5		Disable	Auto		Down	Enable	Enable
1/0/6		Disable	Auto		Down	Enable	Enable
1/0/7		Disable	Auto		Down	Enable	Enable
1/0/8		Disable	Auto		Down	Enable	Enable
1/0/9		Disable	Auto		Down	Enable	Enable
1/0/10		Disable	Auto		Down	Enable	Enable
1/0/11		Disable	Auto		Down	Enable	Enable
1/0/12		Disable	Auto		Down	Enable	Enable
1/0/13		Disable	Auto		Down	Enable	Enable
1/0/14		Disable	Auto		Down	Enable	Enable
1/0/15		Disable	Auto		Down	Enable	Enable
1/0/16		Disable	Auto		Down	Enable	Enable
1/0/17		Disable	Auto		Down	Enable	Enable
1/0/18		Disable	Auto		Down	Enable	Enable

```
--More-- or (q)uit
(Forcel0_S50) #
```

Report Fields

Intf—Valid unit, slot and port number separated by forward slashes. This field only displays for show port all.

Type—If not blank, this field indicates that this port is a special type of port. The possible values are:

Mon—This port is a monitoring port. Look at the Port Monitoring screens to find out more information.

Lag—This port is a member of a port-channel (LAG).

Probe—This port is a probe port.

Admin Mode—Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network—May be enabled or disabled. The factory default is enabled.

Physical Mode—Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.

Physical Status—Indicates the port speed and duplex mode.

Link Status—Indicates whether the Link is up or down.

Link Trap—This object determines whether or not to send a trap when link status changes. The factory default is enabled.

LACP Mode—Displays whether LACP is enabled or disabled on this port.

**Related
Commands**

show tech-support	Displays the output of many show commands, including this one.
-----------------------------------	---

show port protocol

This command displays the protocol-based VLAN information for either the entire system (use **all** keyword), or for the indicated group (specify the group with the value of *groupid*).

Syntax show port protocol {*groupid* | all}

Mode Privileged Exec

Report Fields Group Name—This field displays the group name of an entry in the protocol-based VLAN table.

Group ID—This field displays the group identifier of the protocol group.

Protocol(s)—This field indicates the type of protocol(s) for this group.

VLAN—This field indicates the VLAN associated with this protocol group.

Interface(s)—This field lists the *unit/slot/port* interface(s) that are associated with this protocol group.

shutdown (port)

This command enables or disables a port. The **no** version of this command enables a port.

Syntax [no] shutdown

Default disabled

Mode Interface Config (including Interface Loopback Config); Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

**Command
History**

Version 2.5.1	Added Interface Loopback Config mode
---------------	--------------------------------------

Version 2.3	Added Interface Range mode.
-------------	-----------------------------

**Related
Commands**

interface range	Define an interface range and access the Interface Range mode.
---------------------------------	--

interface	Identify an interface and enter the Interface Config mode.
---------------------------	--

shutdown all (port)	Enable or disable all ports.
-------------------------------------	------------------------------

shutdown (port channel)	Enable or disable the selected port channel.
---	--

shutdown all (port)

This command disables all ports.

The **no** version of this command enables all ports.

Syntax [no] shutdown all**Default** enabled**Mode** Global Config

speed

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

Syntax speed {{ 10 | 100 | 1000 } { half-duplex | full-duplex } }**Parameters**

10 half-duplex	Enter 10 to set the speed as 10BASE-T, followed by half-duplex for half duplex.
10 full-duplex	Enter 10 to set the speed as 10BASE-T, followed by full-duplex for full duplex.
100 half-duplex	Enter 100 to set the speed as 100BASE-T, followed by half-duplex for half duplex.
100 full-duplex	Enter 100 to set the speed as 100BASE-T, followed by full-duplex for full duplex.
1000 half-duplex	Enter 1000 to set the speed as 1000BASE-T, followed by half-duplex for half duplex.
1000 full-duplex	Enter 1000 to set the speed as 1000BASE-T, followed by full-duplex for full duplex.

Default auto-negotiate**Mode** Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.**Command History**

Version 2.3 Added Interface Range mode.

Related Commands

auto-negotiate	Enables automatic speed negotiation on a port.
interface range	Defines an interface range and accesses the Interface Range mode
interface	Identifies an interface and enters the Interface Config mode.

speed all

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

Syntax speed all {{ 10 | 100 | 1000 } { half-duplex | full-duplex } }**Parameters**

10 half-duplex	Enter 10 to set the speed as 10BASE-T, followed by half-duplex for half duplex.
10 full-duplex	Enter 10 to set the speed as 10BASE-T, followed by full-duplex for full duplex.

	100 half-duplex	Enter 100 to set the speed as 100BASE-T, followed by half-duplex for half duplex.
	100 full-duplex	Enter 100 to set the speed as 100BASE-T, followed by full-duplex for full duplex.
	1000 half-duplex	Enter 1000 to set the speed as 1000BASE-T, followed by half-duplex for half duplex.
	1000 full-duplex	Enter 1000 to set the speed as 1000BASE-T, followed by full-duplex for full duplex.
Default	auto-negotiate	
Mode	Global Config	
Related Commands	auto-negotiate all	Enables automatic speed negotiation on all ports.

System Utility Commands

System utility commands in this section are:

- [clear config](#)
- [clear counters on page 106](#)
- [clear igmpsnooping on page 106](#)
- [clear pass on page 106](#)
- [clear traplog on page 106](#)
- [copy on page 106](#)
- [copy \(clibanner\) on page 109](#)
- [enable passwd on page 110](#)
- [logout on page 110](#)
- [ping on page 111](#)
- [reload on page 111](#)
- [show terminal length on page 112](#)
- [terminal length on page 112](#)
- [traceroute on page 113](#)
- [write on page 113](#)

See also port channel commands in the chapter [LAG/Port Channel Commands on page 287](#).

clear config

This command resets the configuration to the factory defaults without powering off the switch. The switch is automatically reset when this command is processed. You are prompted to confirm that the reset should proceed.

Syntax clear config

Mode Privileged Exec

clear counters

This command clears the stats for a specified *unit/slot/port* or for all the ports or for the entire switch based upon the argument.

Syntax clear counters {*unit/slot/port* | all}

Mode Privileged Exec

clear traplog

This command clears the trap log.

Syntax clear traplog

Mode Privileged Exec

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and will attempt to delete these entries from the Multicast Forwarding Database.

Syntax clear igmpsnooping

Mode Privileged Exec

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Syntax clear pass

Mode Privileged Exec

copy

This command has options that enable you to download files to the switch, upload files from the switch, or copy SFTOS images from the management unit to other members of its stack. Local URLs can be specified using TFTP or Xmodem.

Syntax	<pre>copy { { {nvram:script <i>url</i>} nvram:errorlog nvram:startup-config nvram:traplog } <i>url</i>} { <i>url</i> {image1 image2 nvram:cli-banner nvram:script nvram:sshkey-dsa nvram:sshkey-rsa1 nvram:sshkey-rsa2 nvram:sslpem-dhstrong nvram:sslpem-dhweak nvram:sslpem-root nvram:sslpem-server nvram:startup-config} {system:running-config nvram:startup-config} {image1 image2} unit://<i>unit</i>{image1 image2} {image1 image2} unit://*!{image1 image2} }</pre>	
Parameters	nvram:	<p>Specify the nvram: keyword preamble to indicate that the location is NVRAM in the switch. When used before <i>url</i>, the location is the source; when used after <i>url</i>, the location is the destination.</p> <p>For details on the keywords associated with nvram:, see the Usage section, below.</p>
	url	<p>Enter the URL of the download or upload address, consisting first of xmodem or TFTP. The xmodem option is followed by a file path and file name, while TFTP is followed first by an IPv4 address (format: <i>xxx.xxx.xxx.xxx</i>), then by a file path and file name.</p> <p>If the file resides in the root directory of the TFTP server, then you can simply enter the filename. The path and filename can be no more than 31 characters each. The file size cannot be larger than 2K.</p>
	{image1 image2}	<p>Enter image1 to have the identified file be downloaded in place of the SFTOS image that is currently stored as image1, or enter image2 to have the identified file be downloaded in place of the SFTOS image that is currently stored as image2. See the Usage section, below, for details.</p>
Default	None	
Mode	Privileged Exec	
Command History	Version 2.5.1	Modified: Added the ability to download and save up to two SFTOS images, and to copy either image to other members of a stack.
	Version 2.3	Modified: Modified functionality of copy system:running-config nvram:startup-config and copy tftp //tftp_server_ip_address/path/filename nvram:startup-config .
Usage	<p>The following files can be specified as the source file for uploading from the switch:</p> <ul style="list-style-type: none"> • Event log (also called the error log or persistent log) (nvram:errorlog <i>url/filename</i>) • Buffered message log (also called the system log) (nvram:log <i>url/filename</i>) • Startup configuration (nvram:startup-config <i>url/filename</i>) • Startup script (nvram:script <i>source filename url/filename</i>) • SNMP Trap log (nvram:traplog <i>url/filename</i>) <p>Specify a TFTP destination and target filename in this form: tftp://tftp_server_ip_address/path/filename For example: copy nvram:log tftp://tftp_server_ip_address/path/filename</p> <p>You can also overwrite the startup configuration file with the running config: copy system:running-config nvram:startup-config</p>	

The `copy` command can also be used to download the following files:

- CLI banner: See `copy (clibanner)`.
- SFTOS software (often called the “software image”):
 - before SFTOS 2.5: `filename system:image`
 - SFTOS 2.5.1: `filename {image1 | image2}`

For example, to download the software to the location where the current backup image is stored, assuming the backup image is stored in the “image 2” location, enter:

```
copy tftp://tftp_server_ip_address/path/filename:image2
```

- SSH key files (`sshkey-rsa`, `sshkey-rsa2`, or `sshkey-dsa`)
- SSL certificates (HTTP secure-server certificates — `sslpem-dhstrong`, `sslpem-dhweak`, `sslpem-root`, `sslpem-server`) (For more on SSH and SSL, see the chapter “Providing User Access Security” in the *SFTOS Configuration Guide*.)
- startup configuration (`startup-config`)

Except for the SFTOS software, download files from a TFTP server with `copy tftp://`, followed by the source URL and filename, and then specify the destination as `nvrām:name`, where `name` is one of the keywords listed above. For example:

```
copy tftp://tftp_server_ip_address/path/filename nvrām:clibanner
copy tftp://tftp_server_ip_address/path/filename nvrām:script
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-root
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-server
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-dhweak
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-dhstrong
copy tftp://tftp_server_ip_address/path/filename nvrām:sshkey-rsa1
copy tftp://tftp_server_ip_address/path/filename nvrām:sshkey-rsa2
copy tftp://tftp_server_ip_address/path/filename nvrām:sshkey-dsa
copy tftp://tftp_server_ip_address/path/filename nvrām:startup-config
copy tftp://tftp_server_ip_address/path/filename {image1 | image2}
```

For example, to download the software to the location where the current backup image is stored, assuming the backup image is stored in the “image 2” location, enter:

```
copy tftp://tftp_server_ip_address/path/filename image2
```



Note: Starting with SFTOS version 2.3, you can use the command `copy tftp://tftp_server_ip_address/path/filename nvrām:startup-config` to copy either a binary file or a text file to the `startup-config` file. The result is a text file.

You can also copy the SFTOS software image in a stack from the management unit to a specific member unit or all member units:

```
copy {image1 | image2} unit://unit/{image1 | image2}
```

For `unit`, enter a specific member number as an integer from 1 to 6.

An asterisk (*) indicates that the image should be copied to all members:

```
unit://*/{image1 | image2}
```

The following command copies the running config from the switch system memory to flash memory, overwriting the startup configuration file:

```
copy system:running-config nvram:startup-config
```



Note: Starting with SFTOS version 2.3, this command creates a text-based startup-config file instead of a binary file.

Example **Figure 6-35. Using the copy command to Upload the Event Log**

```
Force10 S50 #copy nvram:errorlog tftp://10.10.10.10/errorLog
Mode..... TFTP
Set TFTP Server IP..... 10.10.10.10
TFTP Path.....
TFTP Filename..... errorLog
Data Type..... Error Log

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```

Related Commands		
	copy (clibanner)	Downloads the CLI banner text file to the switch.
	boot system	Select an image to be the active image for subsequent reboots and to be loaded by the boot loader.
	write	Saves the running configuration to NVRAM, duplicating the functionality of <code>copy system:running-config nvram:startup-config</code>

copy (clibanner)

This version of the `copy` command, with the “clibanner” option, downloads the CLI banner text file to the switch. Local URLs can be specified using `tftp` or `xmodem`. The CLI banner is configurable text that you can have displayed when the CLI user logs in to the switch. The file cannot be created on the switch. Instead, create the banner file using a text editor, put it on your TFTP server, and then download it to the switch.

Syntax `copy tftp://tftp_server_ip_address/filepath nvram:clibanner`

Reversing the sequence of the command parameters uploads the text file from the switch:

```
copy nvram:clibanner tftp://tftp_server_ip_address/filepath
```

The `no clibanner` command removes the CLI banner.

Parameters		
	<i>tftp_server_ip_address</i>	Enter the URL of the TFTP server in IP address format: <i>xxx.xxx.xxx.xxx</i>
	<i>filepath</i>	Enter the path on the TFTP server and the filename in this format: <i>path/filename</i> . If the file resides in the root directory, then you can simply enter the filename. The path and filename can be no more than 31 characters each. The file size cannot be larger than 2K.

Default none

Mode Privileged Exec

Example **Figure 6-36. Using the copy command to Download the CLI Banner**

```

copy tftp://192.168.77.52/banner.txt nvram:clibanner

Mode..... TFTP
Set TFTP Server IP..... 192.168.77.52
TFTP Path..... ./
TFTP Filename..... banner.txt
Data Type..... Cli Banner

Are you sure you want to start? (y/n) y

CLI Banner file transfer operation completed successfully!

(Force10 S50) #exit

Force10 S50) >logout

FORCE10's Login Banner - Unauthorized access is punishable by law.
User:

```

**Related
Commands**

copy (clibanner)	Downloads the CLI banner text file to the switch.
write	Saves the running configuration to NVRAM, duplicating the functionality of <code>copy system:running-config nvram:startup-config</code>

enable passwd

This command changes the Privileged Exec password (commonly called the “enable” password), which is not set when SFTOS boots for the first time. First type the command, then press **Enter**.

Syntax	<code>enable passwd <i>password</i></code>
Parameters	<i>password</i> Enter a text string, up to 32 characters long, as the clear text password.
Mode	Global Config
Command History	Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode.

logout

Close the current Telnet connection or reset the current serial connection.



Note: Save configuration changes before logging out.

Syntax	<code>logout</code>
Mode	Privileged Exec
Related Commands	quit Close the current Telnet connection, or reset the current serial connection.

quit

This command duplicates the functionality of the **logout** command, closing the current Telnet connection, or resetting the current serial connection.



Note: Save configuration changes before logging out.

Syntax	quit
Mode	Privileged Exec
Related Commands	<hr/> logout Close the current Telnet connection, or reset the current serial connection. <hr/>

ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Syntax	ping <i>ipaddr</i>
Mode	Privileged Exec and User Exec

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Syntax	reload [<i>unit</i>]
	For <i>unit</i> , enter a switch ID in the range of 1 to 8.
Mode	Privileged Exec
Usage Information	For a sample of the output from the reload command, see the section “Upgrading the Software Image” in the Getting Started chapter of the <i>SFTOS Configuration Guide</i> .
Command History	<hr/> Version 2.5.1 Modified: [<i>unit</i>] parameter added <hr/>
Related Commands	<hr/> copy Downloads and uploads various file types, and copies software between stack members. <hr/>

show terminal length

This command displays how many lines are currently in one page of “show” command output, as configured by the `terminal length` command.

Syntax	show terminal length	
Mode	Privileged Exec and User Exec	
Command History	Version 2.3	Introduced
Related Commands	terminal length	Sets the number of lines displayed on the terminal without pausing.

terminal length

Configure the number of lines to be displayed on the terminal screen in one page of output of `show` commands.

Syntax	terminal length <i>number-of-lines</i>	
Parameters	<i>number-of-lines</i>	Enter the number of lines that you want the output to display before pausing. Entering zero (0) will cause the terminal to display without pausing. Range: 0 5 to 512 (1-4 cannot be set.) Default: 24 lines
Defaults	24 lines	
Mode	Use Exec or Privileged Exec	
Command History	Version 2.3	Introduced
Usage Information	This is a session-based command. The CLI presents 24 lines per page of <code>show</code> command output, as a default, unless the user uses this command to change the number of lines. At the end of each page, the user can press <code>q</code> for quit—to stop the output and return to the command line—or any other key to see the next page of the display.	
Related Commands	show terminal length	Displays the number of lines set by <code>terminal length</code> .

traceroute

This command discovers the routes that packets take when traveling to their destination through the network on a hop-by-hop basis.

Syntax `traceroute ipaddr [port]`

ipaddr should be a valid IP address.

port should be a valid decimal integer in the range of 0 (zero) to 65535. The default value is 33434. The optional *port* parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system.

Mode Privileged Exec

This command is used to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. `<ipaddr>` should be a valid IP address. `[port]` should be a valid decimal integer in the range of 0(zero) to 65535. The default value is 33434.

The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system.

write

The functionality of this command is the same as for the `copy system:running-config nvram:startup-config` command, to save the running configuration to NVRAM, which would be used while the system is rebooted the next time. The `write` command defaults to `write memory`.

Syntax `write memory`

Mode Privileged Exec

**Related
Commands**

<code>copy</code>	Uploads and downloads to/from the switch.
-------------------	---

PoE Commands

SFTOS software, starting with version 2.5.1, supports Power over Ethernet (PoE) functionality on the S50V switch. The commands that support PoE are:

- [inlinepower on page 114](#)
- [inlinepower threshold on page 115](#)
- [inlinepower admin on page 115](#)
- [inlinepower priority on page 116](#)
- [inlinepower limit on page 116](#)
- [inlinepower type on page 116](#)
- [show inlinepower \(stack\) on page 117](#)
- [show inlinepower on page 118](#)

In addition to PoE commands in the CLI, SFTOS support for PoE through SNMP is by the Power-Ethernet MIB.

PoE provides the ability to transmit both electrical power and data to remote devices over standard twisted-pair cable. SFTOS support for PoE conforms to IEEE 802.3af, which defines a standard to deliver power over Ethernet cables.

All 48 physical copper interfaces on the S50V have the capability to provide power. Some of the salient features are as follows:

- The maximum power available for PoE on the switch is 360 watts, subject to factors such as other switch requirements. The minimum available is 320 watts. Each port can provide a maximum of 20 watts, subject to the power budget, voltage, and user settings for power priority and power limits per port and per switch in a stack. See [inlinepower priority on page 116](#) and [inlinepower limit on page 116](#).
- Legacy devices, as well as powered devices specifically compliant with 802.3af, are supported.
- When the power budget is exceeded, the next port attempting to power up causes the currently enabled port with the lowest priority to shut down if the port attempting to power up has a higher PoE priority.

inlinepower

Enable or disable the PoE feature for a specified switch in an S-Series stack.

Syntax	<code>inlinepower { disable enable } <i>unit-id</i></code>	
Parameters	<code>disable enable</code>	Enter one or the other keyword to disable or enable PoE.
	<code><i>unit-id</i></code>	Enter the stack member ID of the switch to which you want to change the PoE setting.
Defaults	Enable	
Mode	Global Config	
Command History	Version 2.5.1	Introduced

**Related
Commands**

show inlinepower (stack)	Display PoE status of stack members.
show inlinepower	Display PoE status of designated port.

inlinepower threshold

Configure the amount of Power over Ethernet (PoE) allotted for a specified switch in the S-Series stack. The amount is specified as a percentage of the total possible power budget.

Syntax inlinepower threshold *0-100 unit-id*

Parameters

<i>0-100</i>	Enter an integer from 1 to 100, representing the percentage of the total power budget to make available to the specified switch in the S-Series stack. By default, 80% (288 Watts) of the total possible power budget is available.
<i>unit-id</i>	Enter the stack member ID of the switch to which you want to change the PoE setting.

Defaults 80 (80% (288 Watts) of the total possible power budget)

Mode Global Config

**Command
History**

Version 2.5.1	Introduced
---------------	------------

**Related
Commands**

show inlinepower (stack)	Display PoE status of stack members.
show inlinepower	Display PoE status of designated port.

inlinepower admin

Enable or disable the Power over Ethernet (PoE) feature on a particular port. Once disabled, that port can no longer supply power.

Syntax inlinepower admin {off | auto}

Parameters

off auto	Enter auto to allow the selected port to supply power. Enter off to stop the selected port from supplying power.
------------	---

Defaults auto

Mode Interface Config; Interface Range Ethernet

**Command
History**

Version 2.5.1	Introduced
---------------	------------

**Related
Commands**

show inlinepower (stack)	Display PoE status of stack members.
show inlinepower	Display PoE status of designated port.

inlinepower priority

Configure the priority of a port in terms of access to power.

Syntax	inlinepower priority {critical high low}	
Parameters	critical high low	Enter critical to enable the selected port to receive power at the highest priority. Enter high to enable the selected port to receive power at the next highest priority. Enter low to set the power priority of the selected port at the lowest level.
Defaults	By default, the power priority of a port is set to low.	
Mode	Interface Config; Interface Range Ethernet	
Command History	Version 2.5.1	Introduced
Related Commands	show inlinepower (stack)	Display PoE status of stack members.
	show inlinepower	Display PoE status of designated port.

inlinepower limit

Configure the power limit of a port (the number of watts available to it if PoE is enabled and other ports do not have higher priority access to the power budget).

Syntax	inlinepower limit <i>1-18</i>	
Parameters	<i>1-18</i>	Enter an integer from 1 to 18, representing the maximum number of watts to make available to the selected port.
Defaults	18 (18 watts)	
Mode	Interface Config; Interface Range Ethernet	
Command History	Version 2.5.1	Introduced
Related Commands	show inlinepower (stack)	Display PoE status of stack members.
	show inlinepower	Display PoE status of designated port.

inlinepower type

Enter a power profile description of the port.

Syntax inlinepower type *type-string*

Parameters	<i>type-string</i>	Enter an alphanumeric description.
Defaults	no description	
Mode	Interface Config; Interface Range Ethernet	
Command History	Version 2.5.1	Introduced
Related Commands	show inlinepower (stack)	Display PoE status of stack members.
	show inlinepower	Display PoE status of designated port.

show inlinepower (stack)

This command shows the status for all switches in a stack that support PoE.

Syntax	show inlinepower
Command Modes	User Exec; Privileged Exec
Command History	Version 2.5.1 Introduced

Example **Figure 6-37. Example Output of show inlinepower Command for a Stack**

```

Forcel0-S50V >show inlinepower
Unit   Status   Power(W)   Consumption(W)   Usage(%)   Threshold(%)   Trap
-----
1      Auto     360        22               6.11       100            enable

```

Table 6-17 defines the fields displayed in [Figure 6-37](#).

Table 6-17. show interfaces description Command Example Fields

Field	Description
Unit	The stack member IDs
Status	Whether PoE from the switch is enabled (“Auto”) or disabled (Off)
Power(W)	The total PoE power budget in watts allotted for the switch
Consumption(W)	The current PoE power usage in watts for the switch
Usage(%)	The percentage of PoE power used by the switch of the allotted amount
Threshold(%)	The allotted percentage of the power that could be made available
Trap	Whether PoE SNMP traps are enabled or disabled

Related Commands	inlinepower	Enable or disable PoE for the switch.
-------------------------	-----------------------------	---------------------------------------

inlinepower threshold	Set the percentage of the PoE power that could be made available.
show inlinepower	Display detailed PoE information for ports.

show inlinepower

This command displays PoE status information for a designated port basis or for all ports.

Syntax show inlinepower { *unit/slot/port* | all }

Command Modes Privileged Exec

Command History

Version 2.5.1	Introduced
---------------	------------

Example **Figure 6-38. Example Output of show inlinepower all Command**

```

Force10-S50V#show inlinepower all
Slot
Port      Type          Admin
           Mode        Class  Priority  Output
           -----  -----  -----  -----  -----  -----
1/0/1     Enable        0       Low       0.000  18       Searching
1/0/2     Enable        0       Low       0.000  18       Searching
1/0/3     Enable        0       Low       0.000  18       Searching
1/0/4     Enable        0       Low       0.000  18       Searching
1/0/5     Enable        0       Low       0.000  18       Searching
1/0/6     Enable        0       Low       0.000  18       Searching
1/0/7     Enable        0       Low       0.000  18       Searching
1/0/8     Enable        0       Low       0.000  18       Searching
1/0/9     Enable        0       Low       0.000  18       Searching
1/0/10    Enable        0       Low       1.3    16       Delivering Power
!-----output truncated-----!

```

Table 6-18 defines the fields in [Figure 6-38](#).

Table 6-18. show inlinepower all Command Fields

Field	Description
Slot Port	List of port IDs, in unit/slot/port format
Type	The description entered by the user in the <code>inlinepower type</code> command
Admin Mode	Whether PoE is enabled or disabled for the port
Class	PoE powered device class, as defined in IEEE 802.3af standard
Priority	PoE priority assigned to the port
Output Power	Amount of PoE power currently being used for the port
Limit	Total PoE power allotted in watts to the port
Status	How the port is using PoE: <ul style="list-style-type: none"> A status of Delivering Power indicates that the port is using PoE. A status of Searching generally indicates that the port is off-line. A status of Disabled indicates that PoE is administratively disabled, matching the status listed under Admin Mode. A status of Other generally indicates that power is not being delivered to the port because of power budget constraints.

**Related
Commands**

inlinepower	Enable or disable PoE for the switch.
inlinepower threshold	Set the percentage of the PoE power that could be made available.
show inlinepower (stack)	Display summary PoE information for each unit in the stack.

Dual Image Management Commands

SFTOS software, starting with version 2.5.1, supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature helps to reduce down-time when you upgrade or downgrade the software.

The following commands are in this section:

- [boot system on page 119](#)
- [delete \(software image\) on page 120](#)
- [filedescr \(software image\) on page 120](#)
- [show bootvar on page 121](#)
- [update bootcode on page 122](#)



Note: All commands in this section depend on the association made by the `copy` command during the download of a particular SFTOS file and a system image identifier of either “image1” or “image2”. See [copy on page 106](#).

boot system

This command selects an SFTOS software image to be the active image for subsequent reboots and to be loaded by the boot loader. The current active image is marked as the backup image for subsequent reboots.

Syntax	<code>boot system [unit] {image1 image2}</code>				
Parameters	<table border="1"><tr><td><i>unit</i></td><td>(OPTIONAL) This parameter is valid only on stacks. An error is returned if a number is entered on a standalone system. In a stack, the parameter identifies the stack member on which this command must be executed. Default: all units in the stack</td></tr><tr><td><code>image1 image2</code></td><td>Identify the software image to become the active image for subsequent reboots. If the specified image does not exist on the system, this command returns an error. For details, see the Upgrading Software in a Stack section of the Getting Started chapter in <i>SFTOS Configuration Guide</i>.</td></tr></table>	<i>unit</i>	(OPTIONAL) This parameter is valid only on stacks. An error is returned if a number is entered on a standalone system. In a stack, the parameter identifies the stack member on which this command must be executed. Default: all units in the stack	<code>image1 image2</code>	Identify the software image to become the active image for subsequent reboots. If the specified image does not exist on the system, this command returns an error. For details, see the Upgrading Software in a Stack section of the Getting Started chapter in <i>SFTOS Configuration Guide</i> .
<i>unit</i>	(OPTIONAL) This parameter is valid only on stacks. An error is returned if a number is entered on a standalone system. In a stack, the parameter identifies the stack member on which this command must be executed. Default: all units in the stack				
<code>image1 image2</code>	Identify the software image to become the active image for subsequent reboots. If the specified image does not exist on the system, this command returns an error. For details, see the Upgrading Software in a Stack section of the Getting Started chapter in <i>SFTOS Configuration Guide</i> .				
Default	all units in the stack				
Mode	Privileged Exec				
Command History	<table border="1"><tr><td>Version 2.5.1</td><td>Introduced</td></tr></table>	Version 2.5.1	Introduced		
Version 2.5.1	Introduced				

Related Commands		
	copy	Download files to the switch, or upload files from the switch.
	update bootcode	Activate the specified software image for subsequent reboots.
	show bootvar	Display version information and activation status for the current active and backup images.

delete (software image)

This command deletes the designated image file from permanent storage on the switch.

Syntax	delete [<i>unit</i>] {image1 image2}	
Parameters	<i>unit</i>	(OPTIONAL) This parameter is valid only on stacks. An error is returned if a number is entered on a standalone system. In a stack, the parameter identifies the stack member on which this command must be executed. Default: all units in the stack
	image1 image2	Identify the software image to delete. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, the CLI displays an error.
Default	all units in the stack	
Mode	Privileged Exec	
Command History	Version 2.5.1	Introduced
Related Commands	update bootcode	Activate the specified software image for subsequent reboots.
	show bootvar	Display version information and activation status for the current active and backup images.

filedescr (software image)

This command associates a given text description with an image. Any existing description is replaced.

Syntax	filedescr [<i>unit</i>] {image1 image2} <i>text-description</i>	
Parameters	<i>unit</i>	(OPTIONAL) For stacking, this parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in the stack. Default: all units in the stack
	image1 image2	Identify the software image to associate with the given text description.
	<i>text-description</i>	Enter a text description for the selected software image.
Default	all units in the stack	
Mode	Privileged Exec	

Command History	Version 2.5.1	Introduced
Related Commands	update bootcode	Activate the specified software image for subsequent reboots.
	show bootvar	Display version information and activation status for the current active and backup images.

show bootvar

This command displays version information and activation status for the current active and backup images on the specified stack member. If you do not specify a unit number, the command displays image details for all nodes on the Stack. The command also displays any text description associated with an image. When this command is used on a standalone system, it displays the switch activation status, and the *unit* parameter is not valid.

Syntax show bootvar [*unit*]

Mode Privileged Exec

Command History	Version 2.5.1	Introduced
------------------------	---------------	------------

Example **Figure 6-39. Example of Output from the show bootvar Command**

```
Force10 #show bootvar
Image Descriptions
image1 : default image
image2 :

Images currently available on Flash
-----
unit      image1      image2      current-active      next-active
-----
1         2.5.1       <none>      image1              image1
```

Report Fields image1 — The SFTOS image stored in the “image1” location in NVRAM

image2 — The SFTOS image stored in the “image2” location in NVRAM

unit — The stack member number

current-active — The SFTOS image currently running the switch

next-active — The SFTOS image set to be invoked on the next reload

Related Commands	boot system	Activate the specified software image for subsequent reboots.
	update bootcode	Activate the specified software image for subsequent reboots.

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active image for subsequent reboots.

Syntax	update bootcode [<i>unit</i>]	
Parameters	<i>unit</i> (OPTIONAL) This parameter is valid only on stacks. An error is returned if a number is entered on a standalone system. In a stack, the parameter identifies the stack member on which this command must be executed. Default: all units in the stack	
Default	all units in the stack	
Mode	Privileged Exec	
Command History	Version 2.5.1	Introduced
Related Commands	boot system	Activate the specified software image for subsequent reboots.
	delete (software image)	Delete the designated image file from permanent storage on the switch.
	show bootvar	Display version information and activation status for the current active and backup images.

Configuration Scripting

Configuration scripting enables you to generate text-formatted script files representing the current configuration. These configuration script files can be uploaded to a PC and edited, downloaded to the system and applied to the system. Configuration scripts can be applied to one or more switches with no/minor modifications.



Note: The file extension must be “.scr”.

A maximum of ten scripts are allowed on the switch.

The combined size of all script files on the switch cannot exceed 500 KB.

Configuration script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.

The commands in this section are:

- [script apply on page 123](#)
- [script delete on page 123](#)
- [script list on page 123](#)
- [script show on page 124](#)
- [script validate on page 124](#)

script apply

This command backs up the running configuration and then starts applying the commands in the script file. Application of the commands stops at the first failure of a command.

Syntax script apply *scriptname*

The *scriptname* is the file name of the script file (including extension) to be applied. The script name must be “startup-config” or have a file extension of “.scr”.

Mode Privileged Exec

Usage Use the `show running-config` command to capture the running configuration into a script. Use the `copy` command to transfer the configuration script to/from the switch.

**Related
Commands**

copy	Downloads files to the switch and uploads files from the switch. Copies files within the system and between switches.
show running-config	Display/capture the current setting of different protocol packages supported on the switch.

script delete

This command deletes a specified script.

Syntax script delete {*scriptname* | all}

Parameters

<i>scriptname</i>	File name, including extension (“.scr”), of the configuration script to be deleted
all	Deletes all configuration script files from the switch.

Mode Privileged Exec

script list

This command lists all scripts present on the switch as well as the total number of files present.

Syntax script list

Mode Privileged Exec

Report Elements Configuration Script Name

Size (Bytes)

script show

This command displays the contents of a script file.

Syntax `script show scriptname`

The *scriptname* is the file name of the script file, including extension. The script name must be “startup-config” or have a file extension of “.scr”.

Mode Privileged Exec

The format of the display is: Line <no>: <Line contents>

script validate

This command validates a configuration script file by parsing each line in the script file where *scriptname* is the name of the script to be validated. The validation stops at the first failure of a command.

Syntax `script validate scriptname`

The *scriptname* is the file name of the script file, including extension. The script name must be “startup-config” or have a file extension of “.scr”.

Mode Privileged Exec

VLAN Commands

Use the commands in this chapter to configure virtual local area networks (VLANs) that conform to IEEE 802.1Q. The three major sections in this chapter are:

- [Virtual LAN \(VLAN\) Commands](#)
- [Protected-Port \(PVLAN\) Commands on page 147](#)
- [VLAN-Stacking Commands on page 150](#)

Virtual LAN (VLAN) Commands

In SFTOS 2.3.1, the `aoCEst OEuogrou` command (see [interface vlan on page 129](#)) is the starting point for VLAN configuration. Execute the command from the Global Config mode.



Note: You can also configure VLANs with bulk configuration commands. See [interface range on page 91](#).

Executing the `aoCEst OEuogrou` command creates a new VLAN if the identified VLAN ID does not already exist; otherwise, the command selects an existing VLAN. Then, in either case, the command invokes the Interface VLAN mode, in which you have access to VLAN configuration commands for the specified VLAN.

Table 7-19. Commands in the Interface VLAN Mode

Commands	Command/Command Family Description	Location of Command Syntax Description
<code>.EnOsadCaeo</code>	Add a description to the VLAN.	This chapter
<code>encapsulation (VLAN)</code>	Configure interface link layer encapsulation type.	This chapter
<code>exit</code>	Leave the mode.	
<code>help</code>	Display help for various special keys.	
<code>igmp</code>	Configure IGMP Snooping parameters for the VLAN.	IGMP Snooping Commands on page 273 IGMP Commands on page 471 (IP Multicast chapter)
<code>ip</code>	Configure IP parameters.	These commands are not part of the Layer 2 Package used for the S2410. See Virtual LAN Routing Commands on page 413 .
IP Subnet-based VLANs	Associate the VLAN with the IP address and subnet mask for a desired partitioning of the network.	Not supported in this release
MAC-based VLANs	Define MAC addresses that belong to the same VLAN.	Not supported in this release

Table 7-19. Commands in the Interface VLAN Mode (continued)

Commands	Command/Command Family Description	Location of Command Syntax Description
makestatic	Change the VLAN type from Dynamic to Static.	This chapter
mtu (VLAN)	Set the default MTU size.	This chapter
name (VLAN)	Configure an optional VLAN name.	This chapter
protocol	Configure the protocols associated with particular group IDs.	This chapter
tagged/untagged	Configure tagging for an interface.	This chapter

Virtual LAN (VLAN) commands in this section are:

- [clear vlan on page 127](#)
- [description on page 127](#)
- [encapsulation \(VLAN\) on page 128](#)
- [interface vlan on page 129](#)
- [makestatic on page 130](#)
- [mtu \(VLAN\) on page 130](#)
- [name \(VLAN\) on page 131](#)
- [network mgmt_vlan on page 131](#)
- [participation \(VLAN\) on page 131](#)
- [priority \(VLAN\) on page 132](#)
- [protocol group on page 132](#)
- [protocol vlan group on page 132](#)
- [protocol vlan group all on page 133](#)
- [pvid \(VLAN\) on page 133](#)
- [show vlan on page 134](#)
- [show vlan association mac on page 136](#)
- [show vlan association subnet on page 137](#)
- [show vlan port on page 138](#)
- [tagged on page 139](#)
- [untagged on page 140](#)
- [vlan on page 141](#)
- [vlan acceptframe on page 141](#)
- [vlan association mac on page 141](#)
- [vlan association subnet on page 142](#)
- [vlan database on page 143](#)
- [vlan ingressfilter on page 143](#)
- [vlan participation \(interface\) on page 143](#)
- [vlan participation all on page 144](#)
- [vlan port acceptframe on page 144](#)

- [vlan port ingressfilter all on page 144](#)
- [vlan port pvid all on page 144](#)
- [vlan port tagging all on page 145](#)
- [vlan protocol group on page 145](#)
- [vlan protocol group add protocol on page 146](#)
- [vlan protocol group remove on page 146](#)
- [vlan pvid on page 146](#)
- [vlan tagging on page 147](#)



Note: For information on commands related to the management VLAN, see [General System Management and Information Commands on page 35](#) (most specifically, [interface managementethernet on page 38](#)) in the Management chapter.

For general instructions on configuring the management VLAN, see the Management chapter in the *SFTOS Configuration Guide*.

For other VLAN information in the *SFTOS Configuration Guide*, see the Creating VLANS section of the Getting Started chapter, the chapters on STP, GARP and GVRP, IGMP Snooping, and the VLAN section of the Layer 3 Routing chapter.

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Syntax	clear vlan	
Default	disabled	
Mode	Privileged Exec	
Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports

description

Enter a description for the selected interface (port or VLAN).

Syntax	[no] description <i>description</i>	
	The <i>description</i> allows spaces if you surround the statement with single or double quotes.	
Default	none	
Mode	Interface VLAN; Interface Config	
Command History	Version 2.3	Introduced

Usage Information

The following example shows the use of both single quotes and double quotes in entering a description for a port. The example also shows the resulting descriptions presented in `show interfaces description` commands.

Example**Figure 7-40. show interfaces description Command Example**

```
S50 #conf
S50 (Config)#interface 1/0/1
S50 (Interface 1/0/1)#description "1/0/1 is access port"
S50 (Interface 1/0/1)#exit
S50 (Config)#interface 1/0/30
S50 (Interface 1/0/30)#description 'management port in vlan 30'
S50 (Interface 1/0/30)#exit
S50 (Config)#exit
S50 #show interfaces description 1/0/1
Interface.....1/0/1
IfIndex.....1
Description....1/0/1 is access port
MAC Address....00:01:E8:D5:BA:C0
Bit Offset Val..1

S50 #show interfaces description 1/0/30
Interface.....1/0/30
IfIndex.....30
Description....management port in vlan 30
MAC Address....00:01:E8:D5:BA:C0
Bit Offset Val..30

S50 #
```

Related Commands

description (port channel)	Add a description for the selected port channel.
interface vlan	Creates a VLAN, assigns it an ID and then enters the Interface VLAN mode
show interfaces	Displays information, including the description, about a selected interface.
show running-config	Display/capture the current setting of different protocol packages supported on the switch.

encapsulation (VLAN)

This command configures the link layer encapsulation type for the packet within the VLAN. Acceptable encapsulation types are Ethernet and SNAP.

Syntax `encapsulation {ethernet | snap}`

Default ethernet

Mode Interface VLAN

Restrictions—Routed frames are always Ethernet-encapsulated when a frame is routed to a VLAN.

Command History

Version 2.3	Introduced
-------------	------------

Related Commands

interface vlan	Creates a VLAN, assigns it an ID and then enters the Interface VLAN mode
encapsulation (interface)	Configures the link layer encapsulation type for the packet within the specific interface.

interface vlan

This command creates a new VLAN if the identified VLAN ID does not already exist, or else the command selects the existing VLAN. Then, in either case, the command invokes the Interface VLAN mode, in which you have access to VLAN configuration commands for the specified VLAN.

Syntax interface vlan *vlanid*

The *vlanid* is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-3965.

The **no** version of this command deletes an existing VLAN.

Default None

Mode Global Config

Command History

Version 2.3	Introduced. Replaces vlan database and vlan commands.
-------------	---

Usage Information

After using this command to access the Interface VLAN mode (the prompt for the Interface VLAN mode is **(conf-if-vl-<vlan-id>#)**), you can configure the selected VLAN.

You can also make configuration changes to a VLAN in the Interface Range mode (see [interface range](#) on page 91) and the Global Config mode. For details on modes, see [Chapter 4, “Using the Command Line Interface,”](#) on page 23.

Example Figure 7-41. Command Options in the Interface VLAN Mode

```
Force10 #config
Force10 (Config)#interface vlan 5
Force10 (Conf-if-vl-5)#?

description          Add Description to the interface
encapsulation        Configure interface link layer encapsulation type.
exit                 To exit from the mode.
help                 Display help for various special keys.
igmp                  Configure IGMP Snooping parameters for the Vlan
ip                    Configure IP parameters.
mtu                   Sets the default MTU size.
protocol              Configure the Protocols associated with particular
                     Group Ids.
makestatic            Change the VLAN type from 'Dynamic' to 'Static'.
name                  Configure an optional VLAN Name.
pvid                  Configure the VLAN id for a specific port.
tagged                Configure tagging for a specific VLAN port.
untagged              Configure untagging for a specific VLAN port.

Force10 (Conf-if-vl-5)#exit
Force10 (Config)#exit
Force10 #show vlan brief
VLAN ID  VLAN Name                               MAC Aging      IP Address
-----  -
1          Default                                     300            unassigned
5                                              300            unassigned

Force10#
```

Related Commands

dot1p-priority	Configures the 802.1p port priority assigned for untagged packets for a specific interface.
--------------------------------	---

interface	Accesses the Interface Config mode for a designated logical or physical interface.
---------------------------	--

interface vlan	Groups a set of individual interfaces, a range of interfaces, or more than one range of interfaces, to which subsequent configuration commands can be applied (bulk configuration)
ip address (VLAN)	Assigns an IP address and subnet mask to the selected VLAN to support Layer 3 routing.
protocol group	Attach a group ID to the selected VLAN.
show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
show port	Displays port information for a selected port or for all ports

makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined).

Syntax	makestatic				
Mode	Interface VLAN				
Command History	Version 2.3 Changed from <code>vlan makestatic <i>vlan-id</i></code> to <code>makestatic</code> and moved to Interface VLAN mode.				
Related Commands	<table border="1"> <tr> <td>show vlan</td> <td>Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.</td> </tr> <tr> <td>show port</td> <td>Displays port information for a selected port or for all ports</td> </tr> </table>	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.	show port	Displays port information for a selected port or for all ports
show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.				
show port	Displays port information for a selected port or for all ports				

mtu (VLAN)

This command sets the MTU (Maximum Transmission Unit) of the selected VLAN.

Syntax	[no] mtu 576-1500										
Default	1500										
Mode	Interface VLAN										
Command History	Version 2.3 Introduced										
Related Commands	<table border="1"> <tr> <td>mtu (port)</td> <td>Sets the MTU for a selected port (Interface Config mode)</td> </tr> <tr> <td>mtu (LAG)</td> <td>Sets the MTU for a selected port channel</td> </tr> <tr> <td>ip mtu</td> <td>Sets the MTU on a routing interface (Interface Config or VLAN mode)</td> </tr> <tr> <td>show vlan</td> <td>Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.</td> </tr> <tr> <td>show port</td> <td>Displays port information for a selected port or for all ports</td> </tr> </table>	mtu (port)	Sets the MTU for a selected port (Interface Config mode)	mtu (LAG)	Sets the MTU for a selected port channel	ip mtu	Sets the MTU on a routing interface (Interface Config or VLAN mode)	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.	show port	Displays port information for a selected port or for all ports
mtu (port)	Sets the MTU for a selected port (Interface Config mode)										
mtu (LAG)	Sets the MTU for a selected port channel										
ip mtu	Sets the MTU on a routing interface (Interface Config or VLAN mode)										
show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.										
show port	Displays port information for a selected port or for all ports										

name (VLAN)

This command changes the name of a VLAN.

Syntax [no] name *newname*

The *newname* is an alphanumeric string of up to 32 characters.

The no version of this command sets the name of a VLAN to a blank string.

Default The name for VLAN ID 1 is always Default. The name for other VLANs is defaulted to a blank string.

Mode Interface VLAN

Command History	Version 2.3	Modified: Changed from <code>vlan name</code> to <code>name</code> and mode changed from VLAN database to Interface VLAN. Removed ID range variable.

Related Commands	<code>show vlan</code>	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	<code>show port</code>	Displays port information for a selected port or for all ports
	<code>ip address (VLAN)</code>	Create VLAN and enter Interface VLAN mode.

network mgmt_vlan

Command History	Version 2.5.1	Removed from CLI
	Version 2.3	Deprecated: The functionality is available in the <code>vlan participation</code> command within the Interface ManagementEthernet mode.

Related Commands	<code>interface managementethernet</code>	Invokes ManagementEthernet mode (the (Config-if-ma)# prompt), in which the user can set the network parameters of the switch, including using the <code>vlan participation</code> command.
	<code>vlan participation (management VLAN only)</code>	Assigns the management VLAN.

participation (VLAN)

Configure how ports participate in a specific VLAN.

Mode Interface VLAN

Command History	Version 2.5.1	Removed from CLI
	Version 2.3	Deprecated

Related Commands	<code>tagged</code>	Sets tagging to enabled for a specific port (or range of ports) in the selected VLAN.
-------------------------	---------------------	---

priority (VLAN)

Configure the priority for untagged frames.

Mode	Interface VLAN	
Command History	Version 2.5.1	Removed from CLI
	Version 2.3	Deprecated
Related Commands	tagged	Sets tagging to enabled for a specific port (or range of ports) in the selected VLAN.

protocol group

Attach a group ID to the selected VLAN. A group ID can only be associated with one VLAN at a time. However, the VLAN association can be changed. The referenced VLAN should be created prior to the creation of the protocol-based VLAN, except when GVRP is expected to create the VLAN.

Syntax	[no] protocol group <i>groupid</i>	
	The no version of this command removes the group ID from this VLAN.	
Default	None	
Mode	Interface VLAN	
Command History	Version 2.3	Modified: Removed <i>vlanid</i> parameter and changed mode from VLAN Database mode to Interface VLAN.
Related Commands	interface vlan	Configure a VLAN and enter Interface VLAN mode.
	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports
	vlan protocol group	Adds a protocol-based VLAN group to the system.
	vlan protocol group add protocol	Add the named protocol to the protocol-based VLAN identified by <i>groupid</i> .

protocol vlan group

This command adds the physical *unit/slot/port* interface to the protocol-based VLAN identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

The **no** version of this command removes the interface from this protocol-based VLAN group that is identified by this *groupid*.

Syntax	[no] protocol vlan group <i>groupid</i>
Default	None
Mode	Global Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	Version 2.5.2 Unsupported: not tested in 2.5.2
	Version 2.5.1 Unsupported: not tested in 2.5.1
	Version 2.3 Added Interface Range mode.
Related Commands	interface range Defines an interface range and accesses the Interface Range mode

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

The **no** version of this command removes all interfaces from this protocol-based VLAN group that is identified by this *groupid*.

Syntax	[no] protocol vlan group all <i>groupid</i>
Default	None
Mode	Global Config
Command History	Version 2.5.2 Unsupported: not tested in 2.5.2
	Version 2.5.1 Unsupported: not tested in 2.5.1

pvid (VLAN)

Configure the VLAN ID for a specific port.

Command History	Version 2.5.1 Removed from CLI
	Version 2.3 Deprecated. Use the untagged command.

**Related
Commands**

untagged	Sets tagging to disabled for a specific port (or range of ports) in the selected VLAN.
--------------------------	--

show vlan

This command displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs. The ID is a valid VLAN identification number.

Syntax show vlan [association | brief | id *vlanid* | name | port]

Parameters

association	(OPTIONAL) See show vlan association mac on page 136 and show vlan association subnet on page 137 .
brief	(OPTIONAL) Enter the keyword brief to display summary information for all configured VLANs.
id <i>vlanid</i>	(OPTIONAL) Enter the keyword id followed, in place of <i>vlanid</i> , by the desired VLAN number to display detailed information for the selected VLAN. Range: 1 to 3965
name	(OPTIONAL) Enter the keyword name to display the names of configured VLANs.
port	(OPTIONAL) Enter the keyword port to display 802.1Q port parameters.

Mode Privileged Exec and User Exec

**Command
History**

Version 2.5.1	Modified: Added “Native VLAN” information to output and revised the presentation of LAG (port channel) in the
Version 2.3	Modified: Changed parameters to include show vlan brief .

**Usage
Information**

The **show vlan association** command is not available for the S50. See [show vlan association mac on page 136](#) and [show vlan association subnet on page 137](#).

For the **show vlan** command, without parameters, the output is shown in [Figure 7-42](#).

For the **show vlan brief** command, the output is shown in [Figure 7-43](#).

For the **show vlan id** command, the output is shown in [Figure 7-44](#).

Example Figure 7-42. Output of the show vlan Command

```

Force10#show vlan
Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface, ^ - Native VLAN
VlanId  Status      Q  Ports
-----
* 1      Active      U  E    ^1/0/1 , 1/0/2 , ^1/0/3 , ^1/0/4 , ^1/0/6 , ^1/0/7
      ^1/0/8 , ^1/0/9 , ^1/0/10, ^1/0/11, ^1/0/12, ^1/0/13
      ^1/0/14, ^1/0/15, ^1/0/16, ^1/0/17, ^1/0/18, ^1/0/19
      ^1/0/23, ^1/0/25, ^1/0/26, ^1/0/27, ^1/0/28, ^1/0/29
      ^1/0/30, ^1/0/31, ^1/0/32, ^1/0/33, ^1/0/34, ^1/0/35
      ^1/0/36, ^1/0/37, ^1/0/38, ^1/0/39, ^1/0/40, ^1/0/41
      ^1/0/42, ^1/0/43, ^1/0/44, ^1/0/45, ^1/0/46, ^1/0/47
      ^1/0/48
      2      Active      U  E    ^1/0/20, ^1/0/21, ^1/0/22, ^1/0/24
      T  E    1/0/40, 1/0/42, 1/0/43, 1/0/44
      U ^Po1  ( 1/0/35, 1/0/36, 1/0/37)
      U ^Po2  ( 1/0/10)
      U ^Po3  ( 1/0/15)
      4      Inactive   T  E    1/0/3 , 1/0/44
      5      Active      U  E    ^1/0/5
      T  E    ^1/0/2 , 1/0/44
      300     Inactive

```


Report Fields Description of the fields in the show vlan report:

Vlan Id: List of configured VLAN IDs

Status: Active or Inactive. A VLAN is active only if the VLAN contains interfaces and those interfaces are operationally up.

Q: "T" indicates that the port is tagged; "U" indicates untagged.

Ports: "E" for Ethernet, followed by the port numbers (unit/slot/port) in the VLAN "E ^", followed by the port numbers in the native VLAN.

 **Note:** Note, in [Figure 7-42](#), that ports added to VLANs as tagged are also still listed in the default VLAN 1. If they had been added as untagged, they would be removed from VLAN 1.

The output of the show vlan brief command is shown in the following example:

Example Figure 7-43. Output of the show vlan brief Command

```

Force10#show vlan brief
VLAN      Name      MAC Aging      IP Address
-----
1          abc       1800           unassigned
2          egf       1800           unassigned
3          sss       1800           unassigned
5                   1800           unassigned
12                  1800           unassigned
13                  1800           unassigned

```

Fields in the show vlan brief report:

VLAN: VLAN ID

Name: Assigned VLAN name

MAC Aging: Displayed in seconds

IP Address: IP Address assigned to the VLAN

Usage Information

For the `show vlan id vlan-id` command, the output is shown in the following example:

Example**Figure 7-44. Output of the show vlan id Command**

```

Forcel0#R1 #show vlan id 2
Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface, ^ - Native Vlan

VlanId  Status      Q  Ports
-----  -
2       Active      U  E   ^1/0/20,^1/0/21,^1/0/22,^1/0/24
          T  E   1/0/40, 1/0/42, 1/0/43, 1/0/44
          U  ^Po1 ( 1/0/35, 1/0/36, 1/0/37)
          U  ^Po2 ( 1/0/10)
          U  ^Po3 ( 1/0/15)

```

Description of the fields in the `show vlan id` report:

VLAN Id: VLAN number

Status: A VLAN is active only if the VLAN contains interfaces and those interfaces are operationally up.

Q: (T) tagged or (U) untagged information

Ports: Speed - whether it is 10G, 1G or fast Ethernet interface and port number (unit/slot/port).
The “^” indicates the native VLAN.

“Po” indicates a port channel (also called a LAG)

show vlan association mac

This command displays the information about either all IP subnet-based VLANs or the VLAN associated with a specific IP address and mask.



Note: The S50V and S25P support MAC-based VLANs. The original S50 does not.

Syntax	<code>show vlan association mac [<i>mac</i>]</code>
Parameters	<i>mac</i> (OPTIONAL) For <i>mac</i> , enter the MAC address to be used for retrieving information about the associated VLAN.
Mode	Privileged Exec
Command History	Version 2.5.1 Introduced
Usage Information	Examples of using the <code>show vlan association mac</code> command, with and without the <i>mac</i> variable, are shown in Figure 7-45 .

Example **Figure 7-45. Output of the show vlan association mac Command**

```
Forcel0#show vlan association mac
MAC Address          VLAN ID
-----
00:06:11:11:11:11   6
00:07:11:12:13:14:15:16 7


Forcel0-S50V #show vlan association mac 11:11:11:11:11:11
MAC Address          VLAN ID
-----
00:06:11:11:11:11   6
```

Related Commands

vlan association mac	Configures a VLAN by associating the VLAN with a set of MAC addresses.
vlan association subnet	Configures a VLAN by associating the VLAN with an IP address and subnet.
interface vlan	Creates a VLAN or selects an already-created VLAN.

show vlan association subnet

This command displays the information about either all IP subnet-based VLANs or the VLAN associated with a specific IP address and mask.

 **Note:** The S50V and S25P support IP subnet-based VLANs. The original S50 does not.

Syntax	show vlan association subnet [<i>ipaddr netmask</i>]
Parameters	<i>ipaddr netmask</i> (OPTIONAL) For <i>ipaddr</i> and <i>netmask</i> , enter the IP address and subnet mask to be used for retrieving information about the associated VLAN.
Mode	Privileged Exec
Command History	Version 2.5.1 Introduced
Usage Information	Examples of using the show vlan association subnet command, with and without the <i>ipaddr netmask</i> variables, are shown in Figure 7-46 .

Example Figure 7-46. Output of the show vlan association subnet Command

```

Forcel0#show vlan association subnet
IP Address      IP Mask      VLAN ID
-----
2.2.2.2         255.0.0.0    6
3.3.3.2         255.0.0.0    7

Forcel0-S50V #show vlan association subnet 2.2.2.2 255.0.0.0
IP Address      IP Mask      VLAN ID
-----
2.2.2.2         255.0.0.0    6

```

**Related
Commands**

show vlan association mac	Display information about either all MAC-based VLANs or the VLAN associated with a specific MAC address.
show port	Displays port information for a selected port or for all ports
interface vlan	Creates a VLAN or selects an already-created VLAN.
vlan association subnet	Configures an IP subnet-based VLAN by associating the VLAN with an IP address and subnet mask.

show vlan port

Display 802.1Q port parameters.

Syntax show vlan port { *unit/slot/port* | all }

Parameters

<i>unit/slot/port</i>	Enter interface in unit/slot/port format for retrieving information about the associated interface.
all	Enter all for retrieving information about all interfaces.

Mode Privileged Exec

**Command
History**

Version 2.1	Introduced
-------------	------------

Example Figure 7-47. Output of the show vlan port Command

```

Forcel0-S50 #show vlan port 1/0/1
  Port      Acceptable  Ingress      Default
Interface  VLAN ID  Frame Types  Filtering    GVRP         Priority
-----
1/0/1      1        Admit All    Enable       Disable      0

Protected Port ..... False

Forcel0-S50 #show vlan port all
  Port      Acceptable  Ingress      Default
Interface  VLAN ID  Frame Types  Filtering    GVRP         Priority
-----
1/0/1      1        Admit All    Enable       Disable      0
1/0/2      1        Admit All    Enable       Disable      0
1/0/3      1        Admit All    Enable       Disable      0
1/0/4      1        Admit All    Enable       Disable      0
1/0/5      1        Admit All    Enable       Disable      0
1/0/6      1        Admit All    Enable       Disable      0
1/0/7      1        Admit All    Enable       Disable      0
1/0/8      1        Admit All    Enable       Disable      0
1/0/9      1        Admit All    Enable       Disable      0
1/0/10     1        Admit All    Enable       Disable      0
1/0/11     1        Admit All    Enable       Disable      0

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

```

tagged

This command sets tagging to enabled for a specific port (or range of ports) in the selected VLAN. If tagging is enabled, traffic is transmitted as tagged frames.

Syntax [no] tagged { *intf-range* [native] | port-channel *port-channel-range* }

To remove tagged interfaces from the VLAN, use the **no tagged** version of the command (not **untagged**). If tagging is disabled, traffic is transmitted as untagged frames.

Parameters

<i>intf-range</i>	Enter one port (<i>unit/slot/port</i> format) or a list of ports. Use a hyphen to designate a range of ports in this format: <i>unit/slot/port-unit/slot/port</i> For nonconsecutive ports, separate each <i>unit/slot/port</i> with a comma and no spaces before or after the comma. Note: The range of interfaces can go across members in a stack.
<i>native</i>	(OPTIONAL) Enter this keyword to configure the VLAN as a Native VLAN.
<i>port-channel</i> <i>port-channel-range</i>	If you do not enter a port (range), enter port-channel followed by one or more port channel numbers, following the hyphen and comma rules described above, for example port-channel 1,3 .

Mode Interface VLAN; Interface Range Vlan Config

Command History

Version 2.5.1	Modified: Added ranges for ports and port channels. Added native . Added Interface Range Vlan Config mode.
Version 2.3	Introduced

Usage Information The `tagged` command includes the functionality of the `vlan participation include` command and the `vlan acceptframe vlanOnly` command. For details, see the VLAN chapter in the *SFTOS Configuration Guide*.

The `tagged` command cannot be applied to ports in VLAN 1, which is the default VLAN.

Example **Figure 7-48. Using the tagged Command**

```
Force10#config
Force10 (Config)#interface vlan 2
Force10 (Conf-if-vl-2)#tagged 1/0/20-1/0/22 native
Force10 (Conf-if-vl-2)#tagged port-channel 1,3
Force10 (Conf-if-vl-2)#
```

Related Commands

<code>show vlan</code>	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
<code>show port</code>	Displays port information for a selected port or for all ports
<code>interface vlan</code>	Creates a VLAN or selects an already-created VLAN.
<code>vlan participation (management VLAN only)</code>	Change the management VLAN of the switch.
<code>vlan port tagging all</code>	Sets the tagging behavior for all interfaces in a VLAN to enabled.

untagged

This command adds a Layer 2 interface to the selected VLAN as an untagged interface.

Syntax `[no] untagged { intf-range | port-channel port-channel-range }`

To remove an untagged interface from the VLAN, use the `no` version of the command.

The `no` option adds the designated interface(s) to the native VLAN. The command sets an `acceptframe` type of the interface to “all”. For details, see the Native VLAN section of the VLAN chapter in the *SFTOS Configuration Guide*.

Parameters

<code><i>intf-range</i></code>	Enter one port (<i>unit/slot/port</i> format) or a list of ports. Use a hyphen to designate a range of ports in this format: <i>unit/slot/port-unit/slot/port</i> For nonconsecutive ports, separate each <i>unit/slot/port</i> with a comma and no spaces before or after the comma. Note: The range of interfaces can go across members in a stack.
<code>port-channel <i>port-channel-range</i></code>	If you do not enter a port (range), enter <code>port-channel</code> followed by one or more port channel numbers, following the hyphen and comma rules described above, for example <code>port-channel 1,3</code> .

Mode Interface VLAN

Command History	Version 2.5.1	Modified: Added ranges for ports and port channels. Added Interface Range Vlan Config mode.
	Version 2.3	Introduced

Usage Information The untagged command includes the functionality of these commands: `participation include`, `pvid`, and `acceptframe untagged`. For details, see the VLAN chapter in the *SFTOS Configuration Guide*.

Related Commands	<code>show vlan</code>	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	<code>show port</code>	Displays port information for a selected port or for all ports
	<code>tagged</code>	Sets tagging to enabled for a specified interface in the selected VLAN.

vlan

Command History	Version 2.3	Modified: Replaced by <code>interface vlan</code> .
------------------------	-------------	---

vlan acceptframe

This command sets the frame acceptance mode per interface.

Mode Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.5.1	Removed from CLI
	Version 2.3	Deprecated

Related Commands	<code>untagged</code>	Sets tagging to disabled for a specific port (or range of ports) in the selected VLAN.
-------------------------	-----------------------	--

vlan association mac

This command configures a VLAN based on a set of MAC addresses, source and destination.

 **Note:** The S50V and S25P support MAC-based VLANs. The original S50 does not.

The `no` version of this command removes the association of the VLAN with the specified MAC address.

Syntax [no] `vlan association mac mac`

For `mac`, enter a source MAC address to be used as the basis for the VLAN.

Default	enabled	
Mode	Interface VLAN	
Command History	Version 2.5.2	Unsupported: not tested in 2.5.2
	Version 2.5.1	Introduced
Related Commands	interface vlan	Creates a new VLAN, or selects one based on ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
	show mac-addr-table	Displays forwarding database entries, including MAC addresses by VLAN.
	show port	Displays port information for a selected port or for all ports
	show interfaces	Displays information about a selected interface or VLAN.
	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show vlan association mac	Displays information about either all MAC-based VLANs or the VLAN associated with a specific MAC address.
	show vlan association subnet	Displays information about either all IP subnet-based VLANs or the VLAN associated with a specific IP address and mask.

vlan association subnet

This command configures an IP subnet-based VLAN by associating the VLAN with an IP address and subnet mask.



Note: The S50V and S25P support IP subnet-based VLANs. The original S50 does not.

The **no** version of this command removes the association of the VLAN with the specified IP address and subnet mask.

Syntax [no] vlan association subnet *ipaddr netmask*

For *ipaddr* and *netmask*, enter the IP address and subnet mask, used as the basis for the VLAN.

Default enabled

Mode Interface VLAN

Command History

Version 2.5.2	Unsupported: not tested in 2.5.2
Version 2.5.1	Introduced

**Related
Commands**

interface vlan	Creates a new VLAN, or selects one based on ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
show vlan association subnet	Displays information about either all IP subnet-based VLANs or the VLAN associated with a specific IP address and mask.
show port	Displays port information for a selected port or for all ports
show interfaces	Displays information about a selected interface or VLAN.
show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.

vlan database

**Command
History**

Version 2.3	Modified: Replaced by interface vlan .
-------------	--

vlan ingressfilter

This command manages ingress filtering.

Mode

Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

**Command
History**

Version 2.5.1	Removed from CLI
Version 2.3	Deprecated

**Related
Commands**

untagged	Sets tagging to disabled for a specific port (or range of ports) in the selected VLAN.
--------------------------	--

vlan participation (interface)

This command configures the degree of participation for a specific interface in a VLAN.

Mode

Interface Config

**Command
History**

Version 2.5.1	Removed from CLI
Version 2.3	Deprecated. Use the tagged and untagged commands.

**Related
Commands**

tagged	Configure a tagged interface in the selected VLAN.
untagged	Configure an untagged interface in the selected VLAN.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN.

Mode	Global Config	
Command History	Version 2.5.1	Deprecated. Removed from CLI
	Version 2.3	Modified: Moved from Interface Config mode to Global Config mode.
Related Commands	tagged	Configure a tagged interface in the selected VLAN.
	untagged	Configure an untagged interface in the selected VLAN.

vlan port acceptframe

This command sets the frame acceptance mode for all interfaces.

Mode	Global Config	
Command History	Version 2.5.1	Deprecated. Removed from CLI
Related Commands	tagged	Configure a tagged interface in the selected VLAN.
	untagged	Configure an untagged interface in the selected VLAN.

vlan port ingressfilter all

This command enables ingress filtering for all ports.

Mode	Global Config	
Command History	Version 2.5.1	Deprecated. Removed from CLI
Related Commands	tagged	Configure a tagged interface in the selected VLAN.
	untagged	Configure an untagged interface in the selected VLAN.

vlan port pvid all

This command changes the VLAN ID for all interfaces.

Mode	Global Config	
Command History	Version 2.5.1	Deprecated. Removed from CLI

Related Commands	tagged	Configure a tagged interface in the selected VLAN.
	untagged	Configure an untagged interface in the selected VLAN.

vlan port tagging all

This command sets the tagging behavior for all interfaces in a VLAN to enabled.

Mode	Global Config	
Command History	Version 2.5.1	Deprecated. Removed from CLI
Related Commands	tagged	Configure a tagged interface in the selected VLAN.
	untagged	Configure an untagged interface in the selected VLAN.

vlan port untagging all

This command sets the tagging behavior for all interfaces in a VLAN to disabled so that traffic is transmitted as untagged frames.

Mode	Global Config	
Command History	Version 2.5.1	Deprecated. Removed from CLI
Related Commands	tagged	Configure a tagged interface in the selected VLAN.
	untagged	Configure an untagged interface in the selected VLAN.

vlan protocol group

This command adds a protocol-based VLAN group to the system. The *groupname* is a character string of 1 to 16 characters. When it is created, the protocol group is assigned a unique number that will be used to identify the group in subsequent commands.

Syntax	vlan protocol group <i>groupname</i>	
Mode	Global Config	
Command History	Version 2.5.2	Unsupported: not tested in 2.5.2
	Version 2.5.1	Unsupported: not tested in 2.5.1
Related Commands	vlan protocol group add protocol	Add the named protocol to the protocol-based VLAN identified by <i>groupid</i> .
	vlan protocol group remove	Remove the protocol-based VLAN group that is identified by the <i>groupid</i> .
	protocol group	Attach a group ID to the selected VLAN.

vlan protocol group add protocol

This command adds the named *protocol* to the protocol-based VLAN identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command will fail and the protocol will not be added to the group. The possible values for protocol are ip, arp, and ipx.

The **no** version of this command removes the *protocol* from this protocol-based VLAN group that is identified by this *groupid*. The possible values for protocol are ip, arp, and ipx.

Syntax	[no] vlan protocol group add protocol <i>groupid protocol</i>	
Default	None	
Mode	Global Config	
Command History	Version 2.5.2	Unsupported: not tested in 2.5.2
	Version 2.5.1	Unsupported: not tested in 2.5.1
Related Commands	vlan protocol group	Adds a protocol-based VLAN group to the system.
	vlan protocol group remove	Remove the protocol-based VLAN group that is identified by the <i>groupid</i> .
	protocol group	Attach a group ID to the selected VLAN.

vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by the *groupid*.

Syntax	vlan protocol group remove <i>groupid</i>	
Mode	Global Config	
Command History	Version 2.5.2	Unsupported: not tested in 2.5.2
	Version 2.5.1	Unsupported: not tested in 2.5.1
Related Commands	vlan protocol group	Adds a protocol-based VLAN group to the system.
	vlan protocol group add protocol	Add the named protocol to the protocol-based VLAN identified by <i>groupid</i> .
	protocol group	Attach a group ID to the selected VLAN.

vlan pvid

This command changes the VLAN ID per interface.

The **no** version of this command sets the VLAN ID per interface to 1.

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.5.1	Removed from CLI
	Version 2.3	Deprecated
Related Commands	untagged	Adds a Layer 2 interface to the selected VLAN as an untagged interface.

vlan tagging

This command sets tagging to enabled for the selected interface in a specified VLAN.

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.5.1	Removed from CLI
	Version 2.3	Deprecated
Related Commands	tagged	Sets tagging to enabled for a specified interface in the selected VLAN.
	untagged	Adds a Layer 2 interface to the selected VLAN as an untagged interface.

vlan untagging

This command sets tagging to disabled for the selected interface in a specified VLAN.

Mode	Interface Config	
Command History	Version 2.5.1	Removed from CLI
	Version 2.3	Deprecated.
Related Commands	untagged	Adds a Layer 2 interface to the selected VLAN as an untagged interface.

Protected-Port (PVLAN) Commands

The commands in this section are:

- [show interfaces switchport on page 148](#)
- [show switchport protected on page 148](#)
- [switchport protected \(Global Config\) on page 149](#)
- [switchport protected \(Interface Config\) on page 150](#)

This section describes commands you use to configure and view protected ports. Ports are unprotected by default. A Private Edge VLAN, also referred to as a “protected VLAN” — PVLAN), prevents ports designated as such in the specified protected port group from forwarding traffic to each other even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports.

show interfaces switchport

The output from this command displays the status of the interface (protected/unprotected) under the *groupid*.

Syntax `show interfaces switchport unit/slot/port groupid`

For *groupid*, enter a number in the range 0–2, as the number that identifies the protected port group.

Mode User Exec; Privileged Exec

Command History

Version 2.5.1	Introduced
---------------	------------

Example **Figure 7-49. Example of Output from the show switchport protected Command**

```
(Force10) #show interfaces switchport 1/0/10 0
Name..... willstest
Protected Port ..... False

pm-s50-1 #show interfaces switchport 1/0/10 1
Name.....
Protected Port ..... True in Group 1

(Force10) #
```

Field Descriptions **Name**—The name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Protected—Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group *groupid*.

Related Commands

switchport protected (Global Config)	Creates a protected port group.
show switchport protected	Displays current memory usage in bytes in tabular format.

show switchport protected

The output from this command displays the status of all interfaces, including protected and unprotected interfaces.


Syntax `show switchport protected groupid`

For *groupid*, enter a number in the range 0–2, as the number that identifies the protected port group.

Mode	User Exec; Privileged Exec
Command History	Version 2.5.1 Introduced
Example	<p>Figure 7-50. Example of Output from the show switchport protected Command</p> <pre>(Force10) #show switchport protected 0 Name.....willstest Member Ports : 1/0/10</pre>
Field Descriptions	<p>Name—An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.</p> <p>Member Ports—List of ports, which are configured as protected for the group identified with <i>groupid</i>. If no port is configured as protected for this group, this field is blank.</p>
Related Commands	<p>switchport protected (Global Config) Create a protected port group that includes all ports on the switch</p>

switchport protected (Global Config)

Use this command to create and name a protected port group that includes all ports on the switch.

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

Syntax	[no] switchport protected <i>groupid</i> [name <i>name</i>]				
Parameters	<table border="1"> <tr> <td><i>groupid</i></td> <td>Identify the set of protected ports. Range: 0–2</td> </tr> <tr> <td>name <i>name</i></td> <td>(OPTIONAL) Assign a name to the protected port group. Default: blank Range: up to 32 alphanumeric characters long, including blanks</td> </tr> </table>	<i>groupid</i>	Identify the set of protected ports. Range: 0–2	name <i>name</i>	(OPTIONAL) Assign a name to the protected port group. Default: blank Range: up to 32 alphanumeric characters long, including blanks
<i>groupid</i>	Identify the set of protected ports. Range: 0–2				
name <i>name</i>	(OPTIONAL) Assign a name to the protected port group. Default: blank Range: up to 32 alphanumeric characters long, including blanks				
	Use the no switchport protected command to remove a protected port group. Alternatively, use the name <i>name</i> pair to remove the name from the group.				
Default	unprotected				
Mode	Global Config				
Command History	Version 2.5.1 Introduced				

**Related
Commands**

show switchport protected	Displays current memory usage in bytes in tabular format.
switchport protected (Interface Config)	Add ports to a protected port group.

switchport protected (Interface Config)

Use this command to add the selected interface to a protected port group. You can only configure an interface as protected in one group.



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

Syntax [no] switchport protected *groupid*

Use the `no switchport protected` command to configure the selected port as unprotected. The *groupid* parameter identifies the set of protected ports to which this interface is assigned.

Parameters

<i>groupid</i>	Identifies the set of protected ports to which this interface is assigned. Range: 0 – 2
----------------	--

Default unprotected

Mode Interface Config

**Command
History**

Version 2.5.1	Introduced
---------------	------------

**Related
Commands**

show switchport protected	Displays current memory usage in bytes in tabular format.
switchport protected (Global Config)	Create a protected port group that includes all ports on the switch.

VLAN-Stacking Commands



Note: The VLAN-Stacking feature was not tested in SFTOS 2.5.1 or 2.5.2, so the commands in this section are not supported, as noted in the Command History of each command.

This section provides a detailed explanation of VLAN-Stacking commands, also called *Double VLAN tagging*, *QinQ*, and *VLAN tunneling*. With this feature, you can “stack” VLANs into one tunnel and switch them through the network. The commands in this section are:

- [dvlan-tunnel l2pdu-forwarding enable](#)
- [dvlan-tunnel l2pdu-forwarding mac-address](#)
- [dvlan-tunnel ethertype on page 152](#)
- [mode dot1q-tunnel on page 152](#)

- [mode dvlan-tunnel on page 153](#)
- [show dot1q-tunnel on page 154](#)
- [show dvlan-tunnel on page 155](#)
- [show dvlan-tunnel l2pdu-forwarding on page 155](#)

dvlan-tunnel l2pdu-forwarding enable

This command is used to enable/disable the l2pdu-forwarding mode, used for BPDU tunneling.

Syntax [no] dvlan-tunnel l2pdu-forwarding enable

The no version of this command disables the l2pdu-forwarding mode.

Default Enable

Mode Global Config

Command History

Version 2.5.2	Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
Version 2.5.1	Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported
Version 2.3.1.9	Introduced

Related Commands

dvlan-tunnel l2pdu-forwarding mac-address	Set/clear the l2pdu-forwarding MAC address.
show dvlan-tunnel l2pdu-forwarding	Displays the current l2pdu tunneling configuration on the switch.
show dvlan-tunnel	Displays whether an interface is enabled for Double VLAN Tunneling, along with the system-configured etherType and detailed information about Double VLAN Tunneling for the specified interface, or a list of interfaces and their tunneling status.

dvlan-tunnel l2pdu-forwarding mac-address

This command sets/clears the l2pdu-forwarding MAC address.

Syntax [no] dvlan-tunnel l2pdu-forwarding mac-address *mac-addr*

Default 01:01:E8:00:00:00

Mode Global Config

Command History

Version 2.5.2	Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
Version 2.5.1	Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported
Version 2.3.1.9	Introduced

**Related
Commands**

dvlan-tunnel l2pdu-forwarding enable	Enable/disable the l2pdu-forwarding mode.
show dvlan-tunnel l2pdu-forwarding	Displays the current l2pdu tunneling configuration on the switch.
show dot1q-tunnel	Displays whether an interface is enabled for Double VLAN Tunneling, along with the system-configured etherType and detailed information about Double VLAN Tunneling for the specified interface, or a list of interfaces and their tunneling status.

dvlan-tunnel ethertype

This command configures the etherType for all vlan-stack (Double VLAN tagging) interfaces on the system. The setting is enabled by default, with the `vman` value. When enabled, all STP BPDUs coming in at a customer port are sent double-tagged, while BPDUs coming in at provider ports are not.

Syntax `dvlan-tunnel ethertype {802.1Q | vman | custom 0-65535}`

The etherType may have the values of `802.1Q`, `vman`, or `custom`. For `custom`, the value of the etherType must be set to a number from 0 to 65535.

The `no` version of this command configures the etherType for the specified interface to the default value.

Default `vman`

Mode Global Config; Interface Range, which is indicated by the `(conf-if-range-interface)#` prompt, such as `(conf-if-range-vlan 10-20)#`.

**Command
History**

Version 2.5.2	Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
Version 2.5.1	Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported
Version 2.3	Interface Range mode added

**Related
Commands**

interface range	Defines an interface range and accesses the Interface Range mode
show dot1q-tunnel	Displays the configured etherType and other information about Double VLAN Tunneling for a specified interface or for all interfaces.
show dvlan-tunnel l2pdu-forwarding	Displays the current l2pdu tunneling configuration present on the switch.

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled. This command performs the same function as `mode dvlan-tunnel`.

The `no` version of this command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Syntax	mode dot1q-tunnel	
Default	disabled	
Mode	Interface Config	
Command History	Version 2.5.2	Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
	Version 2.5.1	Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported
Usage Information	By default, all ports become core ports. To configure a particular port as an access port, enable DVLAN tagging in Interface Config mode for that port with this command.	
Related Commands	show dot1q-tunnel	Displays information about Double VLAN Tunneling for a specified interface or for all interfaces.
	show dvlan-tunnel l2pdu-forwarding	Displays the current l2pdu tunneling configuration present on the switch.

mode dvlan-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled. This command performs the same function as `mode dot1q-tunnel`.

The `no` version of this command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Syntax	mode dvlan-tunnel	
Default	disabled	
Mode	Interface Config; Interface Port Channel Config	
Command History	Version 2.5.2	Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
	Version 2.5.1	Modified: Added Interface Port Channel Config mode. Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported
Usage Information	By default, all ports become core ports. To configure a particular port as an access port, enable DVLAN tagging in Interface Config mode for that port with this command.	
Related Commands	show dot1q-tunnel	Displays information about Double VLAN Tunneling for a specified interface or for all interfaces.
	show dvlan-tunnel l2pdu-forwarding	Displays the current l2pdu tunneling configuration present on the switch.

show dot1q-tunnel

This command displays whether an interface is enabled for Double VLAN Tunneling, along with the system-configured etherType and detailed information about Double VLAN Tunneling for the specified interface, or a list of interfaces and their tunneling status. This command performs the same function as `show dvlan-tunnel`.

Syntax	<code>show dot1q-tunnel [interface { <i>unit/slot/port</i> all }]</code>	
Parameters	<code>interface { <i>unit/slot/port</i> all }</code>	Enter the interface keyword followed by either a specific address in the form of <i>unit/slot/port</i> or enter the word all . Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.
Mode	Privileged Exec and User Exec	
Command History	Version 2.5.2	Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
	Version 2.5.1	Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported

Usage Information The following screen capture shows the use of the three ways of using the command—without the `interface` keyword and with the keyword followed by a port number or `all`.

Example **Figure 7-51. Example of Use of show dvlan-tunnel l2pdu-forwarding Command**

```
(S50-8) >show dot1q-tunnel ?
<cr>                               Press Enter to execute the command.
interface                             Enter interface.

(S50-8) >show dot1q-tunnel
Interfaces Enabled for DVLAN Tunneling..... None

(S50-8) >show dot1q-tunnel interface 1/0/1
Interface Mode   EtherType
-----
1/0/1           Disable 802.1Q

(S50-8) >show dot1q-tunnel interface all
Interface Mode   EtherType
-----
1/0/1           Disable 802.1Q
1/0/2           Disable 802.1Q
1/0/3           Disable 802.1Q
1/0/4           Disable 802.1Q
1/0/5           Disable 802.1Q
1/0/6           Disable 802.1Q
1/0/7           Disable 802.1Q
1/0/8           Disable 802.1Q
1/0/9           Disable 802.1Q
1/0/10          Disable 802.1Q
!-----[output truncated]-----!
```

Related Commands	dvlan-tunnel ethertype	Enable/disable the l2pdu-forwarding mode.
	mode dot1q-tunnel	Enable Double VLAN Tunneling on the specified interface.
	mode dvlan-tunnel	same as above

show dvlan-tunnel

This command displays whether an interface is enabled for Double VLAN Tunneling, along with the system-configured etherType and detailed information about Double VLAN Tunneling for the specified interface, or a list of interfaces and their tunneling status. This command performs the same function as `show dot1q-tunnel`.

Syntax `show dvlan-tunnel [interface {unit/slot/port | all}]`

Parameters	<code>interface {unit/slot/port all}</code> (OPTIONAL) Enter the <code>interface</code> keyword followed by either a specific address in the form of <code>unit/slot/port</code> or enter the word <code>all</code> .
-------------------	---

Mode Privileged Exec and User Exec

Command History	Version 2.5.2 Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
	Version 2.5.1 Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported

Example **Figure 7-52. Example of Output from the show dvlan-tunnel interface Command**

```
Forcel0 #show dvlan-tunnel interface 1/0/1

Interface Mode      EtherType
-----
1/0/1      Disable 802.1Q

Forcel0 # show dvlan-tunnel interface all

Interface Mode      EtherType
-----
1/0/1      Disable 802.1Q
1/0/2      Disable 802.1Q
1/0/3      Disable 802.1Q
1/0/4      Disable 802.1Q
1/0/5      Disable 802.1Q
1/0/6      Disable 802.1Q
1/0/7      Disable 802.1Q
!-----output truncated-----!
```

Related Commands	<code>dvlan-tunnel ethertype</code> Configures the etherType for all vlan-stack (Double VLAN tagging) interfaces on the system.
	<code>mode dot1q-tunnel</code> Enable Double VLAN Tunneling on the specified interface.
	<code>mode dvlan-tunnel</code> same as above

show dvlan-tunnel l2pdu-forwarding

This command displays the current l2pdu tunneling configuration present on the switch.

Syntax `show dvlan-tunnel l2pdu-forwarding`

Mode Privileged Exec

Command History

Version 2.5.2	Unsupported: This command was not tested in SFTOS 2.5.2, so is not supported
Version 2.5.1	Unsupported: This command was not tested in SFTOS 2.5.1, so is not supported
Version 2.3.1.9	Introduced

Example**Figure 7-53. Example of Use of show dvlan-tunnel l2pdu-forwarding Command**

```
Force10 S50 #show dvlan-tunnel l2pdu-forwarding
L2Pdu-Forwarding Mode: enabled.
L2Pdu-Forwarding Mac: 01:01:E8:00:00:00
```

Related Commands

dvlan-tunnel l2pdu-forwarding enable	Enable/disable the l2pdu-forwarding mode.
dvlan-tunnel l2pdu-forwarding mac-address	Set/clear the l2pdu-forwarding MAC address.
mode dvlan-tunnel	Enable Double VLAN Tunneling on the specified interface.

Link Layer Discovery Protocol (LLDP) Commands

The IEEE 802.1AB standard defines the Link Layer Discovery Protocol (LLDP). LLDP support is new in SFTOS 2.5.1.

The commands in this chapter are:

- To clear LLDP information:
 - [clear lldp neighbors on page 159](#)
 - [clear lldp counters on page 159](#)
- To configure LLDP globally (on all ports):
 - [lldp mode \(global\) on page 160](#)
- To configure LLDP on a single port:
 - [lldp mode \(interface\) on page 161](#) (timers not supported at interface level)
 - [lldp notification on page 162](#)
 - [lldp transmit-mgmt on page 163](#)
 - [lldp transmit-tlv on page 163](#)
- To change default timers (all global):
 - [lldp hello on page 160](#)
 - [lldp multiplier on page 161](#)
 - [lldp notification-interval on page 162](#)
 - [lldp timers-reinit on page 163](#)
- To display LLDP information:
 - [show lldp interface on page 164](#)
 - [show lldp local-device on page 165](#)
 - [show lldp neighbors on page 166](#)
 - [show lldp remote-device on page 167](#)

LLDP Overview

LLDP allows a switch residing on an 802.1Q VLAN to advertise connectivity, physical description, management information, and major capabilities. The *TLV (Type/Length/Value)* information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), facilitating multi-vendor interoperability and use of standard management tools to discover and make available physical topology information for network management.

Figure 8-54 presents a diagram of the basic LLDP packet sent to a multicast MAC address. The EtherType is set to 88cc.

Figure 8-54. TLV Packet Overview

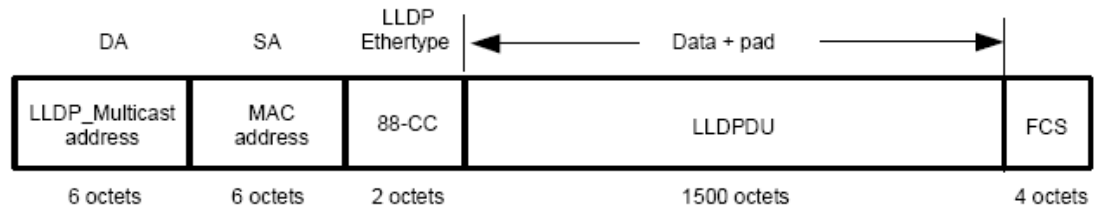


Figure 8-55 shows a more detailed diagram of the TLV sequence in the LLDPDU section of the LLDP packet, showing how TLVs are strung together in the payload of the LLDP PDU:

Figure 8-55. LLDPDU Section of the Packet

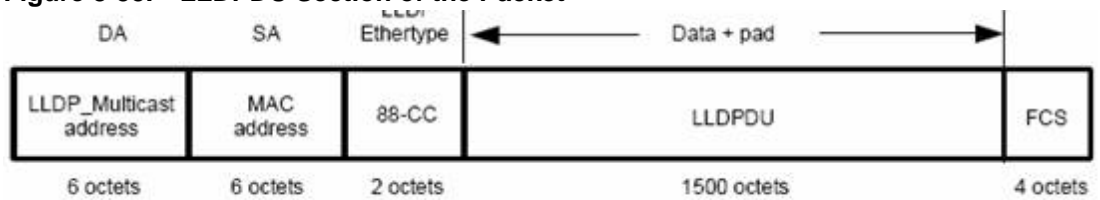
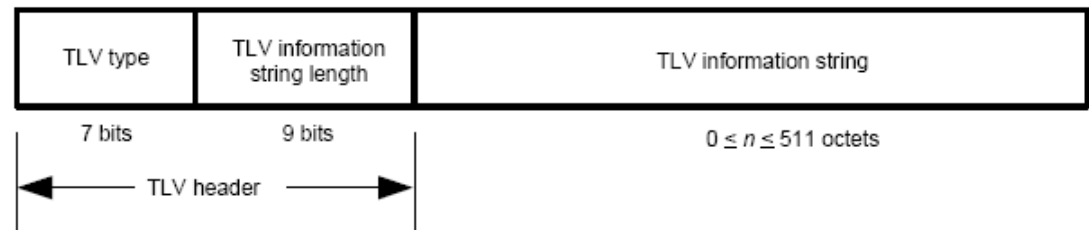


Figure 8-56 shows the structure of each TLV section, for example the Chassis ID TLV. The TLV Type and TLV Length constitute the TLV header, followed by the TLV information string.

Figure 8-56. LLDPDU Section of the LLDP Packet



SFTOS 2.5.1 supports the sending of the following optional TLVs:

- Port Description
- System Name
- System Description
- System Capabilities

LLDP Commands

The commands in this chapter are:

- [clear lldp neighbors on page 159](#)
- [clear lldp counters on page 159](#)
- [lldp hello on page 160](#)
- [lldp mode \(global\) on page 160](#)
- [lldp mode \(interface\) on page 161](#)

- [lldp multiplier on page 161](#)
- [lldp notification on page 162](#)
- [lldp notification-interval on page 162](#)
- [lldp timers-reinit on page 163](#)
- [lldp transmit-mgmt on page 163](#)
- [lldp transmit-tlv on page 163](#)
- [show lldp interface on page 164](#)
- [show lldp local-device on page 165](#)
- [show lldp neighbors on page 166](#)
- [show lldp remote-device on page 167](#)

clear lldp neighbors

Clear LLDP neighbor information.

Syntax `clear lldp neighbors [interface unit/slot/port]`

(Optional) Enter the interface *unit/slot/port* keyword and variable combination to clear LLDP information for a particular interface.

Default none

Mode Global Config

Command History

Version 2.5.1	Introduced
---------------	------------

Related Commands

clear lldp counters	Clear LLDP counter information.
lldp mode (global)	Enable/disable LLDP globally.
lldp mode (interface)	Enable/disable LLDP on a particular interface.
show lldp local-device	Display LLDP information.

clear lldp counters

Clear LLDP counter information.

Syntax `clear lldp counters [interface unit/slot/port]`

(Optional) Enter the interface *unit/slot/port* keyword and variable combination to clear LLDP counters for a particular interface.

Default none

Mode Global Config

Command History

Version 2.5.1	Introduced
---------------	------------

Related Commands

clear lldp neighbors	Clear LLDP neighbor information.
lldp mode (global)	Enable/disable LLDP globally.
lldp mode (interface)	Enable/disable LLDP on a particular interface.
show lldp local-device	Display LLDP neighbor information.

lldp hello

Use this command to set the interval, in seconds, to transmit local LLDP data (LLDPDUs).

Syntax `lldp hello interval`

Range: 1-180 seconds

Default 30 seconds

The **hello** is automatically enabled when the **lldp mode** command is executed in either the global or interface mode. If you change the *interval* value to a non-default value, it takes effect immediately. Then, if you disable LLDP, the value resets to the default.

Mode Global Config

Command History

Version 2.5.1	Introduced
---------------	------------

Related Commands

lldp mode (interface)	Enable/disable LLDP on an interface.
lldp mode (global)	Enable/disable LLDP globally.
lldp timers-reinit	Configure LLDP global timer for delay before re-initialization.
lldp multiplier	The interval multiplier to set local LLDP data TTL
lldp notification-interval	Minimum interval to send remote data change notifications
show lldp local-device	Display LLDP neighbor information.

lldp mode (global)

Enable LLDP on the switch.

Syntax `[no] lldp mode {tx | rx | both}`

Parameters

tx	Enable/Disable LLDP transmit capability.
rx	Enable/Disable LLDP receive capability.
both	Enable/Disable LLDP both transmit and receive capabilities.

Default Not enabled; when enabled, **both** is the default.

Mode Global Config

Command History	Version 2.5.1	Introduced
Related Commands	clear lldp neighbors	Clear LLDP neighbor information.
	lldp mode (interface)	Enable/disable LLDP on a selected port.
	show lldp local-device	Display LLDP neighbor information.

lldp mode (interface)

Enable LLDP on the selected port (timers not supported on one interface). Set whether the LLDP protocol is enabled on sent packets, received packets, or both.

Syntax [no] lldp mode {tx | rx | both}

Parameters	tx	Enable/Disable LLDP transmit capability.
	rx	Enable/Disable LLDP receive capability.
	both	Enable/Disable LLDP both transmit and receive capabilities.

Default Not enabled; when enabled, **both** is the default.

Mode Interface Config

Command History	Version 2.5.1	Introduced
Related Commands	clear lldp neighbors	Clear LLDP neighbor information.
	lldp mode (global)	Enable/disable LLDP globally.
	show lldp local-device	Display LLDP neighbor information.

lldp multiplier

This command sets the TTL (time to live) in local data LLDPDUs.

Syntax lldp multiplier *integer*

The *integer* parameter is the multiplier on the hello transmit interval. It sets the number of consecutive hello misses before LLDP declares the interface dead.

Range: 1–10

Default 4

The multiplier is automatically enabled when the **lldp mode** command is executed in either the global or interface mode. If you change the *integer* value to a non-default value, it takes effect immediately. Then, if you disable LLDP, the value resets to the default.

Mode Global Config

Command History	Version 2.5.1	Introduced
Related Commands	lldp hello	The interval in seconds to transmit local LLDP data
	lldp notification	Configure minimum interval to send remote data change notifications
	lldp timers-reinit	Configure LLDP global timer for delay before re-initialization.
	show lldp local-device	Display LLDP neighbor information.

lldp notification

Enable/Disable LLDP remote data change notifications.

Syntax [no] lldp notification

Use no lldp notification to disable notifications.

Default disabled

Mode Interface Config

Command History	Version 2.5.1	Introduced
Related Commands	lldp notification-interval	Configure how often the system sends remote data change notifications.
	lldp mode (global)	Enable/disable LLDP globally.
	lldp mode (interface)	Enable/disable LLDP on a selected interface.
	show lldp local-device	Display LLDP neighbor information.

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications.

Syntax lldp notification-interval *interval*

The *interval* parameter is the minimum number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default 5

The default *interval* is automatically enabled when the lldp notification command is executed. If you change the value to a non-default value, it takes effect immediately. Then, if you disable lldp notification, the value resets to the default.

Mode Global Config

Command History	Version 2.5.1	Introduced
------------------------	---------------	------------

**Related
Commands**

lldp hello	The interval in seconds to transmit local LLDP data
lldp multiplier	The interval multiplier to set local LLDP data TTL
lldp timers-reinit	Configure LLDP global timer for delay before re-initialization.
lldp notification	Display LLDP neighbor information.

lldp timers-reinit

Configure LLDP global timer for delay before re-initialization.

Syntax `lldp timers-reinit reinit-seconds`

The *reinit-seconds* parameter is the delay before re-initialization of tasks and data structure.

Default 2

Mode Global Config

**Command
History**

Version 2.5.1	Introduced
---------------	------------

**Related
Commands**

lldp hello	The interval in seconds to transmit local LLDP data
lldp multiplier	The interval multiplier to set local LLDP data TTL
lldp notification	Minimum interval to send remote data change notifications

lldp transmit-mgmt

Include/Exclude LLDP management address TLV.

Syntax `lldp transmit-mgmt`

Mode Interface Config

**Command
History**

Version 2.5.1	Introduced
---------------	------------

**Related
Commands**

lldp hello	The interval in seconds to transmit local LLDP data
lldp multiplier	The interval multiplier to set local LLDP data TTL
lldp notification	Minimum interval to send remote data change notifications

lldp transmit-tlv

Specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs.

Syntax `[no] lldp transmit-tlv [port-desc | sys-cap | sys-desc | sys-name]`

Parameters	port-desc	Include/Exclude LLDP port description TLV (the description configured for the transmitting port using the description command within the Interface Config mode).
	sys-cap	Include/Exclude LLDP system capabilities TLV (general info about this switch, e.g. 'switch, router'; not configurable).
	sys-desc	Include/Exclude LLDP system description TLV (the system description that also appears in show run ; not configurable).
	sys-name	Include/Exclude LLDP system name TLV (the system name as configured globally by the snmp-server name command).
Default	not enabled	
Default	2	
Mode	Interface Config	
Command History	Version 2.5.1	Introduced
Related Commands	lldp hello	The interval in seconds to transmit local LLDP data
	lldp multiplier	The interval multiplier to set local LLDP data TTL
	lldp notification	Minimum interval to send remote data change notifications
	show running-config	Display current settings with values that differ from the default value.

show lldp interface

Display LLDP configuration for all interfaces.

Syntax show lldp interface {all | *unit/slot/port*}. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Parameters	interface <i>unit/slot/port</i>	For a particular interface, enter its ID in <i>unit/slot/port</i> format.
	all	Enter the keyword all for all interfaces.
Default	none	
Mode	Privileged Exec	
Command History	Version 2.5.1	Introduced

Example Figure 8-57. Example Output from show lldp interface Commands

```

Force10 #show lldp interface 1/0/1
LLDP Interface Configuration

Interface  Link      Transmit  Receive   Notify    TLVs      Mgmt
-----  -
1/0/1     Down     Disabled  Disabled  Disabled  -----  N

TLV Codes: 0- Port Description, 1- System Name
           2- System Description, 3- System Capabilities

Force10 #show lldp interface all
LLDP Interface Configuration

Interface  Link      Transmit  Receive   Notify    TLVs      Mgmt
-----  -
1/0/1     Down     Disabled  Disabled  Disabled  -----  N
1/0/2     Down     Disabled  Disabled  Disabled  -----  N
1/0/3     Down     Disabled  Disabled  Disabled  -----  N
1/0/4     Down     Disabled  Disabled  Disabled  -----  N
1/0/5     Down     Disabled  Disabled  Disabled  -----  N
-----!output truncated!-----

```

Related Commands

lldp mode (global)	Enable/disable LLDP globally.
lldp mode (interface)	Enable/disable LLDP on a selected interface.
clear lldp neighbors	Clear LLDP neighbor information.

show lldp local-device

Display LLDP configuration for all interfaces.

Syntax `show lldp local-device {all | unit/slot/port}`. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Parameters	<code>interface <i>unit/slot/port</i></code>	For a particular interface, enter its ID in <i>unit/slot/port</i> format.
	<code>all</code>	Enter the keyword all for all interfaces.

Default none

Mode Privileged Exec

Command History	Version 2.5.1	Introduced

Example Figure 8-58. Example Output from show lldp interface Commands

```

Force10 #show lldp interface 1/0/1
LLDP Interface Configuration

Interface  Link      Transmit  Receive   Notify    TLVs      Mgmt
-----  -
1/0/1     Down     Disabled  Disabled  Disabled  -----  N

TLV Codes: 0- Port Description,    1- System Name
            2- System Description,  3- System Capabilities

Force10 #show lldp interface all
LLDP Interface Configuration

Interface  Link      Transmit  Receive   Notify    TLVs      Mgmt
-----  -
1/0/1     Down     Disabled  Disabled  Disabled  -----  N
1/0/2     Down     Disabled  Disabled  Disabled  -----  N
1/0/3     Down     Disabled  Disabled  Disabled  -----  N
1/0/4     Down     Disabled  Disabled  Disabled  -----  N
1/0/5     Down     Disabled  Disabled  Disabled  -----  N
-----!output truncated!-----

```

**Related
Commands**

lldp mode (global)	Enable/disable LLDP globally.
lldp mode (interface)	Enable/disable LLDP on a selected interface.
clear lldp neighbors	Clear LLDP neighbor information.

show lldp neighbors

Display LLDP statistics.

Syntax `show lldp neighbors {all | interface unit/slot/port}` In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Parameters	<code>interface <i>unit/slot/port</i></code>	For a particular interface, enter its ID in <i>unit/slot/port</i> format.
	<code>all</code>	Retrieve information for the system.

Default none

Mode Privileged Exec

Command History	Version 2.5.1	Introduced
------------------------	---------------	------------

Example Figure 8-59. Example Output from show lldp neighbors Commands

```
(S50) #show lldp neighbors interface 1/0/1
Local Intf   Dead Interval   Remote Intf   ChassisID   Tx   Rx
1/0/1       24              2/0/3        S50-2       123  23

S50# show lldp neighbors interface 1/0/2 detail
Local Interface: 1/0/2      Remote Interface: 2/0/4
Dead Interval: 14 seconds   Tx: 51           Rx: 224
Remote Chassis ID: 2
Remote Interface Description: Interface Description
System Name: S50-2
System Description: Best Ethernet Switch
System Capabilities: Router, Switch
Software Version: 2.5.1     Hardware Version:
IPv4 Address: 10.1.1.1     IPv6 Address: 2000::1   Vlan: 10
Speed & Duplex: 1000 Mbps Full
PoE Capable: No
```

Related Commands	lldp mode (global)	Enable/disable LLDP globally.
	lldp mode (interface)	Enable/disable LLDP on a selected interface.
	clear lldp neighbors	Clear LLDP neighbor information.

show lldp remote-device

Display LLDP configuration for all interfaces.

Syntax show lldp remote-device {all | *unit/slot/port*}. In an SVL system, the [fdbid/all] parameter is not used and will be ignored if entered.

Parameters	<i>interface unit/slot/port</i>	For a particular interface, enter its ID in <i>unit/slot/port</i> format.
	all	Enter the keyword all for all interfaces.

Default none

Mode Privileged Exec

Command History	Version 2.5.1	Introduced

Example Figure 8-60. Example Output from show lldp interface Commands

```

Force10 #show lldp interface 1/0/1
LLDP Interface Configuration

Interface  Link      Transmit  Receive   Notify    TLVs      Mgmt
-----  -
1/0/1     Down     Disabled  Disabled  Disabled  -----  N

TLV Codes: 0- Port Description, 1- System Name
            2- System Description, 3- System Capabilities

Force10 #show lldp interface all
LLDP Interface Configuration

Interface  Link      Transmit  Receive   Notify    TLVs      Mgmt
-----  -
1/0/1     Down     Disabled  Disabled  Disabled  -----  N
1/0/2     Down     Disabled  Disabled  Disabled  -----  N
1/0/3     Down     Disabled  Disabled  Disabled  -----  N
1/0/4     Down     Disabled  Disabled  Disabled  -----  N
1/0/5     Down     Disabled  Disabled  Disabled  -----  N
-----!output truncated!-----

```

**Related
Commands**

lldp mode (global)	Enable/disable LLDP globally.
lldp mode (interface)	Enable/disable LLDP on a selected interface.
clear lldp neighbors	Clear LLDP neighbor information.

System Logs

This chapter provides a detailed explanation of the following syslog commands:

- [logging buffered on page 169](#)
- [logging buffered wrap on page 170](#)
- [logging cli-command on page 170](#)
- [logging console on page 170](#)
- [logging facility on page 171](#)
- [logging history on page 172](#)
- [logging host on page 172](#)
- [logging persistent on page 173](#)
- [logging port on page 173](#)
- [logging syslog on page 173](#)
- [show logging on page 174](#)
- [show logging eventlog on page 175](#)
- [show logging history on page 176](#)
- [show logging hosts on page 177](#)
- [show logging traplogs on page 177](#)

See also general management “show” commands in the management chapter, [System Management Commands on page 35](#) and the RMON monitoring commands in [RMON Commands on page 261](#).

logging buffered

This command enables logging of the in-memory log to RAM and any other enabled destination, including the console and any enabled syslog server.

Syntax `ge::ao:urVtEsE.[severitylevel]`

The *severitylevel* value is specified through one of the following keywords or the keyword’s representative integer, as shown here: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Use `no logging buffered` to disable logging to RAM.

Default disabled; critical

Mode Global Config

**Related
Commands**

logging buffered wrap	Enables wrapping of in-memory logging when full capacity is reached.
logging cli-command	Enables logging to the System Log of all Command Line Interface (CLI) commands issued on the system.
logging console	Enables logging of System log messages to the console.
logging host	Configures mirroring of System log messages to a syslog server.
logging history	Specify which messages and how many are logged to the SFTOS logging history table and through SNMP.
show logging	Displays buffered logging (the System log).

logging buffered wrap

This command enables wrapping of in-memory logging when full capacity is reached. Otherwise when full capacity is reached, logging stops.

Syntax logging buffered wrap

Use `no logging buffered wrap` to disable wrapping of in-memory logging and to configure logging to stop when full capacity is reached.

Default wrap

Mode Privileged Exec

logging cli-command

This command enables logging to the System Log of all Command Line Interface (CLI) commands issued on the system.

Syntax [no] logging cli-command

Default enabled

Mode Privileged Exec

logging console

This command enables logging of System log messages to the console.

Syntax logging console [*severitylevel*]

The *severitylevel* value is specified through one of the following keywords or the keyword's representative integer, as shown here: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7). Note that the severity level set here does not change the severity level set for the System log messages saved in RAM.

Use `no logging console` to disable logging to the console.

Default disabled; severity = critical

Mode Global Config

logging facility

Configure the facility type sent to Syslog servers.

Syntax `logging facility [facility-type]`

To remove to the configured value, enter `no logging facility`.

Parameters	<i>facility-type</i>	(OPTIONAL) Enter one of the following keywords. <ul style="list-style-type: none">• auth (authorization system)• cron (Cron/at facility)• 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)• syslog (Syslog process)• user (user process)• uucp (Unix to Unix copy process) The default is local7.
	<hr/>	
Defaults	local7	
Mode	CONFIGURATION	
Command History	Version 2.5.1	Introduced
	<hr/>	
Related Commands	logging buffered	Enable logging to a Syslog server.
	logging history	Specify which messages and how many are logged to the SFTOS logging history table and through SNMP.
	logging host	Configure the mirroring of system log messages to a syslog server.
	show logging history	Show the messages stored in the buffered log

logging history

This command enables logging of system messages to the SFTOS logging history table. Optionally, specify how many messages are to be saved in the SFTOS logging history table before being overwritten. This log collects the same messages as the System log.

Syntax	logging history [size size]	
	To return to the default level, enter no logging history.	
	To return to the default size, enter no logging history size.	
Parameters	size size	Specify the number of messages stored in the SFTOS logging history table. Range: 0 to 500 Default: 1 message
Defaults	4 (level = warnings); size = 1 message	
Mode	CONFIGURATION	
Command History	Version 2.5.1	Introduced
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	View information logged to the SFTOS logging history table.

logging host

Configure the mirroring of buffered log (also called a history table or system log) messages to a syslog host. Up to eight hosts can be configured. Also, use this command to modify the port or logging severity level to a configured host, or to revise or remove a host configuration.

Syntax	logging host { <i>ipaddress</i> [<i>port</i> [<i>severitylevel</i>]] reconfigure <i>host-index</i> <i>hostaddress</i> remove <i>host-index</i> }	
Parameters	<i>ipaddress</i>	Enter the IP address of the target host.
	[<i>port</i>	(OPTIONAL) Enter the UDP port on the target host.
	[<i>severitylevel</i>]]	Default: Port = 514 (OPTIONAL) Specify this value as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7). Note that the severity level set here does not change the severity level for the system log messages saved in RAM. Level = critical (2) Note: Consider entering a lower severity value, because the default of critical is a very tight filter, and your buffered log might remain empty.

reconfigure <i>host-index</i> <i>hostaddress</i>	Revise the IP address of a configured syslog host. To learn the current association of <i>host-id</i> with <i>hostaddress</i> , use the show logging hosts command. The value for <i>host-index</i> is in the Index column of the output of that command.
remove <i>host-index</i>	Remove the identified host, using <i>host-index</i> the described above.

Default UDP Port = 514; severity level = critical

Mode Global Config

**Related
Commands**

logging buffered	Enables logging of the buffered log to RAM and any other enabled destination, including the console and any enabled syslog server.
logging facility	Configure the facility type sent to syslog servers.
logging history	Specify which messages and how many are logged to the SFTOS logging history table and through SNMP.
show logging history	Show the messages stored in the buffered log.
show logging hosts	Learn the association of the host ID with the host address.

logging persistent

**Command
History**

Version 2.3	Deprecated (The event log, also called the persistent log, is always enabled. See show logging eventlog on page 175.)
-------------	--

logging port

**Command
History**

Version 2.3	Deprecated
-------------	------------

logging syslog

This command enables logging to any configured syslog server.

**Command
History**

Version 2.5.1	Deprecated. Use logging host .
---------------	--

**Related
Commands**

logging host	Configure the mirroring of system log messages to a syslog server.
------------------------------	--

show logging

This command displays the buffered log (the in-memory log).

Syntax show logging

Mode Privileged Exec

Example **Figure 9-61. Sample Output from the show logging Command**

```
Force10-S50 #show logging
Syslog Logging           : enabled
CLI Command Logging     : disabled
Console Logging        : disabled
Buffered (In-Memory) Logging : level debug, 305807 Messages Logged
Buffered Logging Wrapping Behavior : On
Logging Host List Empty

<189> DEC 08 16:39:59 10.11.130.247-1 TRAPMGR[194961496]: traputil.c(661) 305807
%% Link Up: LAG- 1
<189> DEC 08 16:39:59 10.11.130.247-1 TRAPMGR[194961496]: traputil.c(661) 305806
%% Link Down: LAG- 1
<189> DEC 08 16:39:59 10.11.130.247-1 TRAPMGR[194961496]: traputil.c(661) 305805
%% Link Down: LAG- 1
<189> DEC 08 16:39:59 10.11.130.247-1 TRAPMGR[194961496]: traputil.c(661) 305804
%% Link Down: LAG- 1
<189> DEC 08 16:39:57 10.11.130.247-1 TRAPMGR[194961496]: traputil.c(661) 305803
%% Link Up: 1/0/36
<189> DEC 08 16:39:56 10.11.130.247-1 TRAPMGR[194961496]: traputil.c(661) 305802
%% Link Up: 1/0/37
<189> DEC 08 16:39:56 10.11.130.247-1 TRAPMGR[194961496]: traputil.c(661) 305801
%% Link Up: 1/0/35
<190> DEC 08 16:39:22 10.11.130.247-1 UNKN[145334272]: dot3ad_lacp.c(901) 305800
%% received default event 8a99f48
<190> DEC 08 16:39:22 10.11.130.247-1 UNKN[145334272]: dot3ad_lacp.c(901) 305799
```

Report Fields Syslog Logging—The mode for logging to configured syslog hosts, whether enabled or disabled. If set to disabled, logging stops to all syslog hosts.

CLI Command Logging—The mode for logging CLI commands, whether enabled or disabled

Console Logging—The mode for console logging, whether enabled or disabled

Buffered (In-Memory) Logging—The severity level for system logging and messages received

Buffered Logging Wrapping Behavior—The behavior of the in-memory log when faced with a log-full situation. “On” when wrapping is enabled, “Off” when not.

Logging Host List

The log messages follow the summary statistics. For details about the log message fields, see the section Displaying System Log Messages in the System Logs chapter of the *SFTOS Configuration Guide*.

Command History

Version 2.5.1	Revised. The command is revised from show logging buffered.
---------------	---

Related Commands

logging buffered	Enables logging of the system log to RAM and any other enabled destination, including the console and any enabled syslog server.
logging cli-command	Displays CLI activity in the log.
logging facility	Configure the Syslog facility, used for error messages sent to Syslog servers.
show logging eventlog	Displays the persistent event log.
show logging traplogs	Displays the SNMP trap log.

show logging eventlog

This command displays the event log (persistent log, error log).

Syntax show logging eventlog [*unit*]

Parameters

unit (OPTIONAL) Specify a particular stack member.

Default If the unit is not specified, the displayed event log is that of the management unit.

Mode Privileged Exec

Command History

Version 2.5.1 Modified: This command is revised from **show eventlog**.

Example Figure 9-62. Sample Output from the show logging Command

```

Force10 ##show logging eventlog

      File                               Line TaskID   Code                d  h  m  s
EVENT> bootos.c                          434 0FFFFFFE0  AAAAAAAAA          0  0  0 10
ERROR> unitmgr.c                         3325 0E14B970  00000000          0  0 11 16
EVENT> bootos.c                          434 0FFFFFFE0  AAAAAAAAA          0  0  0  9
ERROR> unitmgr.c                         3325 0E14B970  00000000          4  2 53 36
EVENT> bootos.c                          434 0FFFFFFE0  AAAAAAAAA          0  0  0  9
ERROR> unitmgr.c                         3325 0E41C9B8  00000000          0  0  7 16

```

Report Fields File—The file in which the event originated

Line—The line number of the event

Task ID—The task ID of the event

Code—The event code

Time—The time this event occurred. “d h m s” indicates the number of days (d), hours (h), minutes (m), and seconds (s) after the switch was booted that the event occurred.

Related Commands	logging buffered	Enables logging of the system log to RAM and any other enabled destination, including the console and any enabled syslog server.
	logging cli-command	Displays CLI activity in the log.
	logging facility	Configure the Syslog facility, used for error messages sent to Syslog servers.

show logging history

Show the messages stored in the buffered log — last logged, first displayed.

Syntax	show logging history <i>size</i>	
Parameters	<i>size</i>	Indicate the number of messages to be displayed. Range: 0 to 500 Default: 1 message
Defaults	1 message	
Mode	EXEC Privilege	
Command History	Version 2.5.1	Introduced
Usage Information	The output of this command is a copy of the buffered log saved locally, depending on the settings made by using the logging host and logging facility commands. Also, when the number of messages reaches the limit you set with the logging history size command, older messages are deleted from the buffered log as newer ones are added to it.	

Example **Figure 9-63. Sample Output from the show logging history Command**

```
Forcel0 #show logging history 3
Syslog History Table: 500 maximum table entries
SNMP notifications      : Enabled
<45> DEC 10 15:54:23 10.16.128.16-1 TRAPMGR[192696176]: traputil.c(661) 30 %%
Failed User Login: Unit: 1 User ID: 123user
<46> DEC 10 15:54:23 10.16.128.16-1 UNKN[192696176]: user_mgr.c(1368) 29 %% User
Login Failed for 123user
<45> DEC 10 15:54:13 10.16.128.16-1 TRAPMGR[192696176]: traputil.c(661) 28 %%
Failed User Login: Unit: 1 User ID: user123
<46> DEC 10 15:54:13 10.16.128.16-1 UNKN[192696176]: user_mgr.c(1368) 27 %% User
Login Failed for user123
<46> DEC 10 15:53:49 10.16.128.16-1 UNITMGR[192696176]: unitmgr.c(3544) 26 %%
Configuration propagation successful
```

Related Commands	logging facility	Configure the facility type sent to Syslog servers
	logging host	Configure the mirroring of system log messages to a syslog server.
	logging history	Set the amount of information to be logged to the syslog.

show logging hosts

This command displays configured logging hosts.

Syntax show logging hosts *unit*

The *unit* variable is the host index

Mode Privileged Exec

Example **Figure 9-64. Using the show logging hosts Command**

```
Force10 #show logging hosts ?
<unit> Enter switch ID in the range of 1 to 8.

Force10 #show logging hosts 1 ?
<cr> Press Enter to execute command.

Force10 #show logging hosts 1

Index IP Address      Severity  Port      Status
-----
1      192.168.77.151     critical  514      Active
```

Report Fields Index—An integer from 1 to 8, used for identifying the desired syslog host

IP Address—IP Address of the configured syslog host

Severity—The minimum severity to log to the specified address

Port—Server Port Number. This is the port on the local host from which syslog messages are sent.

Status—The state of logging to configured syslog hosts. If the status is Active, logging occurs; if Disable, no logging occurs.

**Related
Commands**

[logging history](#) Set the amount of information to be logged to the syslog.

show logging traplogs

This command displays the SNMP trap summary (number of traps since last reset and last view) and trap details.

Syntax show logging traplogs

Mode Privileged Exec

**Command
History**

Version 2.3 Modified: Replaces the **show msglog** command with the use of the keyword **traplogs**, displaying the message log maintained by the switch, including system trace information.

Report Fields

Number of Traps since last reset—The number of traps that have occurred since the last reset of this device.

Number of Traps since log last displayed—The number of traps that have occurred since the traps were last displayed. Getting the traps by any method (terminal interface display, upload file from switch, etc.) will result in this counter being cleared to 0.

Log—The sequence number of this trap.

System Up Time—The relative time since the last reboot of the switch at which this trap occurred.

Trap—The relevant information of this trap.

The log messages appear after the summary statistics. The table consists of three columns — Log (sequential number), System Up Time, and Trap.



Note: Trap log information is not retained across a switch reset.

Note: Traps are replicated in the System log, denoted by the “TRAPMGR” component name and “traputil.c” as the file name.

User Account Commands

These commands manage user accounts. The commands are divided into two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

The user account commands are:

- [disconnect on page 179](#)
- [show loginsession on page 179](#)
- [show users on page 180](#)
- [username passwd on page 180](#)
- [users snmpv3 accessmode on page 181](#)
- [users snmpv3 authentication on page 181](#)
- [users snmpv3 encryption on page 182](#)



Note: See also [Security Commands on page 183](#)

disconnect

This command closes a Telnet session. It can also close SSH sessions.

Syntax `disconnect { sessionID | all }`

Mode Privileged Exec

show loginsession

This command displays current telnet and serial port connections to the switch. It also displays SSH sessions.

Syntax `show loginsession`

Mode Privileged Exec

ID Login Session ID

Report Fields	<p>User Name—The name the user will use to login using the serial port or Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. The Read/Write user 'admin' is the only factory default.</p> <p>Connection From—IP address of the telnet client machine or EIA-232 for the serial port connection.</p> <p>Idle Time—Time this session has been idle.</p> <p>Session Time—Total time this session has been connected.</p> <p>Session Type—Source of connection—serial port, Telnet, etc.</p>
----------------------	--

show users

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges.

Syntax	show users
Mode	Privileged Exec
Report Fields	<p>User Name—The name the user will use to log in. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to eight characters, and is not case sensitive. The Read/Write user 'admin' is the only factory default.</p> <p>User Access Mode—Shows whether the operator is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the 'admin' user has Read/Write access. There can only be one Read/Write user and up to five Read Only users.</p> <p>SNMPv3 Access Mode—This field displays the SNMPv3 access mode. If the value is set to ReadWrite, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI mode.</p> <p>SNMPv3 Authentication—This field displays the authentication protocol to be used for the specified login user.</p> <p>SNMPv3 Encryption—This field displays the encryption protocol to be used for the specified login user.</p>

username passwd

This command adds a new user (account) if space permits, along with the user's password. This command replaces the users name and users passwd commands, which have been removed from SFTOS.

Syntax username *user* passwd *password*

To remove a user, use the no username *user* command.

To delete or change a password, remove and reenter the user with the new password.



Note: The 'admin' user account cannot be deleted.

Parameters	<i>user</i>	Enter a string to represent the new user's name. The name can be up to eight characters in length. The name can be comprised of alphanumeric characters, as well as the dash ('-') and underscore ('_').
	<i>password password</i>	Enter the keyword password , followed by a new password, which cannot be more than eight alphanumeric characters in length. Passwords can include special characters. As of SFTOS 2.5.1.3, the following characters are supported: , . { } . (period, comma, open bracket, close bracket, bar) Note: If a user is authorized for authentication, or encryption is enabled, the password must be at least eight alphanumeric characters in length.
Default	no password	
Mode	Global Config	
Command History	Version 2.5.1.0	Modified. Added support in password for some special characters.
Usage Information	The username and password are not case-sensitive. Six user names can be defined.	

users snmpv3 accessmode

This command specifies the SNMP v3 access privileges for the specified login user.

Syntax [no] users snmpv3 accessmode *username* [readonly | readwrite]

The *username* is the login user name for which the specified access mode applies. The default is **readwrite** for 'admin' user; **readonly** for all other users.

The **no** version of this command sets the SNMP v3 access privileges for the specified login user as **readwrite** for the 'admin' user; **readonly** for all other users. The *username* is the login user name for which the specified access mode will apply.

Default admin -- readwrite; other -- readonly

Mode Global Config

users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are **none**, **md5** or **sha**. If md5 or sha are specified, the user login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *username* is the login user name associated with the authentication protocol.

The **no** version of this command sets the authentication protocol to be used for the specified login user to **none**. The *username* is the login user name for which the specified authentication protocol will be used.

Default no authentication

Syntax users snmpv3 authentication *username* [*none* | md5 | sha]
 users snmpv3 authentication *username*

Mode Global Config

users snmpv3 encryption

This command specifies the encryption protocol to be used for the specified login user. The valid encryption protocols are **des** or **none**.

If **des** is specified, the required key may be specified on the command line. The **key** may be up to 16 characters long. If the **des** protocol is specified but a key is not provided, the user will be prompted for the key. When using the **des** protocol, the user login password is also used as the snmpv3 encryption password and therefore must be at least eight characters in length.

If **none** is specified, a key must not be provided. The *username* is the login user name associated with the specified encryption.

The **no** version of this command sets the encryption protocol to **none**. The *username* is the login user name for which the specified encryption protocol will be used.

Default no encryption

Syntax [no] users snmpv3 encryption *username* *none* | des [*key*]

Mode Global Config

Security Commands

This chapter provides a detailed explanation of the security commands available in SFTOS, presented in the following sections:

- [Port Security Commands](#)
- [Port-Based Network Access \(IEEE 802.1X\) Commands on page 187](#)
- [RADIUS Commands on page 199](#)
- [TACACS+ Commands on page 205](#)
- [Secure Shell \(SSH\) Commands on page 209](#)
- [Hypertext Transfer Protocol \(HTTP\) Commands on page 212](#)

Port Security Commands

This section contains the following commands:

- [port-security on page 183](#)
- [port-security mac-address on page 184](#)
- [port-security mac-address move on page 184](#)
- [port-security max-dynamic on page 185](#)
- [port-security max-static on page 185](#)
- [show port-security on page 186](#)
- [show port-security dynamic on page 187](#)
- [show port-security static on page 187](#)
- [show port-security violation on page 187](#)

This section describes commands you use to configure port security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.



Note: To enable the SNMP trap specific to port security, see [snmp-server enable trap violation on page 83](#).

port-security

This command enables port locking at the system level (Global Config mode) or interface level (Interface Config mode, Interface Port Channel Config, or Interface Range modes).

The `oe` version of this command disables port locking at the selected level.

Syntax	[no] port-security	
Default	Disabled	
Modes	Global Config; Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.5.1	Modified: Added Interface Port Channel Config mode.
	Version 2.3	Added Interface VLAN and Interface Range modes.
Related Commands	interface	Identifies an interface and enters the Interface Config mode.
	interface range	Defines an interface range and accesses the Interface Range mode

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses.

Syntax port-security mac-address *mac-addr 1-3965*

The no port-security mac-address *mac-addr 1-3965* command removes the MAC address from the list of statically locked MAC addresses

The value represented by *1-3965* is a VLAN ID with a range of integers from 1 to 3965.

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.5.1	Modified: Added Interface Port Channel Config mode.
	Version 2.3	Added Interface Range mode.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

port-security mac-address move

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

Syntax port-security mac-address move

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.5.1	Modified: Added Interface Port Channel Config mode.
	Version 2.3	Added Interface Range mode.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

port-security max-dynamic

This command sets the maximum of dynamically locked MAC addresses allowed on a selected interface.

Syntax port-security max-dynamic *maxvalue*

The no port-security max-dynamic command resets the maximum of dynamically locked MAC addresses allowed on a selected interface to its default value.

The *maxvalue* range is from 0 to 600.

Default 600

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.1	Modified: Added Interface Port Channel Config mode.
Version 2.3	Added Interface Range mode.

Related Commands

interface range	Define an interface range and access the Interface Range mode.
port-security max-static	Set the maximum number of statically locked MAC addresses allowed on a selected interface.

port-security max-static

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

Syntax port-security max-static *maxvalue*

Use the no port-security max-static command to reset the maximum of statically locked MAC addresses allowed on a selected interface to its default value.

The *maxvalue* range is from 0 to 20.

Default 20

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.1	Modified: Added Interface Port Channel Config mode.
Version 2.3	Added Interface Range mode

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

show port-security

This command displays the port-security settings for a particular interface or for the entire system.

Syntax show port-security [*unit/slot/port* | all]

Mode Privileged Exec

Report Fields When no parameter is entered, the one report field is:

Port Security Administration Mode—Port-locking mode for the entire system

As shown in [Figure 11-65 on page 186](#), when either the *unit/slot/port* or all parameter is entered, the report fields are:

Intf — Port number (*unit/slot/port*)

Admin Mode — Whether the interface is administratively Enabled or Disabled

Dynamic Limit—Maximum dynamically allocated MAC Addresses

Static Limit—Maximum statically allocated MAC Addresses

Violation Trap Mode—Whether violation traps are Enabled or Disabled

Example **Figure 11-65. Example of show port-security all Command Output**

```

Forcel0 #show port-security all

  Intf      Admin      Dynamic      Static      Violation
  -----  -Mode-      -Limit-      -Limit-      -Trap Mode-
1/0/1      Disabled    600          20          Disabled
1/0/2      Disabled    600          20          Disabled
1/0/3      Disabled    600          20          Disabled
1/0/4      Disabled    600          20          Disabled
1/0/5      Disabled    600          20          Disabled
1/0/6      Disabled    600          20          Disabled
1/0/7      Disabled    600          20          Disabled
1/0/8      Disabled    600          20          Disabled
1/0/9      Disabled    600          20          Disabled
1/0/10     Disabled    600          20          Disabled
1/0/11     Disabled    600          20          Disabled
1/0/12     Disabled    600          20          Disabled
1/0/13     Disabled    600          20          Disabled
1/0/14     Disabled    600          20          Disabled
1/0/15     Disabled    600          20          Disabled
1/0/16     Disabled    600          20          Disabled
1/0/17     Disabled    600          20          Disabled
1/0/18     Disabled    600          20          Disabled
--More-- or (q)uit
!--output truncated--!

```

**Related
Commands**

show port-security dynamic	Displays the dynamically locked MAC addresses for port
show port-security static	Displays the statically locked MAC addresses for port
show port-security violation	Displays the source MAC address of the last packet that was discarded on a locked port

show port-security dynamic

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

Syntax show port-security dynamic *unit/slot/port*

Mode Privileged Exec

Report Field MAC Address — MAC address of the dynamically locked MAC

show port-security static

This command displays the statically locked MAC addresses for the designated port.

Syntax show port-security static *unit/slot/port*

Mode Privileged Exec

Report Field MAC Address—MAC Address of statically locked MAC

show port-security violation

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

Syntax show port-security violation *unit/slot/port*

Mode Privileged Exec

Report Field MAC Address—MAC Address of discarded packet on locked port

Port-Based Network Access (IEEE 802.1X) Commands

This section contains the following commands:

- [authentication login on page 188](#)
- [clear dot1x statistics on page 189](#)
- [clear radius statistics on page 189](#)
- [dot1x defaultlogin on page 189](#)
- [dot1x initialize on page 189](#)
- [dot1x login on page 190](#)
- [dot1x max-req on page 190](#)
- [dot1x port-control on page 190](#)
- [dot1x port-control all on page 191](#)
- [dot1x re-authenticate on page 191](#)
- [dot1x re-authentication on page 191](#)
- [dot1x system-auth-control on page 192](#)

- [dot1x timeout on page 192](#)
- [dot1x user on page 193](#)
- [show authentication on page 193](#)
- [show authentication users on page 194](#)
- [show dot1x on page 194](#)
- [show dot1x users on page 197](#)
- [show users authentication on page 198](#)
- [users defaultlogin on page 198](#)
- [users login on page 199](#)

authentication login

This command defines a particular sequence of authentication methods to be used to allow user access and then assigns a list name to that sequence. To authenticate a user, the authentication methods will be attempted in the order specified by the list until an authentication attempt succeeds or fails.



Note: The default log-in list, named “defaultList”, included with the default configuration cannot be changed.

Syntax authentication login *listname* [*method1* [*method2* [*method3*]]]

no authentication login *listname*

The *listname* is up to 15 alphanumeric characters and is not case-sensitive. Up to 10 authentication log-in lists can be configured on the switch. When a list is created, the authentication method “local” is set as the first method by default.

When the optional parameters *method1*, and, optionally, *method2* and *method3* are used, an ordered list of the methods specified in those parameters is set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the list. The maximum number of authentication login methods is three. The possible method values are *local*, *radius*, *tacacs*, and *reject*:

- The **local** keyword indicates that the user’s locally stored ID and password are used for authentication.
- The **radius** keyword indicates that the user’s ID and password will be authenticated using a RADIUS server.
- The **tacacs** keyword indicates that the user’s ID and password will be authenticated using a TACACS+ server.
- The **reject** keyword indicates the user is never authenticated.

The **no** version of this command deletes the specified authentication login list. The attempt to delete fails if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the non configured user for any component

The login list is the default login list included with the default configuration and was not created using ‘authentication login’. The default login list cannot be deleted.

Mode	Global Config	
Related Commands	radius server host	Configure the RADIUS authentication and accounting server.
	tacacs-server host	Specify a TACACS+ server host.
	users defaultlogin	Assign the authentication login list to use for non-configured users when attempting to log in to the system.

clear dot1x statistics

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

Syntax clear dot1x statistics {*unit/slot/port* | all}

Mode Privileged Exec

clear radius statistics

This command is used to clear all RADIUS statistics.

Syntax clear radius statistics

Mode Privileged Exec

dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Syntax dot1x defaultlogin *listname*

Mode Global Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Syntax dot1x initialize *unit/slot/port*

Mode Global Config

Command History	<hr/>	
	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.

dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The user parameter must be a configured user and the listname parameter must be a configured authentication login list.

Syntax dot1x login *user listname*

Mode Global Config

dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Syntax dot1x max-req *count*

The *count* value must be in the range 1 - 10.

The **no** version of this command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Default 2

Mode Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Interface Range mode added
-------------	----------------------------

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

dot1x port-control

This command sets the authentication mode to be used on the specified port. The control mode may be one of the following.

Force-unauthorized—The authenticator PAE unconditionally sets the controlled port to unauthorized.

Force-authorized—The authenticator PAE unconditionally sets the controlled port to authorized.

Auto—The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

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

Use **no dot1x port-control** to set the authentication mode to be used on the specified port to **auto**.

Default auto

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

dot1x port-control all

This command sets the authentication mode to be used on all ports. The control mode may be one of the following.

Force-unauthorized—The authenticator PAE unconditionally sets the controlled port to unauthorized.

Force-authorized—The authenticator PAE unconditionally sets the controlled port to authorized.

Auto—The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Syntax dot1x port-control all {force-unauthorized | force-authorized | auto}

no dot1x port-control all sets the authentication mode to be used on all ports to **auto**.

Default auto

Mode Global Config

dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Syntax dot1x re-authenticate *unit/slot/port*

Mode Global Config

Command History	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.
------------------------	-------------	--

dot1x re-authentication

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

The no version of this command disables re-authentication of the supplicant for the specified port.

Syntax dot1x re-authentication

Default	disabled	
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

dot1x system-auth-control

This command is used to enable the dot1x authentication support on the switch. By default, the authentication support is disabled. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

The `no` version of this command is used to disable the dot1x authentication support on the switch.

Syntax dot1x system-auth-control

Default disabled

Mode Global Config

dot1x timeout

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

Syntax dot1x timeout {{reauth-period *seconds*} | {quiet-period *seconds*} | {tx-period *seconds*} | {supp-timeout *seconds*} | {server-timeout *seconds*}}

The `no` version of this command sets the value, in seconds, of the specified timer to its default value:

```
no dot1x timeout {reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}
```

Parameters reauth-period—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

quiet-period—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.

tx-period—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.

supp-timeout—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.

server-timeout—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default	reauth-period: 3600 seconds quiet-period: 60 seconds tx-period: 30 seconds supp-timeout: 30 seconds server-timeout: 30 seconds		
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.		
Command History	<hr/> <table><tr><td>Version 2.3</td><td>Interface Range mode added</td></tr></table> <hr/>	Version 2.3	Interface Range mode added
Version 2.3	Interface Range mode added		
Related Commands	<hr/> <table><tr><td>show dot1x</td><td>Display data on the dot1x configuration, for a specified port or all ports,</td></tr></table> <hr/>	show dot1x	Display data on the dot1x configuration, for a specified port or all ports,
show dot1x	Display data on the dot1x configuration, for a specified port or all ports,		

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *user* parameter must be a configured user.

The no version of this command removes the user from the list of users with access to the specified port or all ports.

Syntax	dot1x user <i>user</i> { <i>unit/slot/port</i> all }		
Mode	Global Config		
Related Commands	<hr/> <table><tr><td>show dot1x users</td><td>Display 802.1x port security user information for locally configured users.</td></tr></table> <hr/>	show dot1x users	Display 802.1x port security user information for locally configured users.
show dot1x users	Display 802.1x port security user information for locally configured users.		

show authentication

This command displays the ordered authentication methods for all authentication login lists.

Syntax	show authentication
Mode	Privileged Exec

Example **Figure 11-66. show authentication Command Example**

```
(Force10 ) #show authentication
Authentication Login List  Method 1      Method 2      Method 3
-----
defaultList                local        undefined    undefined
```

Report Fields Authentication Login List—This displays the authentication methods log-in list names. [Figure 11-66](#) shows only the default log-in authentication method list.

Method 1—This field displays the first method in the specified authentication login list.

Method 2—This field displays the second method in the specified authentication login list, if any.

Method 3—This field displays the third method in the specified authentication login list, if any.

**Related
Commands**

authentication login	Define authentication login lists.
--------------------------------------	------------------------------------

show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Syntax show authentication users *listname*

Mode Privileged Exec

User—This field displays the user assigned to the specified authentication login list.

Component—This field displays the component (User or 802.1x) for which the authentication login list is assigned.

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the keywords used.

Syntax show dot1x [detail *unit/slot/port* | statistics *unit/slot/port* | summary { *unit/slot/port* | all}]

Parameters	<i>detail unit/slot/port</i>	(OPTIONAL) Display the details of the configuration for the specified port.
	<i>statistics unit/slot/port</i>	(OPTIONAL) Display the statistics for the specified port.
	<i>summary { unit/slot/port all }</i>	Display the configuration summary for the specified port or all ports.
	<i>users</i>	Display user information for locally configured users. See show dot1x users on page 197

Mode Privileged Exec

Report Fields If none of the optional parameters are used, the global dot1x configuration summary is displayed, as follows:

Administrative mode—Indicates whether authentication control on the switch is enabled or disabled.

If the optional parameter **detail unit/slot/port** is used, the detailed dot1x configuration for the specified port are displayed, as follows:

Example Figure 11-67. Example of Output from the show dot1x detail Command

```
Force10 #show dot1x detail 1/0/1

Port..... 1/0/1
Protocol Version..... 1
PAE Capabilities..... Authenticator
Authenticator PAE State..... Initialize
Backend Authentication State..... Initialize
Quiet Period..... 60
Transmit Period..... 30
Supplicant Timeout..... 30
Server Timeout (secs)..... 30
Maximum Requests..... 2
Reauthentication Period..... 3600
Reauthentication Enabled..... FALSE
Key Transmission Enabled..... FALSE
Control Direction..... both
```

Port—The interface whose configuration is displayed

Protocol Version—The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.

PAE Capabilities—The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.

Authenticator PAE State—Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.

Backend Authentication State—Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.

Quiet Period—The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.

Transmit Period—The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

Supplicant Timeout—The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

Server Timeout—The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.

Maximum Requests—The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.

Reauthentication Period—The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.

Reauthentication Enabled—Indicates if reauthentication is enabled on this port. Possible values are “True” or “False”.

Key Transmission Enabled—Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.

Control Direction—Indicates the control direction for the specified port or ports. Possible values are both or in.

If the optional parameter `statistics unit/slot/port` is used, the dot1x statistics for the specified port are displayed, as follows:

Example Figure 11-68. Example of Output from the show dot1x statistics Command

```
Force10 #show dot1x statistics 1/0/1
Port..... 1/0/1
EAPOL Frames Received..... 0
EAPOL Frames Transmitted..... 0
EAPOL Start Frames Received..... 0
EAPOL Logoff Frames Received..... 0
Last EAPOL Frame Version..... 0
Last EAPOL Frame Source..... 00:00:00:00:00:00
EAP Response/Id Frames Received..... 0
EAP Response Frames Received..... 0
EAP Request/Id Frames Transmitted..... 0
EAP Request Frames Transmitted..... 0
Invalid EAPOL Frames Received..... 0
EAPOL Length Error Frames Received..... 0
```

Port—The interface whose statistics are displayed

EAPOL Frames Received—The number of valid EAPOL frames of any type that have been received by this authenticator

EAPOL Frames Transmitted—The number of EAPOL frames of any type that have been transmitted by this authenticator

EAPOL Start Frames Received—The number of EAPOL start frames that have been received by this authenticator

EAPOL Logoff Frames Received—The number of EAPOL logoff frames that have been received by this authenticator

Last EAPOL Frame Version—The protocol version number carried in the most recently received EAPOL frame.

Last EAPOL Frame Source—The source MAC address carried in the most recently received EAPOL frame

EAP Response/Id Frames Received—The number of EAP response/identity frames that have been received by this authenticator

EAP Response Frames Received—The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator

EAP Request/Id Frames Transmitted—The number of EAP request/identity frames that have been transmitted by this authenticator

EAP Request Frames Transmitted—The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator

Invalid EAPOL Frames Received—The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized

EAP Length Error Frames Received—The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized

If the optional parameter `summary { unit/slot/port | all }` is used, the dot1x configuration for the specified port or all ports are displayed, as follows:

Example **Figure 11-69. Example of Output from the show dot1x summary Command**

```
Force10 #show dot1x summary 1/0/1
-----
Operating      Reauthentication
Interface      Control Mode   Control Mode   Enabled        Port Status
-----
1/0/1          auto           auto           FALSE          Authorized

Force10 #show dot1x summary all
-----
Interface      Control Mode   Operating      Reauthentication
Control Mode   Control Mode   Control Mode   Enabled        Port Status
-----
1/0/1          auto           auto           auto           FALSE          Authorized
1/0/2          auto           auto           auto           FALSE          Authorized
1/0/3          auto           auto           auto           FALSE          Authorized
1/0/4          auto           auto           auto           FALSE          Authorized
1/0/5          auto           auto           auto           FALSE          Authorized
1/0/6          auto           auto           auto           FALSE          Authorized
1/0/7          auto           auto           auto           FALSE          Authorized
1/0/8          auto           auto           auto           FALSE          Authorized
1/0/9          auto           auto           auto           FALSE          Authorized
1/0/10         auto           auto           auto           FALSE          Authorized
1/0/11         auto           auto           auto           FALSE          Authorized
-----output truncated-----!
```

Interface—The interface whose configuration is displayed.

Control Mode—The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto

Operating Control Mode—The control mode under which this port is operating. Possible values are authorized | unauthorized

Reauthentication Enabled—Indicates whether re-authentication is enabled on this port

Port Status—Indicates if the key is transmitted to the supplicant for the specified port

show dot1x users

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

Syntax `show dot1x users unit/slot/port`

Mode Privileged Exec

Example Figure 11-70. Example of Output from the show dot1x users Command

```
Force10 #show dot1x users 1/0/1
Users
-----
admin
```

User—Users configured locally to have access to the specified port.

Related Commands

<code>dot1x user</code>	Add the specified user to the list of users with access to the specified port or all ports.
-------------------------	---

show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Syntax show users authentication

Mode Privileged Exec

Example Figure 11-71. Example Output from the show users authentication Command

```
Force10 #show users authentication
Authentication Login Lists
User      System Login  802.1x
-----
admin     defaultList   defaultList
default   tacConfig     defaultList
```

User—This field lists every user that has an authentication login list assigned.

System Login—This field displays the authentication login list assigned to the user for system login.

802.1x Port Security—This field displays the authentication login list assigned to the user for 802.1x port security.

users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Syntax users defaultlogin *listname*

Mode Global Config

users login

This command assigns the specified authentication login list to the specified user for system login. The *user* must be a configured *user* and the *listname* must be a configured login list.

If the user is assigned a login list that requires remote authentication, all user access (from all sessions) will be blocked until authentication is complete.

Note that the login list associated with the 'admin' user cannot be changed to prevent accidental lockout from the switch.

Syntax users login *user listname*

Mode Global Config

RADIUS Commands

This section contains the following commands for the Remote Authentication Dial-In User Service (RADIUS), one method for validating administration access to the switch:

- [radius accounting mode on page 199](#)
- [radius server host on page 200](#)
- [radius server key on page 201](#)
- [radius server msgauth on page 201](#)
- [radius server primary on page 201](#)
- [radius server retransmit on page 201](#)
- [radius server timeout on page 202](#)
- [show radius on page 202](#)
- [show radius accounting statistics on page 203](#)
- [show radius statistics \(authentication\) on page 204](#)

radius accounting mode

This command is used to enable the RADIUS accounting function.

The `no` version of this command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Syntax radius accounting mode

Default disabled

Mode Global Config

radius server host

Configure the RADIUS authentication and accounting server connections.

Syntax radius server host {auth | acct} *ipaddr* [*port*]

no radius server host {auth | acct} *ipaddr*

Parameters

auth	Use this keyword if you want to configure a connection to a RADIUS authentication server. See Usage, below.
acct	Use this keyword if you want to configure a connection to a RADIUS accounting server. See Usage, below.
<i>ip-addr</i>	Enter the IP address, in dotted decimal format, of the server host.
<i>port</i>	(Optional) Configure the UDP port number to use to connect to the configured RADIUS server. See Usage, below.

Usage

If the **auth** keyword is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the **no** form of the command.

If the optional **port** parameter is used with the **auth** keyword, the command will configure the UDP port number to use to connect to the configured RADIUS authentication server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The port number must lie between 1 - 65535, with 1812 being the default value.

If the **acct** keyword is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the **no** form of the command before this command succeeds. If the optional **port** parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server, then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

The **no** version of this command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the **auth** keyword is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the **acct** keyword is used, the previously configured RADIUS accounting server is removed from the configuration. The **ipaddr** parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

Mode

Global Config

Related Commands

authentication login	Define an authentication login list.
show radius	Display RADIUS servers.
users defaultlogin	Assign the authentication login list to use for non-configured users when attempting to log in to the system.

radius server key

Configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server.

Syntax radius server key {auth | acct} *ipaddr*

Depending on whether the **auth** or **acct** keyword is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 16 characters.

Mode Global Config

radius server msgauth

This command enables the message authenticator attribute for a specified server.

Syntax radius server msgauth *ipaddr*

Mode Global Config

radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Syntax radius server primary *ipaddr*

Mode Global Config

radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The *retries* value is an integer in the range of 1 to 15.

The **no** version of this command sets the maximum number of times a request packet is re-transmitted, when no response is received from the RADIUS server, to the default value, i.e. 10.

Syntax radius server retransmit *retries*
no radius server retransmit

Default	10
Mode	Global Config

radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Syntax radius server timeout *seconds*

The `no radius server timeout` command sets the timeout value to the default value, after which a request must be retransmitted to the RADIUS server if no response is received.

Default 6 seconds

Mode Global Config

show radius

This command is used to display the various RADIUS configuration items for the switch, as well as the configured RADIUS servers.

Syntax show radius [servers]

Mode Privileged Exec

Report Fields If the optional keyword `servers` is not included, the following RADIUS configuration items will be displayed:

Primary Server IP Address—Indicates the configured server currently in use for authentication

Number of configured servers—The configured IP address of the authentication server

Max number of retransmits—The configured value of the maximum number of times a request packet is retransmitted

Timeout Duration—The configured timeout value, in seconds, for request re-transmissions

Accounting Mode—Yes or No

If the optional keyword `servers` is included, the following information regarding configured RADIUS servers is displayed.

IP Address—IP Address of the configured RADIUS server

Port—The port in use by this server

Type—Primary or secondary

Secret Configured—Yes / No

show radius accounting statistics

This command is used to display the configured RADIUS accounting mode, accounting server, and the statistics for the configured accounting server.

Syntax show radius accounting [statistics *IP address*]

Mode Privileged Exec

Example **Figure 11-72. show radius accounting Command Example**

```
(Force10_S50) #show radius accounting
RADIUS Accounting Mode..... Disable
IP Address..... 1.1.1.1
Port..... 1813
Secret Configured..... NoForce10#
```

Report Fields If the optional keyword *statistics IP address* is not included, then only the accounting mode and the RADIUS accounting server details are displayed, as listed here:

Table 11-20. show radius accounting Command Example Fields

Field	Description
RADIUS Accounting Mode	Enabled or disabled
IP Address	The configured IP address of the RADIUS accounting server
Port	The port in use by the RADIUS accounting server
Secret Configured	Yes or No

If the optional keyword *statistics IP address* is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Example **Figure 11-73. show radius accounting statistics IP address Command Example**

```
(Force10_S50) #show radius accounting accounting statistics 1.1.1.1
RADIUS Accounting Server IP Address..... 1.1.1.1
Round Trip Time..... 0.00
Requests..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

Table 11-21. show radius accounting Command Example Fields

Field	Description
RADIUS Accounting Server IP Address	IP Address of the configured RADIUS accounting server
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

show radius statistics (authentication)

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Syntax show radius statistics [*IP address*]

Mode Privileged Exec

Report Fields If the IP address is not specified, then only the Invalid Server Address field is displayed. Otherwise all the following listed fields are displayed:

Invalid Server Addresses—The number of RADIUS Access-Response packets received from unknown addresses.

Server IP Address—IP address of the server.

Round Trip Time—The time interval, in hundredths of a second, between the most recent Access-Reply | Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

Access Requests—The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

Access Retransmission—The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

Access Accepts—The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.

Access Rejects—The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.

Access Challenges—The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.

Malformed Access Responses—The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.

Bad Authenticators—The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.

Pending Requests—The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.

Timeouts—The number of authentication timeouts to this server.

Unknown Types—The number of RADIUS packets of unknown types, which were received from this server on the authentication port.

Packets Dropped—The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

TACACS+ Commands

FTOS supports Terminal Access Controller Access Control System (TACACS+) as another method for administrator login authentication. This section contains these commands:

- [tacacs-server host on page 205](#)
- [tacacs-server key on page 206](#)
- [tacacs-server timeout on page 207](#)
- [key on page 207](#)
- [port on page 207](#)
- [priority on page 208](#)
- [single-connection on page 208](#)
- [show tacacs on page 208](#)
- [timeout on page 209](#)

tacacs-server host

Configure a TACACS+ server and enter into TACACS+ Configuration mode.

Syntax	<code>tacacs-server host <i>ip-address</i></code>	
	To remove a TACACS+ server host, use the <code>no tacacs-server host { <i>hostname</i> <i>ip-address</i> }</code> command.	
Parameters	<i>ip-address</i>	Enter the IP address, in dotted decimal format, of the TACACS+ server host.
Default	Not configured	
Mode	CONFIGURATION	
Usage Information	In CONFIGURATION mode, you can set several global values for all TACACS+ servers, as listed below. Successful use of the <code>tacacs-server host</code> command to identify a particular host puts you into the TACACS configuration mode for that particular host. In that mode, you can override global and default settings of those parameters. In that TACACS configuration mode, you can also use the following commands for the particular TACACS host: <code>key</code> , <code>port</code> , <code>priority</code> , <code>single-connection</code> , and <code>timeout</code>	
Related Commands	authentication login	Specify the login authentication method.
	tacacs-server key	Configure a TACACS+ key for the TACACS server.
	tacacs-server timeout	Specify a global timeout value for all TACACS+ hosts.
	port	Specify a server port number for a particular TACACS host.
	timeout	Specify the timeout value for a particular TACACS host.
	key	Specify the authentication and encryption key for all communications between the client and the particular TACACS server.
	priority	Specify the priority value for a particular TACACS server.
	show tacacs	Display settings for all or a particular TACACS server.

tacacs-server key

Configure a key for communication between a TACACS+ server and client.

Syntax	<code>tacacs-server key <i>key</i></code>	
	To delete a key, use the <code>no tacacs-server key <i>key</i></code>	
Parameters	<i>key</i>	Enter a text string, up to 127 characters long, as the clear text password. Leading spaces are ignored.
Default	Not configured.	
Command Modes	CONFIGURATION	
Usage Information	The key configured with this command must match the key configured on the TACACS+ daemon.	

Related Commands	tacacs-server host	Identify a TACACS server.
	key	Specify the authentication and encryption key for all communications between the client and a particular TACACS server.

tacacs-server timeout

Specify a global timeout value for all TACACS+ hosts.

Syntax `tacacs-server timeout timeout`

To restore the default, enter `no tacacs-server timeout`.

Parameters	<i>timeout</i>	Range: 1 to 30 seconds
-------------------	----------------	------------------------

Default 5 seconds

Mode Global Config

Related Commands	tacacs-server host	Identify a TACACS server.
	timeout	Specify the timeout value for a particular TACACS server.
	show tacacs	Display TACACS+ settings.

key

Specify the authentication and encryption key for all communications between the client and the particular TACACS server. This key must match the key configured on the server.

Syntax `key key-string`

Parameters	<i>key-string</i>	Range: 1 to 128 characters
-------------------	-------------------	----------------------------

Default If unspecified, the key-string defaults to the global value.

Command Mode TACACS Configuration

Related Commands	tacacs-server host	Identify a TACACS server.
	tacacs-server key	Specify the authentication and encryption key at a global level for communications between the client and TACACS servers.

port

Specify a server port number for a particular TACACS host.

Syntax `port port-number`

Parameters	<i>port-number</i> Range: zero (0) to 65535
-------------------	---

Default	If unspecified, the port number defaults to 49.
----------------	---

Command Mode	TACACS Configuration
---------------------	----------------------

tacacs-server host	Identify a TACACS server.
------------------------------------	---------------------------

show tacacs	Display TACACS+ settings.
-----------------------------	---------------------------

priority

Use the priority command to determine the order in which the servers will be used, with 0 being the highest priority.

Syntax	priority <i>priority</i>
---------------	--------------------------

Parameters	<i>priority</i> Range: zero (0) to 65535
-------------------	--

Default	If unspecified, the priority defaults to 0.
----------------	---

Command Mode	TACACS Configuration
---------------------	----------------------

Related Commands	tacacs-server host Identify a TACACS server.
-------------------------	--

show tacacs	Display TACACS+ settings.
-----------------------------	---------------------------

single-connection

Configure the client to maintain a single open connection with the TACACS server.

Mode	TACACS Configuration
-------------	----------------------

Command History	Version 2.5.1 Deprecated and removed
------------------------	---

Related Commands	tacacs-server host Identify a TACACS server.
-------------------------	--

show tacacs

Display configuration and status for a particular TACACS server.

Syntax	show tacacs [<i>ip-address</i>]
---------------	-----------------------------------

Parameters	<i>ip-address</i> IP address of the server host, in dotted decimal format.
-------------------	--

Command Mode	Privileged Exec
---------------------	-----------------

Example **Figure 11-74. Example of show tacacs Command Output**

```
Force10 #show tacacs
Global Timeout: 5
IP address          Port    Timeout  Priority
-----
10.10.10.226       49     Global   0
10.16.1.58         49     Global   0
Force10#
```

Command History

Version 2.5.1	Modified: Removed fields from report output — Status, Single, Connection
---------------	--

Related Commands

tacacs-server host	Identify a TACACS server.
------------------------------------	---------------------------

timeout

Specify the timeout value for a particular TACACS host.

Syntax

`timeout timeout`

Parameters

<i>timeout</i>	Range: 1 to 30 seconds
----------------	------------------------

Default

If no timeout value is specified, the global value is used.

Command Mode

TACACS Configuration

Related Commands

tacacs-server host	Identify a TACACS server.
tacacs-server timeout	Specify the authentication and encryption key for all communications between the client and the particular TACACS server.
show tacacs	Display TACACS+ settings.

Secure Shell (SSH) Commands

The commands in this section are:

- [ip ssh maxsessions on page 210](#)
- [ip ssh protocol on page 210](#)
- [ip ssh server enable on page 211](#)
- [ip ssh timeout on page 211](#)
- [show ip ssh on page 212](#)
- [sshcon maxsessions on page 212](#)
- [sshcon timeout on page 212](#)

This section provides a detailed explanation of the SSH commands. The commands are of two functional types:

- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display switch settings, statistics and other information.

ip ssh maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established.

The range is from 0 to 5.

Syntax ip ssh maxsessions 0-5

The command no ip ssh maxsessions sets the maximum number of SSH connection sessions that can be established to the default value.

Default 5

Mode Global Config

Command History

Version 2.3	Changed from sshcon maxsessions and moved from Privileged Exec mode to Global Config mode.
-------------	--

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Syntax ip ssh protocol [1] [2]

Default 1 and 2

Mode Global Config

Command History

Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.
-------------	--

ip ssh server enable

Enable SSH.

The no version of this command disables SSH.



Note: Previous to SFTOS 2.5.1, this command required keys/certificates to be generated offline before the service starts. See *s50-secure-management.pdf* at: <https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx>

Syntax	ip ssh server enable
	no ip ssh server enable
Default	disabled
Mode	Global Config
Command History	<hr/> Version 2.5.1 Modified: Removed requirement to generate keys offline. <hr/> Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode. <hr/>
Related Commands	<hr/> ip telnet server enable Enable/disable Telnet services. <hr/> ip http secure-server enable Enable/disable HTTPS services. <hr/>

ip ssh timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set.

Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Syntax	ip ssh timeout 1-160
	The time is a decimal value from 1 to 160.
	The no ip ssh timeout version of this command sets the SSH connection session timeout value, in minutes, to the default.
Default	5 (minutes)
Mode	Global Config
Command History	<hr/> Version 2.3 Changed from sshcon timeout and moved from Privileged Exec mode to Global Config. <hr/>
Related Commands	<hr/> show ip ssh This command displays the ssh settings. <hr/>

show ip ssh

This command displays the ssh settings.

Syntax	show ip ssh
Mode	Privileged Exec
Report Fields	<p>Administrative Mode—This field indicates whether the administrative mode of SSH is enabled or disabled.</p> <p>Protocol Levels—The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.</p> <p>Connections—This field specifies the current ssh connections.</p> <p>SSH Sessions Currently Active</p> <p>Max SSH Sessions Allowed</p> <p>SSH Timeout—SSH login timeout configured by ip ssh timeout command</p>


sshcon maxsessions

Command History	Version 2.3	Replaced by adunniu , GnEnnaeon
------------------------	-------------	---

sshcon timeout

Command History	Version 2.3	Replaced by ip ssh timeout .
------------------------	-------------	--

Hypertext Transfer Protocol (HTTP) Commands

 **Note:** The SFTOS Web UI is not supported in SFTOS v. 2.5.1 or 2.5.2, and the commands in this section were designed primarily to support the Web UI.

The commands in this section are:

- [ip http javamode enable on page 213](#)
- [ip http secure-port on page 213](#)
- [ip http secure-protocol on page 213](#)
- [ip http secure-server enable on page 214](#)
- [ip http server enable on page 214](#)
- [show ip http on page 215](#)

This section provides a detailed explanation of the HTTP commands. The commands are divided into the following groups:

- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display switch settings, statistics and other information.

ip http javamode enable

Enable Java mode for the Web User interface (Web UI) to SFTOS.

Syntax ip http javamode enable

Use no ip http javamode enable to disable Java mode.

Default disabled

Mode Global Config

Command History

Version 2.5.1	Unsupported: The SFTOS Web UI is not supported in v. 2.5.1 or 2.5.2.
Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.

ip http secure-port

This command is used to set the SSLT port.

Syntax ip http secure-port *portid*

The no ip http secure-port command resets the SSLT port to the default value.

The *portid* value can be from 1 to 65535.

Default 443

Mode Global Config

Command History

Version 2.5.1	Unsupported: The SFTOS Web UI is not supported in v. 2.5.1 or 2.5.2.
Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Syntax ip http secure-protocol [SSL3] [TLS1]

Default SSL3 and TLS1

Mode	Global Config	
Command History	Version 2.5.1	Unsupported: The SFTOS Web UI is not supported in v. 2.5.1 or 2.5.2.
	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode.

ip http secure-server enable

This command is used to enable the secure socket layer for secure HTTP.

The no version of this command is used to disable the secure socket layer for secure HTTP.



Note: This command requires keys/certificates to be generated offline before the service will start. See *s50-secure-management.pdf* at (log-in required): <https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx>

Syntax	[no] ip http secure-server enable	
Default	disabled	
Mode	Global Config	
Command History	Version 2.5.1	Unsupported: The SFTOS Web UI is not supported in v. 2.5.1 or 2.5.2.
	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode and added enable to the command.

ip http server enable

This command enables access to the switch through the Web User Interface (Web UI) of SFTOS. When access is enabled, the user can log in to the switch from the Web UI.

Syntax	[no] ip http server enable	
	Use no ip http server enable to disable access to the switch through the Web UI. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web UI takes effect immediately. All interfaces are affected.	
Default	enabled	
Mode	Global Config	
Command History	Version 2.5.1	Unsupported: The SFTOS Web UI is not supported in v. 2.5.1 or 2.5.2.
	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode and added enable to the command.
Related Commands	ip address (management)	Configures the IP address of the management interface.

ip http secure-server enable	Enable the secure socket layer for secure HTTP.
show ip http	Displays the HTTP settings for the switch.

show ip http

This command displays the HTTP settings for the switch.

Syntax show ip http

Mode Privileged Exec

Command History

Version 2.5.1	Unsupported: The SFTOS Web UI is not supported in v. 2.5.1 or 2.5.2.
---------------	--

Report Fields

HTTP Mode (Unsecure) — This field indicates whether basic HTTP is enabled or disabled on the switch.

HTTP Mode (Secure) — This field indicates whether the administrative mode of secure HTTP (HTTPS) is enabled or disabled on the switch.

Java Mode — This field indicates whether Java mode is enabled or disabled on the switch.

Secure Port—This field specifies the port configured for SSLT.

Secure Protocol Level—The protocol level may have the values of SSL3, TLS1, or both SSL3 and TLS1.

Example Figure 11-75. Example of show ip http Command Output

```
Force10 #show ip http
Java Mode: Disabled
HTTP Mode (Unsecure): Disabled
HTTP Mode (Secure): Disabled
Secure Port: 443
Secure Protocol Level(s): TLS1 SSL3
Force10#
```


Stacking Commands

This chapter provides a detailed explanation of the stacking commands. The commands are listed under two headings:

- [Stacking on page 217](#)
- [Slot and Card Commands on page 226](#)

See also the [copy and Dual Image Management Commands on page 119](#) in the System Configuration chapter.

Stacking

This section provides detailed explanations of the commands that manage the stacking of S-Series switches into a single virtual switch:

- [archive copy-sw on page 217](#)
- [archive download-sw on page 218](#)
- [on page 218](#)
- [movemanagement on page 219](#)
- [reload on page 219](#)
- [show stack-port on page 219](#)
- [show stack-port diag on page 220](#)
- [show switch on page 221](#)
- [show supported switchtype on page 223](#)
- [stack on page 224](#)
- [switch priority on page 225](#)
- [switch renumber on page 225](#)

archive copy-sw

This command replicates the SFTOS software image (.OPR file) from the management unit to the other switch(es) in the stack. The code is loaded on the destination system *unit*, if specified, otherwise the code is loaded on all switches in the stack. Switch(es) must be reset for the new code to start running.

Syntax sOiabEuOedl6rAs *destination-system unit*

Mode Stacking Config (prompt is “(config-stack)#”)



Note: This command must be executed only if the new unit is added to a stack that is running a different version than the management unit.

Command History	Version 2.5.1	Deprecated
Related Commands	copy	Copy software from the stack management unit to a stack member. copy {image1 image2} unit://unit/{image1 image2}

archive download-sw

This command downloads the SFTOS software image (.OPR file) to the switch. The *url* is the transfer mode. The switch must be reset for the new code to start running.

Syntax	archive download-sw <i>url</i>
Mode	Stacking Config (prompt is “(config-stack)#”)

Command History	Version 2.5.1	Deprecated
Related Commands	copy	Download software to the stack management unit. copy tftp://tftp_server_ip_address/path/filename {image1 image2}

member

This command is optional. The command is executed on the management unit to pre-configure the stacking characteristics of a switch that will join the stack.

Syntax	member <i>unit switchindex</i>
---------------	--------------------------------

The *unit* is the stack ID (from 1 to 8) to which you want to assign the switch that you are adding to the stack. The ID must be a currently unused number.

The *switchindex* is the SID number of the supported switch type that is displayed by show supported switchindex, indicating the type of the switch being preconfigured.

Use no member *unit* to remove the specified switch from the stack.



Note: The required switch index (SID) can be obtained by executing the show supported switchtype command in User Exec or Privileged Exec mode.

Mode	Stacking Config (prompt is “(config-stack)#”)
Related Commands	show supported switchtype Displays the switch index (SID) of supported switches
	stack Accesses the Stacking Config mode

movemanagement

This command moves the management unit functionality from one switch to another. The *fromunit* is the switch identifier on the current Management Unit. The *tounit* is the switch identifier on the new management unit. Upon execution, the entire stack (including all interfaces in the stack) will be unconfigured and reconfigured with the configuration on the new management unit. After the reload is complete, all stack management capability must be performed on the new management unit. To preserve the current configuration across a stack move, save the current configuration before executing the command. A stack move will cause all routes and Layer 2 addresses to be lost. This command is executed on the management unit. The administrator is prompted to confirm the management move.

- Syntax** `movemanagement fromunit tounit`
- Mode** Stacking Config (prompt is “(config-stack)#”)

reload

This command resets the entire stack or the identified [*unit*]. The administrator is prompted to confirm that the reset should proceed.

- Syntax** `sEge .[unit]`
- Mode** Privileged Exec

show stack-port

This command displays summary stack-port information.

- Syntax** `show stack-port [counters]`
- Mode** Privileged Exec

Example 2 The S50V has two expansion slots for up to four stacking ports, so this report is set up to display all four ports, as shown in [Figure 12-76](#), whether or not all are installed (in this case, only a 10G CX4 module is installed in the left-hand slot and a 2-port stacking module is installed, but it is not linked). The ports are numbered left to right as you face them on the back of the chassis.

Figure 12-76. Example of Output from the show stack-port Command on an S50V

```
Force10-S50V#show stack-port
```

Unit	Interface	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gb/s)
1	0/49	Stack	Stack	Link Down	12
1	0/50	Stack	Stack	Link Down	12
1	0/51	Ethernet	Ethernet	Link Down	10
1	0/52	Ethernet	Ethernet	Link Down	10

When the `counters` argument is not used, the report contains the following fields:

Unit—Unit

Interface—Stack port number (A or B)

Configured Stack Mode—Stack or Ethernet

Stack Mode—Stack or Ethernet

Link Status—Status of the link

Link Speed—Speed (Gb/s) of the stack port link

Example 2

The S50V has two expansion slots for up to four stacking ports, so this report is set up to display all four ports, as shown in [Figure 12-77](#), whether or not all are installed (in this case, only a 10G XFP module is installed, but it is not linked). The ports are numbered left to right as you face them on the back of the chassis.

Figure 12-77. Example of Output from the show stack-port counters Command on an S50V

```
Forcel0-S50V#show stack-port counters
```

Unit	Interface	TX			RX		
		Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors	Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors
1	0/49	0	0	0	0	0	0
1	0/50	0	0	0	0	0	0
1	0/51	0	0	0	0	0	0
1	0/52	0	0	0	0	0	0

When the `counters` argument is used, the report contains the following fields:

Unit—Unit

Interface—Stack port number (A or B)

Tx Data Rate—Transmit data rate in megabits per second on the stacking port

Tx Error Rate—Platform-specific number of transmit errors per second

Tx Total Errors—Platform-specific number of total transmit errors since power-up

Rx Data Rate—Receive data rate in megabits per second on the stacking port

Rx Error Rate—Platform-specific number of receive errors per second

Rx Total Errors—Platform-specific number of total receive errors since power-up

show stack-port diag

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

Syntax show stack-port diag

Mode Privileged Exec

Unit—Unit

Interface—Stack port number (A or B)

Diagnostic Entry1—80 character string used for diagnostics.

Diagnostic Entry—80 character string used for diagnostics.

Diagnostic Entry3—80 character string used for diagnostics.

show switch

This command displays information about all units in the stack or about a specified unit.

Syntax show switch [*unit*]

Mode User Exec; Privileged Exec

Example 1 Figure 12-78 shows the output of both show switch and show switch *unit-id* for on an S50.

Figure 12-78. Example of Output from the show switch Command on an S50

```
Forcel0 #show switch ?
<cr>                               Press enter to execute the command.
<unit>                             Enter switch ID in the range of 1 to 8.

Forcel0-S50 #show switch

Switch      Management      Preconfig      Plugged-in      Switch      Code
            Status        Model ID       Model ID        Status      Version
-----
1           Mgmt Switch   SA-01-GE-48T  SA-01-GE-48T   OK          2.5.1.0

Forcel0-S50 #show switch 1

Switch..... 1
Management Status..... Management Switch
Hardware Management Preference.... Unassigned
Admin Management Preference..... Unassigned
Switch Type..... 0x56950201
Preconfigured Model Identifier.... SA-01-GE-48T
Plugged-in Model Identifier..... SA-01-GE-48T
Switch Status..... OK
Switch Description..... Force10 48 port Gigabit S50
Expected Code Type..... 0x100b000
Detected Code Version..... F.9.15
Detected Code in Flash..... F.9.15
Serial Number..... DE4541040
Up Time..... 0 days 0 hrs 26 mins 37 secs

Forcel0-S50 #show switch 8

Switch 8 does not exist!
```

Example Figure 12-79 shows the output of both `show switch` and `show switch unit-id` for on an S50V.

Figure 12-79. Example of Output from the show switch Command on an S50V

```

Forcel0-S50V>show switch

Switch      Management      Preconfig      Plugged-in      Switch      Code
  Status      Model ID       Model ID       Status          Version
-----
1      Mgmt Switch  S50-01-GE-48T-V S50-01-GE-48T-V OK              2.5.1.1

Forcel0 #show switch ?

<cr>                Press enter to execute the command.
<unit>              Enter switch ID in the range of 1 to 8.

Forcel0-S50V>show switch 1

Switch..... 1
Management Status..... Management Switch
Hardware Management Preference.... Unassigned
Admin Management Preference..... Unassigned
Switch Type..... 0xe5040002
Preconfigured Model Identifier.... S50-01-GE-48T-V
Plugged-in Model Identifier..... S50-01-GE-48T-V
Switch Status..... OK
Switch Description..... Forcel0 S50V - 48 GE, 4 TENGIG POE
Expected Code Type..... 0x100b000
Detected Code Version..... 2.5.1
Detected Code in Flash..... 2.5.1
Serial Number..... DEF634014
Up Time..... 4 days 19 hrs 32 mins 13 secs

```

Report Fields When a unit is not specified, the fields displayed are the following:

Switch—This field displays the unit identifier assigned to the switch.

Management Status—This field indicates whether the switch is the management unit, a stack member, or the status is unassigned.

Preconfigured Model Identifier—This field displays the model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.

Plugged-In Model Identifier—This field displays the model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.

Switch Status—This field indicates the switch status. Possible values for this state are: OK, Unsupported, CodeMismatch, ConfigMismatch, or NotPresent.

Code Version—This field indicates the detected version of code on this switch.

When a unit is specified, the fields displayed are the following:

Switch—This field displays the unit identifier assigned to the switch.

Management Status—This field indicates whether the switch is the management unit a, stack member, or the status is unassigned.

Hardware Management Preference—This field indicates the hardware management preference of the switch. The hardware management preference can be disabled or unassigned.

Admin Management Preference—This field indicates the administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the management unit.

Switch Type—This field displays the 32-bit numeric switch type.

Preconfigured Model Identifier—This field displays the preconfigured model identifier for this switch. A Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.

Plugged-in Model Identifier—This field displays the plugged-in model identifier for this switch.

Switch Status—This field displays the switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, or Not Present.

Switch Description—This field displays the switch description.

Expected Code Type—This field indicates the expected code type.

Detected Code Version—This field displays the version of code running on this switch. If the switch is not present and the data is from pre-configuration, then the code version is “None”.

Detected Code in Flash—This field displays the version of code that is currently stored in FLASH memory on the switch. This code will execute after the switch is reset. If the switch is not present and the data is from pre-configuration, then the code version is “None”.

Serial Number—Serial number of the switch.

Up Time—This field displays the system up time.

**Related
Commands**

show hardware	Display inventory information for the switch.
show sysinfo	Display switch information.
show tech-support	Display a compilation of many “show” commands.
show version	Display details of the software/hardware present on the system

show supported switchtype

This command displays information about the switch types supported by the installed version of SFTOS.

Syntax show supported switchtype [*switchindex*]

The *switchindex* variable is the switch index of the switch model for which you want details. The ID is listed in the SID field of the show supported switchtype report, as shown in [Figure 12-80](#).

Mode User Exec; Privileged Exec

Example 1 **Figure 12-80. Sample Output from the show supported switchtype Command**

```
Force10-S50 #show supported switchtype

SID          Switch Model ID          Mgmt Code
-----          -----          Pref Type
1   S50-01-GE-48T-V          1     0x100b000
2   S50-01-GE-48T           1     0x100b000
3   S25-01-GE-24P           1     0x100b000
```

Report Fields When the *switchindex* variable is not entered, the report fields are as follows:

Switch Index (SID)—This field displays the index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.

Switch Model ID—This field displays the model identifier for the supported switch type.

Management Pref—This field indicates the administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the management unit.

Code Type—This field displays the code load target identifier of the switch type.

Example 2 **Figure 12-81. Sample Output from the show supported switchtype Command**

```
Force10-S50 #show supported switchtype 1
Switch Type..... 0x56950201
Model Identifier..... SA-01-GE-48T
Switch Description..... Force10 48 port Gigabit S50
Management Preference..... 1
Expected Code Type..... 0x100b000

Supported Cards:
Slot..... 0
Card Index (CID)..... 2
Model Identifier..... SA-01-10GE-2P
```

Report Fields When the *switchindex* variable is entered, the report fields are as follows:

Switch Type—This field displays the 32-bit numeric switch type for the supported switch.

Model Identifier—This field displays the model identifier for the supported switch type.

Switch Description—This field displays the description for the supported switch type.

Management Preference—Priority of the switch in management sequence

Expected Code Type—This field indicates the expected code type

Supported Cards—Slot, Card Index (CID), Model Identifier

**Related
Commands**

show supported cardtype	Displays information about all card types (expansion modules) supported in the system
---	---

stack

This command enables the user to enter Stacking Config mode—“(config-stack)#”.

Syntax stack

Mode Global Config

**Related
Commands**

copy	Download files to the switch, upload files from the switch, or copy SFTOS images from the management unit to other members of its stack.
member	Configure a switch as a member of the stack.
movemanagement	Moves the management unit functionality from one switch to another

switch priority

This command configures the ability of a switch to become the management unit in a stack.

Syntax `switch unit priority value`

The *unit* is the switch identifier.

The *value* is the preference parameter that allows the user to specify the priority of one backup switch over another. The priority range is 0 to 15. The switch with the highest priority value will be chosen to become the management unit if the active management unit fails. The switch priority defaults to the hardware management preference value 1. Switches that do not have the hardware capability to become the management unit are not eligible for management. If priority is 0, then the unit is not considered as a potential candidate to become the management unit when the current management unit fails.

Default enable

Mode Global Config

switch renumber

This command changes the switch ID for a switch in the stack.

Syntax `switch oldunit renumber newunit`

The *oldunit* is the current switch identifier on the switch whose identifier is to be changed. The *newunit* is the updated value of the switch identifier.



Caution: When you renumber the management unit, the current configuration is lost and default configuration is loaded.

Mode Global Config

**Related
Commands**

member	Pre-configures a switch as a member of the stack
movemanagement	Moves the management unit functionality from one switch to another

Slot and Card Commands

This section provides detailed explanations of the slot and card commands:

- [set slot disable on page 226](#)
- [set slot power on page 226](#)
- [show slot on page 226](#)
- [show supported cardtype on page 227](#)
- [slot on page 229](#)

set slot disable

Command History	Version 2.3	Replaced by the slot command.
------------------------	-------------	---

set slot power

Command History	Version 2.3	Replaced by the slot command.
------------------------	-------------	---

show slot

This command displays information about all the slots in the system, or, when the *unit/slot* argument is included, this command displays information for the requested slot in the specified stack member. If that slot holds a card or module, information about the contents of the slot is also displayed.

Syntax `show slot [unit/slot]`

Mode User Exec; Privileged Exec

Example **Figure 12-82. Using the show slot command**

```
Force10 #show slot
Slot      Status   Admin   Power   Configured Card      Hot   Power
          State   State   State   Model ID             Pluggable Down
-----
1/0      Full    Enable  Enable  SA-01-10GE-2P        No    No
2/0      Empty   Enable  Disable SA-01-10GE-2P        No    No
3/0      Empty   Enable  Disable SA-01-10GE-2P        No    No
```

Figure 12-82 shows three S50 switches in a stack. “Slot” 1/0 indicates with “Full” in the Status column that the unit contains a 10Gb module.

Report Fields Slot—This field displays the slot identifier in a *unit/slot* format.

Slot Status—This field indicates whether the slot is empty, full, or has encountered an error.

Admin State—This field displays the slot administrative mode as enabled or disabled.

Power State—This field displays the slot power mode as enabled or disabled.

Configured Card Model Identifier—This field displays the model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card.

Pluggable—This field indicates whether cards are pluggable or non-pluggable in the slot.

Power Down—This field indicates whether the slot can be powered down.

When the `show slot` command includes the `unit/slot` argument, the report displays the following information for the requested slot if the slot holds a module.

Report Fields Slot—This field displays the slot identifier. In a stacking environment this field is displayed in a `unit/slot` format.

Slot Status—This field indicates whether the slot is empty, full, or errored.

Admin State—This field displays the slot administrative mode as enabled or disabled.

Power State—This field displays the slot power mode as enabled or disabled.

Inserted Card Model Identifier—This field displays the model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.

Inserted Card Description—This field displays the card description. This field is displayed only if the slot is full.

Configured Card Model Identifier—This field displays the model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is preconfigured.

Configured Card Description—This field displays the card description. This field is displayed only if the slot is preconfigured.

Pluggable—This field indicates whether cards are pluggable or non-pluggable in the slot.

Power Down—This field indicates whether the slot can be powered down.

show supported cardtype

This command displays information about all card types (expansion modules) supported in the system.

Syntax show supported cardtype [*cardindex*]

Mode User Exec; Privileged Exec

Figure 12-83 shows the output from an S50, while Figure 12-84 shows the output from an S50V.

Example 1 Figure 12-83. Using the show supported cardtype Command on an S50

```

Forcel0-S50 #show supported cardtype

CID          Card Model ID
-----
2   SA-01-10GE-2P <===== catalog # of Forcel0 10G XFP fiber module for S50
3   SA-01-GE-48T  <===== catalog # of S50 model switch

Forcel0-S50#show supported cardtype 3

Card Type..... 0x56304002
Model Identifier..... S50-01-GE-48T
Card Description..... Forcel0 S50E - 48 GE, 4 TENGIG

```

Example 2 Figure 12-84. Using the show supported cardtype Command on an S50V

```

Forcel0-S50 #show supported cardtype

CID          Card Model ID
-----
3   S50-01-GE-48T <===== catalog # of S50 model switch
4   S50-01-GE-48T-V <===== catalog # of S50V model switch
5   S25-01-GE-24P <===== catalog # of S25P model switch
6   S50-01-10GE-2P <===== catalog # of 10G XFP fiber module for S50V and S25P
7   S50-01-10GE-2C <===== catalog # of CX4 module for S50V and S25P
8   S50-01-12G-2S <===== catalog # of 12G stacking module for S50V and S25P
9   S50-01-24G-1S <===== catalog # of 24G stacking module for S50V and S25P

Forcel0-S50V#show supported cardtype 6

Card Type..... 0x563042f2
Model Identifier..... Forcel0 48 Ten-Gig Card
Card Description..... Forcel0 48 10GB Card

```

Report Fields When *cardindex* is not specified, the fields are:

CID—CID stands for Card Index. This field displays the card index numbers of device types supported by the installed software. This index is used when preconfiguring a slot.

Card Model ID—This field displays the model ID for the supported device.

When *cardindex* is specified (not supported on the S50), the fields are:

Card Type—This field displays the 32-bit numeric card type for the supported device.

Model Identifier—This field displays the model identifier for the supported device.

Card Description—This field displays the description for the supported device.

Related Commands

show supported switchtype	Displays the switch index (SID) of supported switches
stack	Accesses the Stacking Config mode

slot

(This command is not usable for S-Series switches, because they do not have slots in the conventional sense.) This command configures a slot in a system.

Command History

Version 2.3	Modified: Added the disable and power options, replacing the set slot disable and set slot power commands.
-------------	--

Related Commands

show slot	Displays information about the expansion slots.
show supported cardtype	Displays information about all card types supported in the system.

DHCP Server Commands

These commands configure the Dynamic Host Configuration Protocol (DHCP) server parameters and address pools. The following commands are covered in this chapter:

- [bootfile on page 232](#)
- [clear ip dhcp binding on page 232](#)
- [clear ip dhcp server statistics on page 232](#)
- [clear ip dhcp conflict on page 232](#)
- [client-identifier on page 233](#)
- [client-name on page 233](#)
- [default-router on page 233](#)
- [dns-server on page 234](#)
- [domain-name on page 234](#)
- [hardware-address on page 234](#)
- [host on page 235](#)
- [ip dhcp bootp automatic on page 235](#)
- [ip dhcp conflict logging on page 235](#)
- [ip dhcp excluded-address on page 235](#)
- [ip dhcp filtering \(global\) on page 236](#)
- [ip dhcp filtering \(interface\) on page 236](#)
- [ip dhcp ping packets on page 236](#)
- [ip dhcp pool on page 237](#)
- [lease on page 237](#)
- [network on page 237](#)
- [netbios-name-server on page 238](#)
- [netbios-node-type on page 238](#)
- [next-server on page 238](#)
- [option on page 239](#)
- [service dhcp on page 239](#)
- [show ip dhcp binding on page 239](#)
- [show ip dhcp global configuration on page 240](#)
- [show ip dhcp pool configuration on page 240](#)
- [show ip dhcp server statistics on page 241](#)
- [show ip dhcp conflict on page 241](#)

bootfile

The command specifies the name of the default boot image for a DHCP client. The filename specifies the boot image file.

The `no` version of this command deletes the boot image name.

Syntax	<code>bootfile filename</code>
	<code>no bootfile</code>
Default	none
Mode	DHCP Pool Config

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If “*” is specified, the bindings corresponding to all the addresses are deleted. address is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Syntax	<code>clear ip dhcp binding {address *}</code>
Default	none
Mode	Privileged Exec

clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Syntax	<code>clear ip dhcp server statistics</code>
Mode	Privileged Exec

clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (*) character is used as the address parameter.

Syntax	<code>clear ip dhcp conflict {address *}</code>
Default	none
Mode	Privileged Exec

client-identifier

This command specifies the unique identifier for a DHCP client. The unique identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. Refer to the “Address Resolution Protocol Parameters” section of RFC 1700, Assigned Numbers for a list of media type codes.

The `no` version of this command deletes the client identifier.

Syntax [no] `client-identifier uniqueidentifier`

Default None

Mode DHCP Pool Config

client-name

This command specifies the name for a DHCP client. The name is a string consisting of standard ASCII characters.

The `no` version of this command removes the client name.

Syntax `client-name name`

`no client-name`

Default 8eoE

Mode DHCP Pool Config

default-router

This command specifies the default router list for a DHCP client. {*address1, address2... address8*} are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

The `no` version of this command removes the default router list.

Syntax `default-router address1 [address2...address8]`

`no default-router`

Default None

Mode DHCP Pool Config

dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

The `no` version of this command removes the DNS Server list.

Syntax	<code>dns-server <i>address1</i> [<i>address2</i>....<i>address8</i>]</code> <code>no dns-server</code>
Default	none
Mode	DHCP Pool Config

domain-name

This command specifies the domain name for a DHCP client. The domain specifies the domain name string of the client.

The `no` version of this command removes the domain name.

Syntax	<code>domain-name <i>domain</i></code>
Default	none
Mode	DHCP Pool Config

hardware-address

This command specifies the hardware address of a DHCP client.

The `hardware-address` is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format.

The `type` indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

The `no` version of this command removes the hardware address of the DHCP client.

Syntax	<code>[no] hardware-address <i>hardware-address</i> [<i>type</i>]</code>
Default	ethernet
Mode	DHCP Pool Config

host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

The prefix-length is an integer from 0 to 32.

The `no` version of this command removes the IP address of the DHCP client.

Syntax `host address [mask | prefix-length]`

`no host`

Default none

Mode DHCP Pool Config

ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

The `no` version of this command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Syntax `ip dhcp bootp automatic`

Default disable

Mode Global Config

ip dhcp conflict logging

This command enables conflict logging on the DHCP server.

The `no` version of this command disables conflict logging on the DHCP server.

Syntax `ip dhcp conflict logging`

Default enabled

Mode Global Config

ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Syntax	ip dhcp excluded-address <i>lowaddress</i> [<i>highaddress</i>] The no version of this command removes the excluded IP addresses for a DHCP client.
Default	none
Mode	Global Config

ip dhcp filtering (global)

This command enables DHCP filtering on all interfaces (globally). DHCP requests/replies will be blocked on all physical and VLAN interfaces.

Syntax	[no]ip dhcp filtering The no version of this command removes DHCP filtering globally.
Default	no filtering
Mode	Global Config

ip dhcp filtering (interface)

This command specifies the selected interface as trusted/untrusted for DHCP filtering. DHCP requests/replies will be allowed on the selected interface, overriding the global setting.

Syntax	[no] ip dhcp filtering trust The no version of this command blocks DHCP messages on the selected port.
Default	no filtering
Mode	Interface Config

ip dhcp ping packets

This command is used to specify the number in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. Setting the number of ping packets to 0 is the same as 'no ip dhcp ping packets' and will prevent the server from pinging pool addresses.

Syntax	ip dhcp ping packets <i>0,2-10</i> Use no ip dhcp ping packets to prevent the server from pinging pool addresses and will set the number of packets to 0.
Default	2
Mode	Global Config

ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP Pool Config mode.

Syntax ip dhcp pool *name*

The **no** version of this command removes the DHCP address pool. The name should be a previously configured pool name.

Default none

Mode Global Config Mode

lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client.

The **no** version of this command restores the default value of the lease time for DHCP Server.

Syntax lease {[*days* [*hours*] [*minutes*]] | [infinite]}

The overall lease time should be between 1-86400 minutes. If **infinite** is specified, lease is set for 60 days. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 1439. *Minutes* is an integer from 0 to 86399.

Default 1 (day)

Mode DHCP Pool Config

network

This command is used to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

The **no** version of this command removes the subnet number and mask.

Syntax network *networknumber* [mask | prefixlength]

no network

Default none

Mode DHCP Pool Config

netbios-name-server

This command configures Windows Internet Naming Service (WINS) name servers that are available to DHCP clients. WINS name servers map NetBIOS names to IP addresses on TCP/IP networks.

Syntax [no] netbios-name-server *address* [*address2...address8*]

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (*address1* is the most preferred server, *address2* is the next most preferred server, and so on).

Default none

Mode DHCP Pool Config

netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients.

The **no** version of this command removes the NetBIOS node type.

Syntax netbios-node-type *type*

The *type* variable specifies the NetBIOS node type. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed
- h-node—Hybrid (recommended)

Default none

Mode DHCP Pool Config

next-server

This command configures the next server in the boot process of a DHCP client.

Address is the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

The **no** version of this command removes the boot server list.

Syntax next-server *address*

no next-server

Default If the `next-server` command is not used to configure a boot server list, the DHCP Server uses inbound interface helper addresses as boot servers.

Mode DHCP Pool Config

option

The command configures DHCP Server options. *Code* specifies the DHCP option code. Ascii string specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. *Hex string* specifies hexadecimal data. In hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.

Example: `a3:4f:22:0c` / `a3 4f 22 0c` / `a34f.220c.9fed` The *address* specifies an IP address.

The `no` version of this command removes the options.

Syntax `option code {ascii string | hex string1 [string2...string8] | ip address1 [address2...address8]}`
`no option code`

Default none

Mode DHCP Pool Config

service dhcp

This command enables the DHCP server and relay agent features on the router.

The `no` version of this command disables the DHCP server and relay agent features.

Syntax `service dhcp`

Default disabled

Mode Global Config

show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Syntax `show ip dhcp binding [address]`

Mode Privileged Exec and User Exec

IP address—The IP address of the client.

Hardware Address—The MAC Address or the client identifier.

Lease expiration—The lease expiration time of the IP Address assigned to the client.

Type—The manner in which IP Address was assigned to the client.

show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Syntax show ip dhcp global configuration

Mode Privileged Exec and User Exec

Service DHCP—The field to display the status of dhcp protocol.

Number of Ping Packets—The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.

Excluded Address—The ranges of IP addresses that a DHCP server should not assign to DHCP clients.

show ip dhcp pool configuration

This command displays pool configuration. If all is specified, configuration for all the pools is displayed.

Syntax show ip dhcp pool configuration {*name* | all}

Mode Privileged Exec and User Exec

Pool Name—The name of the configured pool.

Pool Type—The pool type.

Lease Time—The lease expiration time of the IP Address assigned to the client.

DNS Servers—The list of DNS servers available to the DHCP client

Default Routers—The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Network—The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Client Name—The name of a DHCP client.

Client Identifier—The unique identifier of a DHCP client.

Hardware Address—The hardware address of a DHCP client.

Hardware Address Type—The protocol of the hardware platform.

Host—The IP address and the mask for a manual binding to a DHCP client.

show ip dhcp server statistics

This command displays DHCP server statistics.

Syntax show ip dhcp server statistics

Mode Privileged Exec and User Exec

Address Pool—The number of configured address pools in the DHCP server.

Automatic Bindings—The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.

Manual Bindings—The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.

Expired Bindings—The number of expired leases.

Malformed Bindings—The number of truncated or corrupted messages that were received by the DHCP server.

Messages Received

DHCPREQUEST—The number of DHCPREQUEST messages that were received by the server.

DHCPDECLINE—The number of DHCPDECLINE messages that were received by the server.

DHCPRELEASE—The number of DHCPRELEASE messages that were received by the server.

DHCPINFORM—The number of DHCPINFORM messages that were received by the server.

Messages Sent

DHCPOFFER— The number of DHCPOFFER messages that were sent by the server.

DHCPACK—The number of DHCPACK messages that were sent by the server.

DHCPNACK—The number of DHCPNACK messages that were sent by the server.

show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Syntax show ip dhcp conflict [*ip-address*]

Mode Privileged Exec and User Exec

IP address—The IP address of the host as recorded on the DHCP server.

Detection Method—The manner in which the IP address of the hosts were found on the DHCP Server

Detection time—The time when the conflict was found.

Time Commands

Use the commands in this chapter to configure and monitor time and date on the switch. You can manually set the system clock or use SNTP (see [SNTP Commands on page 244](#)).

- [clock time on page 243](#)
- [show clock on page 243](#)
- [sntp broadcast client poll-interval on page 244](#)
- [sntp client mode on page 245](#)
- [sntp client port on page 245](#)
- [sntp unicast client poll-interval on page 245](#)
- [sntp unicast client poll-timeout on page 246](#)
- [sntp unicast client poll-retry on page 246](#)
- [sntp server on page 246](#)
- [show sntp on page 247](#)
- [show sntp client on page 248](#)
- [show sntp server on page 248](#)

System Clock Commands

clock time

This command manually sets the system clock, configuring the date and/or time.

Syntax `clock {date/mm/yyyy | hh:mm:ss}`

Enter the date in dd/mm/yyyy format (for example, 10/01/2007 for October 1, 2007) or the time in hh:mm:ss format (for example, 22:45:00, for 10:45 P.M.).

Default If you enter only one parameter (either date or time), leaving the other parameter unchanged, the unchanged parameter continues to be based on the previous command execution.

Mode Global Config

Command History	Version 2.5.1.0	Introduced
------------------------	-----------------	------------

show clock

This command is used to display clock settings and status.

Syntax `show clock`

Mode	Privileged Exec
Command History	Version 2.5.1.0 Introduced
Example	<p>Figure 14-85. Example of Output from show clock Command</p> <pre>Force10# show clock FRI MAR 02 08:57:47 2006</pre>

SNTP Commands

This section provides a detailed explanation of the Simple Network Time Protocol (SNTP) commands. The commands are comprised of two functional groups:

- Configuration Commands configure features and options of the switch.
- Show commands display settings, statistics, and other information. For every configuration command there is a show command that displays the configuration setting.

This section describes the following commands:

- [sntp broadcast client poll-interval](#)
- [sntp client mode](#)
- [sntp client port](#)
- [sntp unicast client poll-interval](#)
- [sntp unicast client poll-timeout](#)
- [sntp unicast client poll-retry](#)
- [sntp server](#)
- [show sntp](#)
- [show sntp client](#)
- [show sntp server](#)

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 16.

Syntax `sntp broadcast client poll-interval poll-interval`

Use the `no sntp broadcast client poll-interval` version of this command to reset the poll interval for SNTP broadcast client back to its default value.

Default 6

Mode Global Config

sntp client mode

This command enables the Simple Network Time Protocol (SNTP) client, and optionally sets the mode to either broadcast or unicast.

Syntax `sntp client mode [broadcast | unicast]`

Use the `no sntp client mode` command to disable SNTP client mode.

Parameters	broadcast	SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet-wide scope.
	unicast	SNTP operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.

Default Disabled (No SNTP requests are sent from the client, nor are any received SNTP messages processed.)

Mode Global Config

sntp client port

This command sets the SNTP client port ID to a value from 1–65535.

Syntax `sntp client port portid [poll-interval]`

Parameters	<i>portid</i>	Specify the local UDP port to listen for responses/broadcasts. The allowed range is (1 to 65535). Default value is 123.
	<i>poll-interval</i>	Optionally, set the poll interval for the client in seconds, as a power of two, in the range from 6 to 10. Default value is 6. This setting is true for both unicast and broadcast poll requests. Broadcasts received prior to the expiry of this interval are discarded.

Use the `no sntp client port` command to reset the SNTP client port to its default values.

Default 123

Usage You can also set the poll interval for a unicast client with the `sntp unicast client poll-interval` command.

Mode Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 16.

Syntax `sntp unicast client poll-interval poll-interval`

Use the `no sntp unicast client poll-interval` command to reset the poll interval for SNTP unicast clients to its default.

Usage	You can also set the poll interval for an SNTP client with the <code>sntp client port</code> command.
Default	6
Mode	Global Config

sntp unicast client poll-timeout

This command sets the number of seconds to wait for an SNTP response when the client is configured in unicast mode.

Syntax `sntp unicast client poll-timeout poll-timeout`

The *poll-timeout* range is 1 to 30 seconds.

Use the `no sntp unicast client poll-timeout` command to reset the poll timeout for SNTP unicast clients to its default value.

Default 5 seconds

Mode Global Config

sntp unicast client poll-retry

This command sets the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode.

Syntax `sntp unicast client poll-retry poll-retry`

The *poll-retry* for SNTP unicast clients is an integer from 0 to 10 retries.

Use the `no sntp unicast client poll-retry` version of this command to reset the poll retry for SNTP unicast clients to its default value.

Default 1 retry

Mode Global Config

sntp server

This command configures an SNTP server connection (with a maximum of three).

Syntax `sntp server ipaddress [priority [version [portid]]]`

Parameters

<i>ipaddress</i>	Specify either the IPv4 address of the server or a DNS hostname. If DNS, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
<i>priority</i>	Optionally, specify the priority of this server entry in determining the sequence of servers to which SNTP requests will be sent. The client continues sending requests to different servers until a successful response is received or all servers are exhausted. A server entry with a priority of 1 is queried before a server with a priority of 2, and then a server with a priority of 3. If more than one server has the same priority then the requesting order follows the lexicographical ordering of the entries in this table. Allowed range is 1 to 3. Default value is 1.
<i>version</i>	If <i>priority</i> is specified, optionally identify the NTP version running on the server. Allowed range is (1 to 4). Default value is 4.
<i>portid</i>	The port ID is a value from 1–65535.

Use the `no sntp server remove ipaddress` command to delete the server from the list of SNTP servers.

Mode Global Config

show sntp

This command is used to display SNTP settings and status.

Syntax show sntp

Mode Privileged Exec

Example **Figure 14-86. show sntp Command Example**

```
Force10# show sntp
Last Update Time:                AUG 20 09:04:15 2006
Last Unicast Attempt Time:       AUG 20 09:04:15 2006
Last Attempt Status:             Success

Broadcast Count:                 0

Force10#
```

Field Descriptions

Last Update Time—Time of last clock update

Last Attempt Time—Time of last transmit query (in unicast mode).

Last Attempt Status—Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).

Broadcast Count—Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

Multicast Count—Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot

show sntp client

This command displays SNTP client settings.

Syntax show sntp client

Mode Privileged Exec

Example **Figure 14-87. show sntp client Command Example**

```
Force10# show sntp client
Client Supported Modes:          unicast broadcast
SNTP Version:                   4
Port:                           123
Client Mode:                     disabled
Force10#
```

Field Descriptions

Client Supported Modes—Supported SNTP Modes (broadcast and/or unicast)

SNTP Version—The highest SNTP version the client supports

Port—SNTP Client Port

Client Mode—Configured SNTP Client Mode

Poll Interval—If enabled, the poll interval value for SNTP clients in seconds as a power of two

Poll Timeout—If enabled, the poll timeout value in seconds for SNTP clients

Poll Retry—If enabled, the poll retry value for SNTP clients

show sntp server

This command is used to display SNTP server settings and configured servers.

Syntax show sntp server

Mode Privileged Exec

Example **Figure 14-88. show sntp server Command Example**

```
Force10# show sntp server
Server IP Address:
Server Type:                unknown
Server Stratum:              0
Server Reference Id:
Server Mode:                 Reserved
Server Maximum Entries:     3
Server Current Entries:     0
No SNTP Servers exist.
Force10#
```


**Field
Descriptions**

Server IP Address—IP address of configured SNTP server

Server Type—Address type of server

Server Stratum—Claimed stratum of the server for the last received valid packet

Server Reference ID—Reference clock identifier of the server for the last received valid packet

Server Mode—SNTP server mode

Server Max Entries—Total number of SNTP Servers allowed

Server Current Entries—Total number of SNTP configured

For each configured server:

IP Address—IP Address of configured SNTP Server

Address Type—Address Type of configured SNTP server

Priority—IP priority type of the configured server

Version—SNTP version number of the server. The protocol version used to query the server in unicast mode

Port—Server port number

Last Attempt Time—Last server attempt time for the specified server

Last Attempt Status—Last server attempt status for the server


Total Unicast Requests—Number of requests to the server

Failed Unicast Requests—Number of failed requests from server

GARP Commands

This chapter provides a detailed explanation of the General Attribute Registration Protocol (GARP) commands, including GVRP and GMRP commands. The commands are divided into two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

 **Note:** The GARP and GVRP features were available in SFTOS before version 2.5.1, but the commands were not tested in either 2.5.1 or 2.5.2, so the commands in this chapter are not supported.

The sections in this chapter are:

- [GARP Commands on page 251](#)
- [GARP VLAN Registration Protocol \(GVRP\) Commands on page 254](#)
- [GARP Multicast Registration Protocol \(GMRP\) Commands on page 257](#)

GARP Commands

The commands in this sections are:

- [set garp timer join on page 251](#)
- [set garp timer leave on page 252](#)
- [set garp timer leaveall on page 253](#)
- [show garp on page 253](#)

set garp timer join

This command sets the GVRP join time per port and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group.

This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). the value 20 centiseconds is 0.2 seconds.


Syntax nECu: sduCa,EsuTe#00
 oeunECu: sduCa,EsuTeaou

The **no** version of this command sets the GVRP join time per port and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

Default	20 centiseconds						
Mode	Interface Config, Global Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.						
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Version 2.5.2</td> <td>Unsupported: not tested in 2.5.2</td> </tr> <tr> <td>Version 2.5.1</td> <td>Added Interface Port Channel Config mode Unsupported: not tested in 2.5.1</td> </tr> <tr> <td>Version 2.3</td> <td>Interface Range mode added</td> </tr> </table>	Version 2.5.2	Unsupported: not tested in 2.5.2	Version 2.5.1	Added Interface Port Channel Config mode Unsupported: not tested in 2.5.1	Version 2.3	Interface Range mode added
Version 2.5.2	Unsupported: not tested in 2.5.2						
Version 2.5.1	Added Interface Port Channel Config mode Unsupported: not tested in 2.5.1						
Version 2.3	Interface Range mode added						
Related Commands	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">interface range</td> <td>Defines an interface range and accesses the Interface Range mode</td> </tr> </table>	interface range	Defines an interface range and accesses the Interface Range mode				
interface range	Defines an interface range and accesses the Interface Range mode						

set garp timer leave

This command sets the GVRP leave time per port. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds.


Syntax	set garp timer leave 20-600						
	Use no set garp timer leave to set the GVRP leave time per port to 60 centiseconds (0.6 seconds).						
Default	60						
	 Note: This command has an effect only when GVRP is enabled.						
Mode	Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.						
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Version 2.5.2</td> <td>Unsupported: not tested in 2.5.2</td> </tr> <tr> <td>Version 2.5.1</td> <td>Added Interface Port Channel Config mode Unsupported: not tested in 2.5.1</td> </tr> <tr> <td>Version 2.3</td> <td>Interface Range mode added</td> </tr> </table>	Version 2.5.2	Unsupported: not tested in 2.5.2	Version 2.5.1	Added Interface Port Channel Config mode Unsupported: not tested in 2.5.1	Version 2.3	Interface Range mode added
Version 2.5.2	Unsupported: not tested in 2.5.2						
Version 2.5.1	Added Interface Port Channel Config mode Unsupported: not tested in 2.5.1						
Version 2.3	Interface Range mode added						
Related Commands	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">interface range</td> <td>Defines an interface range and accesses the Interface Range mode</td> </tr> </table>	interface range	Defines an interface range and accesses the Interface Range mode				
interface range	Defines an interface range and accesses the Interface Range mode						

set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated per port. A *Leave All PDU* indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds.

Syntax set garp timer leaveall 200-6000

Use no set garp timer leaveall to set how frequently *Leave All PDUs* are generated per port to 1000 centiseconds (10 seconds).

 **Note:** This command has an effect only when GVRP is enabled.

Default 1000

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.2	Unsupported: not tested in 2.5.2
Version 2.5.1	Added Interface Port Channel Config mode Unsupported: not tested in 2.5.1
Version 2.3	Interface Range mode added

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

show garp

This command displays Generic Attributes Registration Protocol (GARP) information.

Syntax show garp

Mode Privileged Exec; User Exec

Example **Figure 15-89. Example of Using show garp Command**

```
(Forcel0#show garp
GMRP Admin Mode..... Disable
GVRP Admin Mode..... Disable
```

Field Descriptions

GMRP Admin Mode—The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.

GVRP Admin Mode—The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system

GARP VLAN Registration Protocol (GVRP) Commands

This section provides a detailed explanation of the GVRP commands:

- [gvrp adminmode enable on page 254](#)
- [gvrp interfacemode enable on page 254\]](#)
- [gvrp interfacemode enable all on page 255](#)
- [set gvrp adminmode on page 255](#)
- [set gvrp interfacemode on page 255](#)
- [set gvrp interfacemode all on page 255](#)
- [show gvrp configuration on page 255](#)

gvrp adminmode enable

This command enables GVRP globally.

Syntax gvrp adminmode enable

Use no gvrp adminmode enable to disable GVRP.

Default disabled

Mode Global Config

Command History

Version 2.5.2	Unsupported: not tested in v.2.5.2
Version 2.5.1	Unsupported: not tested in v.2.5.1
Version 2.3	Changed from set gvrp interfacemode ; revised syntax.

gvrp interfacemode enable

This command enables GVRP (GARP VLAN Registration Protocol) for a specific port.

Syntax gvrp interfacemode enable

Use no gvrp interfacemode enable to disable GVRP (GARP VLAN Registration Protocol) for a specific port. If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Default disabled

Mode Interface Config

Command History

Version 2.5.2	Unsupported: not tested in v.2.5.2
Version 2.5.1	Unsupported: not tested in v.2.5.1
Version 2.3	Changed from set gvrp interfacemode

gvrp interfacemode enable all

This command enables GVRP (GARP VLAN Registration Protocol) for all ports.

Syntax set gvrp interfacemode enable all

Use no set gvrp interfacemode enable all to disable GVRP for all ports. If GVRP is disabled, Join Time, Leave Time, and Leave All Time have no effect.

Default disabled

Mode Global Config

Command History	Version 2.5.2	Unsupported: not tested in v.2.5.2
	Version 2.5.1	Unsupported: not tested in v.2.5.1
	Version 2.3	Changed from set gvrp interfacemode all

set gvrp adminmode

Command History	Version 2.3	Changed to :bsd .,ao,e.EuEo rgE
------------------------	-------------	---

set gvrp interfacemode

This command enables GVRP (GARP VLAN Registration Protocol) for a specific port.

Mode Interface Config

Command History	Version 2.3	Changed to gvrp interfacemode enable
------------------------	-------------	--

set gvrp interfacemode all

Command History	Version 2.3	Changed to gvrp interfacemode enable all
------------------------	-------------	--

show gvrp configuration

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

Syntax show gvrp configuration {unit/slot/port | gg}

Mode Privileged Exec and User Exec

Example Figure 15-90. Example of show gvrp configuration Command

```
(Force10_S50) #show gvrp configuration 1/0/1
Interface      Join      Leave      LeaveAll      Port
                Timer      Timer      Timer          GVRP Mode
                (centisecs) (centisecs) (centisecs)
-----
1/0/1          20         60         1000          Disabled

Force10-S50 #show gvrp configuration all
Interface      Join      Leave      LeaveAll      Port
                Timer      Timer      Timer          GVRP Mode
                (centisecs) (centisecs) (centisecs)
-----
1/0/1          20         60         1000          Disabled
1/0/2          20         60         1000          Disabled
1/0/3          20         60         1000          Disabled
1/0/4          20         60         1000          Disabled
1/0/5          20         60         1000          Disabled
1/0/6          20         60         1000          Disabled
1/0/7          20         60         1000          Disabled
1/0/8          20         60         1000          Disabled
1/0/9          20         60         1000          Disabled
1/0/10         20         60         1000          Disabled
!-----output truncated-----!
```

Field Descriptions

Interface—Valid unit, slot and port number separated by forward slashes.

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

Leave Timer—Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

LeaveAll Timer—This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Port GMRP Mode—Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

Port GVRP Mode—Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

GARP Multicast Registration Protocol (GMRP) Commands

This chapter provides a detailed explanation of the GMRP commands. The commands are divided into two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

The commands in this sections are:

- [gmrp adminmode on page 257](#)
- [set gmrp adminmode on page 257](#)
- [gmrp interfacemode enable all on page 258](#)
- [set gmrp interfacemode all on page 259](#)
- [show gmrp configuration on page 259](#)
- [show mac-address-table gmrp on page 260](#)

gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system. The default value is disable.

Syntax gmrp adminmode enable

Use no gmrp adminmode enable to disable GARP Multicast Registration Protocol (GMRP) on the system.

Mode Global Config

Command History

Version 2.5.2	Unsupported: not tested in v.2.5.2
Version 2.5.1	Unsupported: not tested in v.2.5.1
Version 2.3	Changed from set gmrp adminmode . Modified syntax and moved to Global Config mode from Privileged Exec mode.

set gmrp adminmode

Command History

Version 2.3	Changed to gmrp adminmode .
-------------	------------------------------------

gmrp interfacemode enable all

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

Syntax gmrp interfacemode enable all

Use no gmrp interfacemode enable all to disable GARP Multicast Registration Protocol on all interfaces.

Default disabled

Mode Global Config

Command History

Version 2.5.2	Unsupported: not tested in v.2.5.2
Version 2.5.1	Unsupported: not tested in v.2.5.1
Version 2.3	Changed from set gmrp interfacemode all ; revised syntax.

Related Commands

show gmrp configuration	Display GARP Multicast Registration Protocol information for one or all interfaces.
gmrp interfacemode enable (LAG)	Enable GMRP on the selected LAG.

set gmrp interfacemode

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

Default disabled

Syntax set gmrp interfacemode

Use no set gmrp interfacemode to disable GARP Multicast Registration Protocol on a selected interface.

Mode Interface Config

Command History

Version 2.5.2	Unsupported: not tested in v.2.5.2
Version 2.5.1	Unsupported: not tested in v.2.5.1

Related Commands

show gmrp configuration	Display GARP Multicast Registration Protocol information for one or all interfaces.
---	---

set gmrp interfacemode all

Command History

Version 2.3

Changed to **gmrp interfacemode enable all**.

show gmrp configuration

This command displays GARP Multicast Registration Protocol information for one or all interfaces.

Syntax show gmrp configuration {*unit/slot/port* | all}

Mode Privileged Exec and User Exec

Example **Figure 15-91. Example of show gmrp configuration Command**

```
Forcel0 #show gmrp configuration 1/0/1
  Interface      Join      Leave      LeaveAll      Port
                Timer      Timer      Timer          GMRP Mode
                (centiseecs) (centiseecs) (centiseecs)
-----
1/0/1           20         60         1000          Disabled

Forcel0-S50 #show gmrp configuration all
  Interface      Join      Leave      LeaveAll      Port
                Timer      Timer      Timer          GMRP Mode
                (centiseecs) (centiseecs) (centiseecs)
-----
1/0/1           20         60         1000          Disabled
1/0/2           20         60         1000          Disabled
1/0/3           20         60         1000          Disabled
1/0/4           20         60         1000          Disabled
1/0/5           20         60         1000          Disabled
1/0/6           20         60         1000          Disabled
1/0/7           20         60         1000          Disabled
1/0/8           20         60         1000          Disabled
!-----output truncated-----!
```

Field Descriptions

Interface—This displays the *unit/slot/port* of the interface that is described in this row of the table.

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

Leave Timer—Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

LeaveAll Timer—This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Port GMRP Mode—Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

Port GVRP Mode—Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

**Related
Commands**

<code>set gmrp interfacemode</code>	Enable GARP Multicast Registration Protocol on a selected interface.
<code>gmrp interfacemode enable all</code>	Enable GARP Multicast Registration Protocol on all interfaces.

show mac-address-table gmrp

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

Syntax show mac-address-table gmrp

Mode Privileged Exec

Field Descriptions Mac Address—A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In a system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.

Type—This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description—The text description of this multicast table entry

Interfaces—The list of interfaces that are designated for forwarding (Fwd:) and filtering (Fit:)

RMON Commands

This chapter contains syntax statements for the following commands:

- [rmon alarm on page 261](#)
- [rmon collection history on page 263](#)
- [rmon collection statistics on page 264](#)
- [rmon event on page 264](#)
- [show rmon on page 265](#)
- [show rmon alarms on page 266](#)
- [show rmon alarms brief on page 266](#)
- [show rmon events on page 267](#)
- [show rmon events brief on page 268](#)
- [show rmon history on page 268](#)
- [show rmon history brief on page 269](#)
- [show rmon log on page 269](#)
- [show rmon log brief on page 270](#)
- [show rmon statistics on page 271](#)
- [show rmon statistics brief on page 271](#)

SFTOS Remote Network Monitoring (RMON) is based on RFC standards providing both 32-bit and 64-bit monitoring of S-Series switches, along with long-term statistics collection. SFTOS 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, 64 bits
Ethernet History Control Table	RFC-2819
Ethernet History Table	RFC-2819
Ethernet History High-Capacity Table	RFC-3273, 64 bits
Alarm Table	RFC-2819
High-Capacity Alarm Table (64 bits)	RFC-3434, 64 bits
Event Table	RFC-2819
Log Table	RFC-2819

rmon alarm

Set an alarm on a MIB object.

Syntax `s,eou g s,u 1-65535 SNMP_OID 5-3600 {delta | absolute} rising-threshold 0-4294967295 index falling-threshold 0-4294967295 index [owner string]`

To disable the alarm, use the `no rmon alarm 1-65535` command.

Parameters	<i>1-65535</i>	An integer, from 1 to 65535 that uniquely identifies the alarm in the RMON Alarm Table.
	<i>SNMP_OID</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. For general MIB queries, the OIDs start from 1.3.6.1.2.1. For private MIB queries, the OIDs start from 1.3.6.1.4.1.6027.1, where 6027 is the Dell Force10 Enterprise Number. The object type must be a 32-bit integer.
	<i>5-3600</i>	Sample interval, in seconds, with which the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds
	<i>delta</i>	Enter the keyword delta to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.
	<i>absolute</i>	Enter the keyword absolute to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.
	<i>rising-threshold</i> <i>0-4294967295 index</i>	Enter the keyword rising-threshold followed by the value (32-bit) at which the rising-threshold alarm is either triggered or reset — the minimum threshold for causing a rising alarm. Range: 0-4294967295 Then, in place of <i>event-number</i> , 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. Range: 0-65535
	<i>falling-threshold</i> <i>0-4294967295 index</i>	Enter the keyword falling-threshold followed by the value (32-bit) the falling-threshold alarm is either triggered or reset — the maximum threshold for causing a falling alarm. Range: 0-4294967295 Then enter the event number to trigger (0-65535) 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. Range: 0-65535
	<i>owner string</i>	(OPTIONAL) Enter the keyword OWNER followed by a name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB. Range: string of 127 characters maximum

Defaults owner

Mode Global Config

Command History

Version 2.5.1.0	Introduced
-----------------	------------

Usage A pair relationship exists between the *index* numbers entered here in **rising-threshold index** and **falling-threshold index** and *index* numbers defined by the command **rmon event index**.

For example, the following command sequence requires that RMON event 10 be triggered by RMON alarm 50 when the rising threshold of 200 is exceeded. RMON event 20 will be triggered by RMON alarm 50 when the falling threshold of 100 is passed.

Example **Figure 16-92. RMON configuration Example**

```
Forcel0# config
Forcel0 (config)#rmon event 10
Forcel0 (config)#rmon event 20
Forcel0 (config)#rmon alarm 50 1.3.6.1.4.1.6027.1.1.16.0.2 absolute
rising-threshold 200 10 falling-threshold 100 20
```

**Related
Commands**

show rmon alarms	Display the contents of the RMON Alarm Table for a specific index number.
show rmon alarms brief	Display a summary of the contents of the RMON Alarm Table.

rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

Syntax `rmon collection history controlEntry 1-65535 [buckets number] [interval 5-3600] [owner name]`

To remove a specified RMON history group of statistics collection, use the `no rmon collection history controlEntry 1-65535` command.

Parameters

<code>controlEntry 1-65535</code>	Enter the keyword controlEntry to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 to uniquely identify, in the RMON History Table, the RMON group of statistics.
<code>buckets <i>number</i></code>	(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
<code>interval 5-3600</code>	(OPTIONAL) Enter the keyword interval followed the number of seconds in each polling cycle. Range: 5 to 3600 seconds Default: 1800 seconds
<code>owner <i>name</i></code>	(OPTIONAL) Enter the keyword owner followed by the owner name to record the owner of the RMON group of statistics. Range: 1–127 alphanumeric characters

Defaults As described above

Mode Interface Config

**Command
History**

Version 2.5.1.0	Introduced
-----------------	------------

**Related
Commands**

show rmon history	Display the contents of the RMON Ethernet History table for a specific index number.
show rmon history brief	Display the contents of RMON Log table for a specific index entry.

rmon collection statistics

Enable RMON MIB statistics collection on an interface.

Syntax `rmon collection statistics controlEntry 1-65535 [owner name]`

To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics controlEntry 1-65535` command.

Parameters	<code>controlEntry 1-65535</code>	Enter the keyword controlEntry to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that uniquely identifies the entry in the RMON Statistics Table.
	<code>owner name</code>	(OPTIONAL) Enter the keyword owner followed by the owner name to record the owner of the RMON group of statistics. Range: 1–127 alphanumeric characters
Defaults	No default behavior	
Mode	Interface Config	
Command History	Version 2.5.1.0	Introduced
Related Commands	show rmon statistics	Display the contents of RMON Statistics table for a specific index entry.
	show rmon statistics brief	Display a summary of the contents of the RMON Ethernet Statistics log.

rmon event

Add an event in the RMON event table.

Syntax `rmon event 1-65535 [log] [trap SNMP_community] [description string] [ownername]`

To remove an RMON event, use the `no rmon event 1-65535` command.

Parameters	<code>1-65535</code>	Assign an event number in integer format from 1 to 65535. The value must be unique in the RMON Event Table.
	<code>log</code>	(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
	<code>trap SNMP_community</code>	(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 <i>string</i>	(OPTIONAL) Enter the keyword description followed by a string describing the event. Range: 1–127 alphanumeric characters
	owner <i>name</i>	(OPTIONAL) Enter the keyword OWNER followed by a name for the owner of this event. Range: 1–127 alphanumeric characters
Defaults	As described above	
Mode	Global Config	
Command History	Version 2.5.1.0 Introduced	
Usage	A pair relationship exists between the <i>index</i> number defined by this command and the <i>index</i> numbers used in the command rmon alarm . See the example in Figure 16-92 on page 263 .	
Related Commands	show rmon events	Display the contents of RMON Event Table for a specific index entry.
	show rmon events brief	Display a summary of the contents of the RMON Event Table.

show rmon

Display the RMON running status, including the memory usage, and total RMON entries configured in the system.

Syntax	show rmon	
Defaults	No default behavior	
Mode	Privileged Exec	
Command History	Version 2.5.1.0 Introduced	

Example **Figure 16-93. show rmon Command Example**

```

Forcel0# show rmon
RMON status
  Total memory used ..... 202260 bytes.
  Ether statistics table ..... 2 entries, 1184 bytes
  Ether history table ..... 9 entries, 198876 bytes
  Alarm table ..... 2 entries, 536 bytes
  Event table ..... 4 entries, 1664 bytes
  Log table ..... 0 entries, 0 bytes
Forcel0#

```

Related Commands	rmon alarm	Set an alarm on a MIB object.
	rmon collection history	Enable the RMON MIB history group of statistics collection on an interface.

rmon collection statistics	Enable RMON MIB statistics collection on an interface.
rmon event	Add an event in the RMON event table.

show rmon alarms

Display the contents of the RMON Alarm Table for a specific index number.

Syntax	show rmon alarms [<i>index</i>]	
Parameters	<i>index</i>	(OPTIONAL) Enter the RMON table index number to display just that entry. Range: 1-65535
Defaults	No default behavior	
Mode	Privileged Exec	
Command History	Version 2.5.1.0	Introduced

Example **Figure 16-94. show rmon alarms index Command Example**

```
Force10#show rmon alarms 1
RMON alarm entry 1
  Sample Interval ..... 5
  Object ..... 2.2
  Sample type ..... absolute value.
  Value ..... not available
  Alarm type ..... rising or falling alarm.
  Rising threshold ..... 1
  RMON event index ..... 1
  Falling threshold ..... 1
  RMON event index ..... 1
  Alarm owner ..... owner-string
  Alarm status ..... OK
Force10#
```

Related Commands	rmon alarm	Set an alarm on a MIB object.
-------------------------	----------------------------	-------------------------------

show rmon alarms brief

Display a summary of the contents of the RMON Alarm Table.

Syntax	show rmon alarms brief
Defaults	No default behavior

Mode	Privileged Exec
Command History	Version 2.5.1.0 Introduced
Example	<p>Figure 16-95. show rmon alarms brief Command Example</p> <pre> Forcel0#show rmon alarms 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 Forcel0# </pre>
Related Commands	rmon alarm Set an alarm on a MIB object.

show rmon events

Display the contents of RMON Event Table for a specific index entry.

Syntax	show rmon events [<i>index</i>]
Parameters	<i>index</i> (OPTIONAL) Enter the table index number to display just that entry. Range: 1-65535
Defaults	No default behavior
Mode	Privileged Exec
Command History	Version 2.5.1.0 Introduced
Example	<p>Figure 16-96. show rmon event index Command Example</p> <pre> Forcel0#show rmon events 3 RMON event entry 3 Description abc Event type none. Event community public Event last time sent none Event owner bhd Event status OK Forcel0# </pre>
Related Commands	rmon event Add an event in the RMON event table.

show rmon events brief

Display a summary of the contents of the RMON Event Table.

Syntax	show rmon events brief
Defaults	No default behavior
Mode	Privileged Exec
Command History	<hr/> Version 2.5.1.0 Introduced <hr/>

Example **Figure 16-97. show rmon event brief Command Example**

```
Force10#show rmon events brief
index          description
-----
1              abc
2              rt
Force10#
```

Related Commands	<hr/> rmon event Add an event in the RMON event table. <hr/>
-------------------------	--

show rmon history

Display the contents of the RMON Ethernet History table for a specific index number.

Syntax	show rmon history [<i>index</i>]
Parameters	<hr/> <i>index</i> (OPTIONAL) Enter the table index number to display just that entry. Range: 1-65535 <hr/>
Defaults	No default behavior
Mode	Privileged Exec
Command History	<hr/> Version 2.5.1.0 Introduced <hr/>

Example **Figure 16-98. show rmon history index Command Example**

```
Forcel0#show rmon history 1800
RMON history control entry 1800
  Interface ..... 0/2
  IfIndex ..... 2
  Bucket requested ..... 678
  Bucket granted ..... 678
  Sampling interval ..... 890 sec
  Owner ..... jhdhd
  Status ..... OK
Forcel0#
```

Related Commands	rmon collection history	Enable the RMON MIB history group of statistics collection on an interface.
-------------------------	---	---

show rmon history brief

Display a summary of the contents of the RMON Ethernet History table.

Syntax show rmon history brief

Defaults No default behavior

Mode Privileged Exec

Command History	Version 2.5.1.0	Introduced
------------------------	-----------------	------------

Example **Figure 16-99. show rmon history brief Command Example**

```
Forcel0#show rmon history brief
index      Interface      Ifindex
-----
2          0/1            1
3          0/3            3
Forcel0#
```

Related Commands	rmon collection history	Enable the RMON MIB history group of statistics collection on an interface.
-------------------------	---	---

show rmon log

Display the contents of RMON Log table for a specific index entry.

Syntax show rmon log [*index*]

Parameters	<i>index</i>	(OPTIONAL) Enter the log index number to display just that entry. Range: 1-65535
-------------------	--------------	---

Defaults	No default behavior				
Mode	Privileged Exec				
Command History	Version 2.5.1.0 Introduced				
Example	<p>Figure 16-100. show rmon log index Command Example</p> <pre>Force10#show rmon log 1 RMON Log entry 1 Log event Index 5 Log time Log Description xyz Force10#</pre>				
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.				
Related Commands	<table border="1"> <tr> <td>rmon event</td> <td>Add an event in the RMON event table.</td> </tr> <tr> <td>rmon collection history</td> <td>Enable the RMON MIB history group of statistics collection on an interface.</td> </tr> </table>	rmon event	Add an event in the RMON event table.	rmon collection history	Enable the RMON MIB history group of statistics collection on an interface.
rmon event	Add an event in the RMON event table.				
rmon collection history	Enable the RMON MIB history group of statistics collection on an interface.				

show rmon log brief

Display a summary of the contents of the RMON Log table.

Syntax	show rmon log brief
Defaults	No default behavior
Mode	Privileged Exec
Command History	Version 2.5.1.0 Introduced
Example	<p>Figure 16-101. show rmon log brief Command Example</p> <pre>Force10#show rmon log brief Index Description ----- 2 abs 4 ndf Force10#</pre>
Usage Information	The log 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.

**Related
Commands**

rmon event	Add an event in the RMON event table.
rmon collection history	Enable the RMON MIB history group of statistics collection on an interface.

show rmon statistics

Display the contents of RMON Statistics table for a specific index entry.

Syntax	show rmon statistics [<i>index</i>]
Parameters	<i>index</i> (OPTIONAL) Enter the index number to display just that entry. Range: 1-65535
Defaults	No default behavior
Mode	Privileged Exec
Command History	Version 2.5.1.0 Introduced
Example	Figure 16-102. show rmon statistics index Command Example

```
Force10#show rmon statistics 2
RMON statistics entry 2
Interface ..... 0/1
IfIndex ..... 1
Packets dropped ..... 0
Bytes received ..... 1682964573
Packets received ..... 19020083
Broadcast packets ..... 0
Multicast packets ..... 0
CRC error ..... 0
Under-size packets ..... 0
Over-size packets ..... 0
Fragment errors ..... 0
Jabber errors ..... 0
Collision ..... not supported
64bytes packets ..... 4047937
65-127 bytes packets ..... 14785903
128-255 bytes packets ..... 190
256-511 bytes packets ..... 186041
512-1023 bytes packets ..... 12
1024-1518 bytes packets ..... 0
Owner .....
Status ..... OK
Force10#
```

**Related
Commands**

rmon collection statistics	Enable RMON MIB statistics collection on an interface.
--	--

show rmon statistics brief

Display a summary of the contents of the RMON Ethernet Statistics table.

Syntax show rmon statistics brief

Defaults No default behavior

Mode Privileged Exec

Command History

Version 2.5.1.0 Introduced

Example **Figure 16-103. show rmon statistics brief Command Example**

```
Forcel0#show rmon statistics brief
Index          Interface
-----
4              0/1
5              0/3
Forcel0#
```

Related Commands

[rmon collection statistics](#) Enable RMON MIB statistics collection on an interface.

IGMP Snooping Commands

This chapter provides a detailed explanation of the IGMP (Internet Group Management Protocol) Snooping commands. The IGMP Snooping commands are:

- `igmp enable` (global) on page 274
- `igmp enable` (interface) on page 274
- `igmp fast-leave` on page 275
- `igmp groupmembership-interval` on page 275
- `igmp interfacemode enable all` on page 276
- `igmp maxresponse` on page 276
- `igmp mcrtexpiretime` (interface) on page 277
- `igmp mrouter` on page 277
- `igmp mrouter interface enable` on page 278
- `set igmp` (interface) on page 278
- `set igmp` (system) on page 278
- `set igmp fast-leave` on page 279
- `set igmp groupmembership-interval` (system level) on page 279
- `set igmp groupmembership-interval` (interface level) on page 279
- `set igmp groupmembership-interval all` on page 280
- `set igmp interfacemode all` on page 280
- `set igmp maxresponse` on page 280
- `set igmp maxresponse` on page 281
- `set igmp maxresponse all` on page 281
- `set igmp mcrtexpiretime` (global) on page 281
- `set igmp mcrtexpiretime` (interface) on page 282
- `set igmp mcrtexpiretime all` on page 282
- `set igmp mrouter interface` on page 283
- `set igmp mrouter` on page 283
- `show igmpsnooping` on page 283
- `show igmpsnooping fast-leave` on page 285
- `show igmpsnooping mrouter interface` on page 285
- `show mac-address-table igmpsnooping` on page 285

See also the Layer 3 IGMP Commands on page 471 in the IP Multicast chapter.

igmp enable (global)

This command enables IGMP Snooping on the system. The default value is disabled.



Note: The IGMP application supports the following:

- Global configuration or per interface configuration. Per VLAN configuration is unsupported in the IGMP snooping application.
- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Syntax	[no] igmp enable	
Default	disabled	
Mode	Global Config	
Command History	<hr/> Version 2.3 Changed from set igmp (system) <hr/>	
Related Commands	<hr/> igmp enable (interface) This command enables IGMP Snooping on a selected interface. <hr/> show igmpsnooping Displays IGMP Snooping status. <hr/>	

igmp enable (interface)

This command enables IGMP Snooping on a selected interface, including VLANs and LAGs. If an interface that has IGMP Snooping enabled is enabled for routing or is enlisted as a member of a port channel (LAG), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or port channel membership is removed from an interface that has IGMP Snooping enabled.

Syntax	[no] igmp enable	
Default	disabled	
Mode	Interface Config; Interface Port Channel Config; Interface VLAN Config	
Command History	<hr/> Version 2.5.1 Added to the new Interface Port Channel Config mode <hr/> Version 2.3 Revised from set igmp . Added to the new Interface VLAN Config mode. <hr/>	
Related Commands	<hr/> igmp enable (global) This command enables IGMP Snooping on the system. <hr/> show igmpsnooping Displays IGMP Snooping status. <hr/>	

igmp fast-leave

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

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

Syntax [no] igmp fast-leave

The no version of this command disables IGMP Snooping fast-leave admin mode on a selected interface.

Default disable

Mode Interface Config; Interface Port Channel Config

Command History

Version 2.5.1	Added to the new Interface Port Channel Config mode
Version 2.3	Revised from set igmp fast-leave .

Related Commands

igmp enable (global)	Enables IGMP Snooping on the system.
show igmpsnooping	Displays IGMP Snooping status information.

igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on the selected interface or LAG (port channel). The group membership interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.

Syntax igmp groupmembership-interval 2-3600

The variable must be greater than the IGMPv3 maximum response time value. The range is 2 to 3600 seconds.

The no igmp groupmembership-interval command sets the IGMP v3 group membership interval time on the interface to the default value.

Default 260 seconds

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.3	Modified: Revised from <code>set igmp groupmembership-interval</code> . Added Interface Range mode.
	Version 2.5.1	Added Interface Port Channel Config mode
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	interface	Identifies an interface and enters the Interface Config mode.
	show igmpsnooping	Displays IGMP Snooping status information.

igmp interfacemode enable all

This command enables IGMP Snooping on all interfaces. If an interface that has IGMP Snooping enabled is enabled for routing or is enlisted as a member of a port channel (LAG), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will be subsequently re-enabled if routing is disabled or port-channel (LAG) membership is removed from an interface that has IGMP Snooping enabled.

Syntax [no] igmp interfacemode enable all

The `no` version of this command disables IGMP Snooping on all interfaces.

Default disabled

Mode Global Config

Command History	Version 2.3	Changed from <code>set igmp interfacemode all</code>
Related Commands	igmp enable (interface)	This command enables IGMP Snooping on a selected interface.
	show igmpsnooping	Displays IGMP Snooping status.

igmp maxresponse

This command sets the IGMP maximum response time on a selected interface, including VLAN and LAG interfaces. The maximum response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface.

Syntax igmp maxresponse 1-3599

The variable must be less than the IGMP query interval time value. The range is 1 to 3599 seconds.

The `no igmp maxresponse` command sets the IGMP maximum response time on the interface to the default value.

Default 10 seconds

Mode	Interface Config; Interface Port Channel Config; Interface Vlan Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.5.1	Modified: Added Interface Port Channel Config mode.
	Version 2.3	Modified: Revised from set igmp maxresponse . Added Interface Range and Interface Vlan Config modes.
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	interface	Identifies an interface and enters the Interface Config mode.
	show igmpsnooping	Displays IGMP Snooping status information.

igmp mcrterptime (interface)

This command sets the Multicast Router Present Expiration time on a selected interface.

Syntax `igmp mcrterptime 0-3600`

The variable is the amount of time in seconds that a switch will wait for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

The `no igmp mcrterptime` command sets the Multicast Router Present Expiration time on the interface to 0. A value of 0 indicates an infinite timeout, i.e. no expiration.

Default 0

Mode Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.5.1	Modified: Added Interface Port Channel Config mode.
	Version 2.3	Modified: Revised from set igmp mcrterptime . Added Interface Range mode and Interface VLAN Config mode.

Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	show igmpsnooping	Displays IGMP Snooping status information.

igmp mrouter

This command configures the VLAN ID (*vlanId*) that has the multicast router mode enabled.

Syntax `[no] igmp mrouter vlanId`

The `no` version of this command disables multicast router mode for a particular VLAN ID (*vlanId*).

Mode	Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.5.1	Modified: Added Interface Port Channel Config mode.
	Version 2.3	Modified: Revised from set igmp mrouter . Added Interface Range mode.
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	interface	Identifies an interface and enters the Interface Config mode.

igmp mrouter interface enable

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

Syntax	[no] igmp mrouter interface enable	
	The no version of this command disables the status of the interface as a statically configured multicast router interface.	
Default	disable	
Mode	Interface Config; Interface Port Channel Config	
Command History	Version 2.5.1	Modified: Added Interface Port Channel Config mode.
	Version 2.3	Revised from set igmp mrouter interface .
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp (interface)

Command History	Version 2.3	Revised to igmp (interface) .
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp (system)

Command History	Version 2.3	Changed to igmp enable (global)
------------------------	-------------	---

**Related
Commands**

igmp enable (global)	Enables IGMP Snooping on the system.
igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp fast-leave

**Command
History**

Version 2.3	Revised to igmp fast-leave .
-------------	--

**Related
Commands**

igmp fast-leave	Enables or disables IGMP Snooping fast-leave admin mode on a selected interface.
igmp enable (global)	Enables IGMP Snooping on the system.

set igmp groupmembership-interval (system level)

This command sets the IGMP Group Membership Interval time on the system. The Group Membership Interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMP Maximum Response time value.

Syntax [no] set igmp groupmembership-interval 2-3600

The range is 2 to 3600 seconds.

The **no** version of this command sets the IGMP Group Membership Interval time on the system to 260 seconds.

Default 260

Mode Global Config

**Related
Commands**

igmp enable (global)	Enables IGMP Snooping on the system.
show igmpsnooping	Displays IGMP Snooping status information.

set igmp groupmembership-interval (interface level)

**Command
History**

Version 2.3	Revised to igmp groupmembership-interval (interface level) .
-------------	--

**Related
Commands**

igmp groupmembership-interval	Sets the IGMP Group Membership Interval time on a particular interface.
igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp groupmembership-interval all

This command sets the IGMP Group Membership Interval time on the system for all the interfaces. The Group Membership Interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.

Syntax `set igmp groupmembership-interval all 2-3600`

This variable must be greater than the IGMP Maximum Response time value. The range is 2 to 3600 seconds.

The `no set igmp groupmembership-interval all` command sets the IGMP Group Membership Interval time on all interfaces to the default value.

Default 260 seconds

Mode Global Config

Related Commands

igmp enable (interface)	Enables IGMP Snooping on a selected interface.
show igmpsnooping	Displays IGMP Snooping status information.

set igmp interfacemode all

Command History

Version 2.3	Changed to igmp interfacemode enable all
-------------	--

Related Commands

igmp interfacemode enable all	Sets the IGMP Group Membership Interval time on a particular interface.
igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp maxresponse

This command sets the IGMP Maximum Response time on the system. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3599 seconds.

The `no` version of this command sets the IGMP Maximum Response time on the system to 10 seconds.

Syntax `set igmp maxresponse 1-3599`

`no set igmp maxresponse`

Default 10

Mode Global Config

**Related
Commands**

igmp enable (interface)	Enables IGMP Snooping on a selected interface.
show igmpsnooping	Displays IGMP Snooping status information.

set igmp maxresponse

**Command
History**

Version 2.3	Revised to igmp maxresponse .
-------------	---

**Related
Commands**

igmp maxresponse	Sets the IGMP Maximum Response time on a particular interface.
----------------------------------	--

set igmp maxresponse all

This command sets the IGMP Maximum Response time on the system for all the interfaces. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3599 seconds.

The `no` version of this command sets the IGMP Maximum Response time on all interfaces to the default value.

Syntax `set igmp maxresponse all <1-3599>`

`no set igmp maxresponse all`

Default 10 seconds

Mode Global Config

**Related
Commands**

igmp enable (interface)	Enables IGMP Snooping on a selected interface.
show igmpsnooping	Displays IGMP Snooping status information.

set igmp mcrtrexpiretime (global)

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

The `no` version of this command sets the Multicast Router Present Expiration time on the system to 0. A value of 0 indicates an infinite timeout, i.e. no expiration.

Syntax `set igmp mcrtrexpiretime 0-3600`

	no set igmp mcrtpiretime	
Default	0	
Mode	Global Config	
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	set igmp mcrtpiretime (global)	Sets the Multicast Router Present Expiration time on the system for all the interfaces.
	show igmpsnooping	Displays IGMP Snooping status information.

set igmp mcrtpiretime (interface)

Command History	Version 2.3	Revised to igmp mcrtpiretime .
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	show igmpsnooping	Displays IGMP Snooping status information.

set igmp mcrtpiretime all

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

The no version of this command sets the Multicast Router Present Expiration time on all interfaces to 0. A value of 0 indicates an infinite timeout, i.e. no expiration.

Syntax	set igmp mcrtpiretime all <i>0-3600</i>	
	no set igmp mcrtpiretime all	
Default	0	
Mode	Global Config	
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	show igmpsnooping	Displays IGMP Snooping status information.

set igmp mrouter interface

Command History	Version 2.3	Revised to <code>igmp mrouter interface</code> .
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	igmp mrouter interface enable	Configures a selected interface as a multicast router interface.

set igmp mrouter

Command History	Version 2.3	Revised to <code>igmp mrouter</code> .
Related Commands	igmp mrouter	Enables IGMP Snooping on a selected interface.
	igmp enable (global)	Enables IGMP Snooping.

show igmpsnooping

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

Syntax	<code>show igmpsnooping [unit/slot/port 1-3965 mrouter interface unit/slot/port]</code>	
Parameters	<code>unit/slot/port</code>	(OPTIONAL) Display ports on which Multicast routers are detected. Enter interface in unit/slot/port format.
	<code>1-3965</code>	(OPTIONAL) Display VLANs for the specified interface on which Multicast routers are detected.
	<code>mrouter interface { unit/slot/port vlan 1-3965 }</code>	(OPTIONAL) See show igmpsnooping mrouter interface on page 285 .
Mode	Privileged Exec	
Command History	Version 2.3	Modified: <code>1-3965</code> option added (VLAN ID).

Example **Figure 17-104. Output of the show igmpsnooping Command**

```

Forcel0#show igmpsnooping
Admin Mode.....Enable
Multicast Control Frame Count.....0
Interfaces Enabled for IGMP Snooping....1/0/10
Vlans enabled for IGMP snooping.....20

Forcel0-S50 #show igmpsnooping 1/0/1
IGMP Snooping Admin Mode..... Disable
Fast Leave Mode..... Disable
Group Membership Interval..... 260
Max Response Time..... 10
Multicast Router Present Expiration Time..... 0

Forcel0-S50 #show igmpsnooping 3965
Vlan ID..... 3965
IGMP Snooping Admin Mode..... Disabled
Fast Leave Mode..... Disabled
Group Membership Interval..... 260
Maximum Response Time..... 10
Multicast Router Expiry Time..... 0

```

Report Fields When **no parameter** is specified, the response contains the following fields:

Admin Mode—Enabled or Disabled

Multicast Control Frame Count—The number of multicast control frames that are processed by the CPU

Interfaces Enabled for IGMP Snooping—The list of interfaces on which IGMP Snooping is enabled

Vlans enabled for IGMP snooping—The number of VLANs on which IGMP Snooping is enabled

When the **optional argument** *unit/slot/port* is used, the response is as follows:

IGMP Snooping Admin Mode—This indicates whether or not IGMP Snooping is active on the interface.

Fast Leave Mode—Disable or Enabled

Group Membership Interval—This is the amount of time a switch will wait for a report for a particular group on a particular interface before it sends a query on that interface. This value may be configured

Max Response Time—This displays the amount of time the switch will wait after sending a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.

Multicast Router Present Expiration Time—If a query is not received on an interface within this amount of time, the interface is removed from the list of interfaces with multicast routers attached. This value may be configured.

When the **optional argument** *1-3965* is used, the response is the same as for *unit/slot/port*, except that one more report field is added:

Vlan ID—This echoes the number of the VLAN specified in the parameter.

show igmpsnooping fast-leave

Command History	Version 2.3	Deprecated: Use show igmpsnooping to display whether or not IGMP Snooping is enabled on the designated interface.
------------------------	-------------	---

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Syntax show igmpsnooping mrouter interface { *unit/slot/port* | vlan 1-3965 }

Parameters	<i>unit/slot/port</i>	Display ports on which Multicast Routers are detected. Enter interface in unit/slot/port format.
	vlan 1-3965	Display VLANs for the specified interface on which Multicast Routers are detected. Routing must be enabled on the VLAN in order for the VLAN to be reported by this command.

Mode Privileged Exec

Example **Figure 17-105. Output of the show igmpsnooping Command**

```
Forcel0#show igmpsnooping mrouter interface 1/0/1
Slot/Port..... 1/0/1
Multicast Router Attached..... Disable
```

Report Fields Slot/Port—The port on which multicast router information is being displayed
Multicast Router Attached—Whether or not multicast router is statically enabled on the interface
VLAN ID—(only for the vlan 1-3965 option) The list of VLANs in which the interface is a member

show mac-address-table igmpsnooping

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

Syntax show mac-address-table igmpsnooping

Mode Privileged Exec

Example **Figure 17-106. Output of the show mac-address-table igmpsnooping Command**

```

Force10#show mac-address-table igmpsnooping
<cr> Press Enter to execute the command.
(LVL7 FASTPATH Routing) #show mac-address-table igmpsnooping
Type Description Interfaces
-----
00:01:01:00:5E:00:01:16 DynamicNetwork AssistFwd: 1/0/47
00:01:01:00:5E:00:01:18 DynamicNetwork AssistFwd: 1/0/47
00:01:01:00:5E:37:96:D0 DynamicNetwork AssistFwd: 1/0/47
00:01:01:00:5E:7F:FF:FA DynamicNetwork AssistFwd: 1/0/47

```

Report Fields

Mac Address—A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In a system the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes.

Type—This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description—The text description of this multicast table entry.

Interfaces—The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Related Commands

show mac-address-table	Depending on selected display parameters, displays various Multicast Forwarding Database (MFDB) information.
show mac-addr-table	Displays forwarding database entries

LAG/Port Channel Commands

This chapter provides syntax details of the Link Aggregation Group (LAG) commands (802.3ad), also called port channel, port trunking, and other terms. The commands in this chapter are:

- [addport on page 288](#)
- [channel-member on page 289](#)
- [clear port-channel on page 290](#)
- [cos-queue max-bandwidth on page 290](#)
- [cos-queue strict on page 291](#)
- [deleteport \(interface config\) on page 291](#)
- [deleteport \(global config\) on page 291](#)
- [description \(port channel\) on page 292](#)
- [dot1p-priority on page 293](#)
- [gmrp interfacemode enable \(LAG\) on page 294](#)
- [igmp enable on page 294](#)
- [igmp fast-leave on page 294](#)
- [igmp groupmembership-interval on page 294](#)
- [igmp mrcvertime \(interface\) on page 294](#)
- [igmp mrouter on page 295](#)
- [igmp mrouter interface on page 295](#)
- [interface port-channel on page 295 \(create LAG and/or access Interface Port Channel Config mode\)](#)
- [ip access-group \(port channel\) on page 295](#)
- [mac access-group \(port channel\) on page 296](#)
- [mode dvlan-tunnel on page 297](#)
- [mtu \(LAG\) on page 297](#)
- [port-channel on page 297](#)
- [port-channel enable all \(global\) on page 298](#)
- [port-channel enable \(interface\) on page 298](#)
- [port-channel linktrap on page 298](#)
- [port-channel name on page 299](#)
- [port-channel staticcapability on page 299](#)
- [port lacpmode enable on page 299](#)
- [port lacpmode enable all on page 299](#)
- [port lacptimeout \(global\) on page 300](#)
- [port lacptimeout \(interface\) on page 300](#)
- [port-security on page 301](#)
- [port-security mac-address on page 301](#)
- [port-security mac-address move on page 301](#)
- [port-security max-dynamic on page 301](#)

- [port-security max-static](#) on page 301
- [protocol lacp](#) on page 301
- [protocol static](#) on page 302
- [rate-interval](#) on page 302
- [service-policy](#) on page 302
- [set garp timer join](#) on page 302
- [set garp timer leave](#) on page 302
- [set garp timer leaveall](#) on page 303
- [show interfaces port-channel](#) on page 303
- [show port-channel](#) on page 304
- [show port-channel brief](#) on page 304
- [shutdown \(port channel\)](#) on page 305
- [snmp-server enable trap violation](#) on page 305
- [snmp trap link-status \(port channel\)](#) on page 305
- [spanning-tree \(LAG\)](#) on page 306
- [spanning-tree 0 cost \(LAG\)](#) on page 306
- [spanning-tree 0 priority \(LAG\)](#) on page 307
- [spanning-tree MSTi cost \(LAG\)](#) on page 307
- [spanning-tree MSTi priority \(LAG\)](#) on page 307
- [spanning-tree mstp edge-port \(LAG\)](#) on page 308



Note: SFTOS 2.5.1 introduces the Interface Port Channel Config mode, which contains new commands and some commands that are versions of previous commands. Some of the previous commands are deprecated, while some remain, providing alternative ways to accomplish a task.

SFTOS 2.5.1 discontinues the logical interface identifier (0/1/xx) for a LAG (port channel). Instead, the ID is an integer, as exemplified in [Figure 18-110](#) on page 304 and [Figure 18-109](#) on page 303.



Note: An IP address is not supported on a LAG interface.

addport

In Interface Config mode, this command adds the selected port to the designated LAG (port channel).

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.5.1	Deprecated. Removed from CLI
	Version 2.3	Added Interface Range mode
Related Commands	channel-member	Adds/deletes the specified range of ports to the LAG selected by the aoCEst OEudesC6Qioofg .

interface range	Defines an interface range and accesses the Interface Range mode
interface port-channel	Creates the port channel (LAG) and invokes the Interface Port Channel Config mode. Or, if the port channel is already created, simply invokes the Interface Port Channel Config mode.

channel-member

This command adds/deletes the specified range of ports to the LAG (port channel) selected by the `interface port-channel` command.



Note: Before adding a port to a port channel, set the physical mode of the port. See the [speed](#) command.

Syntax [no] channel-member *unit/slot/port–unit/slot/port,unit/slot/port*

Enter the ports that are to be members of the selected port channel. You enter port IDs in *unit/slot/port* format. You can enter a single port or multiple ports. To enter a non-sequential list of ports, separate two port numbers with a comma (no spaces before or after the comma). To enter a sequential range of ports, use a hyphen to designate between the low and high port number in the range.

Mode Interface Port Channel Config

Command History

Version 2.5.1	Introduced in the new Interface Port Channel Config mode
---------------	--

Example

Figure 18-107. Example of Configuring a Port Channel

```

Force10#config
Force10 (Config)#interface port-channel 2
Force10 (conf-if-po- 2)#channel-member 1/0/22-1/0/25

1/0/22 interface is part of a port-channel.
1/0/23 interface is part of a port-channel.
1/0/24 interface is part of a port-channel.

Force10 (conf-if-po- 2)#no shutdown
Force10 (conf-if-po- 2)#exit
Force10 (Config)#exit
Force10#show interface port-channel brief

Codes: L - LACP Port-channel

LAG Status Ports
-----
2    Down    1/0/22 (Up)
          1/0/23 (Up)
          1/0/24 (Up)
          1/0/25 (Up)

Force10#

```

Related Commands

interface port-channel	Creates the port channel (LAG) or, if the port channel is already created, invokes the Interface Port Channel Config mode.
show interfaces port-channel	Displays an overview of all port channels (LAGs) on the switch or details on the selected LAG.

classofservice dot1p-mapping

See [classofservice dot1p-mapping](#) on page 328 in the QoS chapter.

clear port-channel

This command removes all currently configured port-channels (LAGs).

Syntax	clear port-channel	
Mode	Privileged Exec	
Related Commands	cos-queue max-bandwidth	Deletes the selected port from the specified logical interface.
	interface port-channel	Creates the port channel (LAG) or, if the port channel is already created, invokes the Interface Port Channel Config mode.
	show interfaces port-channel	Displays an overview of all port channels (LAGs) on the switch or details on the selected LAG.

cos-queue max-bandwidth

This command specifies the maximum transmission bandwidth limit for each interface queue. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The total number of queues supported per interface is platform specific.

Syntax	cos-queue max-bandwidth <bw-1> ... <bw-n>
Modes	Global Config and Interface Config

no cos-queue max-bandwidth

This command restores the default for each queue's maximum bandwidth value.

Syntax	no cos-queue max-bandwidth
Mode	Global Config and Interface Config

cos-queue min-bandwidth

See [cos-queue min-bandwidth](#) on page 330 in the QoS chapter.

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the 'random-detect queue-parms' and the 'random-detect exponential-weighting-constant' commands.

The `no` version of this command disables WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Syntax [no] cos-queue random-detect <queue-id-1> [<queue-id-2> ... <queue-id-n>]

Modes Global Config and Interface Config

cos-queue strict

See [cos-queue strict](#) on page 331 in the QoS chapter.

deleteport (interface config)

This command deletes the selected port from the specified logical interface (port-channel (LAG) or VLAN) or, in Interface Range mode, from the selected range of interfaces.

Mode Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.1	Deprecated. Removed from CLI
Version 2.3	Interface Range mode added

Related Commands

channel-member	Adds/deletes the specified range of ports to the LAG selected by the <code>interface port-channel</code> command.
clear port-channel	Removes all port-channels (LAGs).
interface range	Defines an interface range and accesses the Interface Range mode
interface port-channel	Creates the port channel (LAG) and invokes the Interface Port Channel Config mode. Or, if the port channel is already created, simply invokes the Interface Port Channel Config mode.
show interfaces port-channel	Displays an overview of all port channels (LAGs) on the switch or details on the selected LAG.

deleteport (global config)

This command deletes a specific port channel (LAG) or all port channels.

Mode Global Config

Command History

Version 2.5.1	Deprecated. Removed from CLI
Version 2.3	Interface Range mode added

**Related
Commands**

addport	In Interface Config mode, adds a port to the port-channel (LAG), or, in Interface Range mode, the selected range of interfaces
channel-member	Adds/deletes the specified range of ports to the LAG selected by the interface port-channel command.
clear port-channel	Removes all port-channels (LAGs).
interface port-channel	Creates the port channel (LAG) and invokes the Interface Port Channel Config mode. Or, if the port channel is already created, simply invokes the Interface Port Channel Config mode.
show interfaces port-channel	Displays an overview of all port channels (LAGs) on the switch or details on the selected LAG.

description (port channel)

Enter a description for the selected port channel.

Syntax [no] **description** *line*

The *line* field is for a textual description; it allows spaces if you surround the statement with single or double quotes.

Default none

Mode Interface Port Channel Config

**Command
History**

Version 2.5.1	Introduced in the new Interface Port Channel Config mode. Replaces the port channel name command.
---------------	--

**Related
Commands**

interface port-channel	Creates the port channel (LAG) or, if the port channel is already created, invokes the Interface Port Channel Config mode.
description (VLAN)	Enter a description for the selected VLAN.

**Usage
Information**

The following example shows the use of both single quotes and double quotes in entering a description. The example also shows the resulting descriptions presented in `show interfaces` commands.

Example Figure 18-108. show interfaces description Command Example

```
S50 #conf
S50 (Config)#interface 1/0/1
S50 (Interface 1/0/1)#description "1/0/1 is access port"
S50 (Interface 1/0/1)#exit
S50 (Config)#interface 1/0/30
S50 (Interface 1/0/30)#description 'management port in vlan 30'
S50 (Interface 1/0/30)#exit
S50 (Config)#exit
S50 #show interfaces description 1/0/1
Interface.....1/0/1
IfIndex.....1
Description....1/0/1 is access port
MAC Address....00:01:E8:D5:BA:C0
Bit Offset Val..1

S50 #show interfaces description 1/0/30
Interface.....1/0/30
IfIndex.....30
Description....management port in vlan 30
MAC Address....00:01:E8:D5:BA:C0
Bit Offset Val..30

S50 #
```

Related Commands

interface vlan	Creates a VLAN, assigns it an ID and then enters the Interface VLAN mode
show interfaces	Displays information, including the description, about a selected interface.
show running-config	Display/capture the current setting of different protocol packages supported on the switch.

dot1p-priority

This command configures the priority for untagged frames.

Syntax dot1p-priority 0–7

The 0–7 field is an integer that sets the priority value for untagged frames received.

Mode Interface Port Channel Config

Command History

Version 2.5.1	Introduced in the new Interface Port Channel Config mode.
---------------	---

Related Commands

channel-member	Add a port or range of ports to the selected LAG. LAG ports must be physical ports, not other LAGs.
interface port-channel	Creates the port channel (LAG) or, if the port channel is already created, invokes the Interface Port Channel Config mode.
show interfaces port-channel	Displays an overview of all port channels (LAGs) on the switch or details on the selected LAG.

gmrp interfacemode enable (LAG)

This command enables GARP Multicast Registration Protocol (GMRP) on the selected LAG. If an interface with GARP enabled is enabled for routing or is enlisted as a member of the LAG (port channel), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled on that interface if routing is disabled and port-channel (LAG) membership is removed from the interface.

Syntax gmrp interfacemode enable

Use `no gmrp interfacemode enable` to disable GMRP on the LAG.

Default disabled

Mode Interface Port Channel Config

Command History

Version 2.5.1	Introduced in the new Interface Port Channel Config mode
---------------	--

Related Commands

gmrp interfacemode enable all	Enable GMRP on all interfaces.
---	--------------------------------

show gmrp configuration	Display GMRP information for one or all interfaces.
---	---

igmp enable

This command is available in the Interface Port Channel Config mode. See [igmp enable \(interface\)](#) on page 274 in the IGMP chapter.

igmp fast-leave

This command is available in the Interface Port Channel Config mode. See [igmp fast-leave](#) on page 275 in the IGMP chapter.

igmp groupmembership-interval

This command is available in the Interface Port Channel Config mode. See [igmp groupmembership-interval](#) on page 275 in the IGMP chapter.

igmp mcrtexpiretime (interface)

This command is available in the Interface Port Channel Config mode. See [igmp groupmembership-interval](#) on page 275 in the IGMP chapter.

igmp mrouter

This command is available in the Interface Port Channel Config mode. See [igmp mrouter on page 277](#) in the IGMP chapter.

igmp mrouter interface

This command is available in the Interface Port Channel Config mode. See [igmp mrouter interface enable on page 278](#) in the IGMP chapter.

interface port-channel

This command invokes the Interface Port Channel Config mode, along with creating a port channel (LAG) if one with the designated number does not exist.

The `no` version of this command deletes a port channel (LAG).



Note: Before including a port in a port channel, set the physical mode of the port. See the [speed](#) command.

Syntax `[no] interface port-channel r1-128`

The `r1-128` field is an integer that uniquely identifies the port channel. The maximum number of supported port channels is 128, out of which, at most, six dynamic port channels are recommended.

Mode Global Config

Command History

Version 2.5.1.0	Modified: Before 2.5.1, the command syntax was <code>desC6Oi ooEame</code> . The previous number of supported port channels was 32.
-----------------	---

Related Commands

channel-member	Add a port or range of ports to the selected LAG. LAG ports must be physical ports, not other LAGs.
show interfaces port-channel	Displays an overview of all port channels (LAGs) on the switch or details on the selected LAG.
speed	Set the physical mode of the port.

ip access-group (port channel)

This command attaches a specified access control list (ACL) to the port channel selected by the `interface port-channel` command.

Syntax `ip access-group 1-199 [1-4294967295]`

Parameters	<i>1–199</i>	Enter the number of the ACL, which was assigned using the access-list command.
	<i>1-4294967295</i>	(OPTIONAL) Enter a sequence number that indicates the desired order of this ACL relative to other ACLs already assigned to this LAG. A lower number indicates higher precedence order. If the number is already in use for this LAG, this ACL replaces the currently attached ACL using that sequence number. If you do not specify a number with this command, a number that is one greater than the highest sequence number currently in use for this LAG is used for this ACL.
Default	none	
Mode	Interface Port Channel Config	
Command History	Version 2.5.1	Introduced in the new Interface Port Channel Config mode
Related Commands	access-list	Creates an IP access control list
	interface range	Defines an interface range and accesses the Interface Range mode
	interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode
	ip access-group (Interface)	Attaches an ACL to the selected interface (Interface Config or Interface Range modes)
	show ip access-lists	Displays an IP Access Control List (ACL) and all of the rules that are defined for the ACL. The accesslistnumber is the number used to identify the ACL

mac access-group (port channel)

This command attaches a specified MAC Access Control List (ACL) identified by *name* to the selected port channel in the ingress direction.

Syntax `mac access-group name [1-4294967295]`

The `no mac access-group name` command removes the specified MAC ACL from the port channel.

Parameters	<i>name</i>	Enter the name assigned by the mac access-list extended command.
	<i>1-4294967295</i>	(OPTIONAL) This is a sequence number that will indicate the order of application of this ACL relative to other ACLs assigned to this port channel. A lower sequence number indicates higher precedence order. If the number you select is already in use for this port channel, this ACL replaces the currently attached ACL using that sequence number. If you do not specify a number with this command, a number that is one greater than the highest sequence number currently in use for this port channel is used for this ACL.
Modes	Interface Port Channel Config	
Command History	Version 2.5.1	Introduced, along with its Interface Port Channel Config mode

**Related
Commands**

interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode
interface range	Defines an interface range and accesses the Interface Range mode
mac access-group	In the Global Config, Interface Config, or Interface Range modes, attaches a MAC ACL to the selected interface.
mac access-list extended	Creates a MAC Access Control List (ACL) identified by name, consisting of classification fields defined for the Layer 2 header of an Ethernet frame.
show mac access-lists	Displays the rules defined for the MAC access list specified by <i>name</i> .
show ip access-lists	Displays an IP Access Control List (ACL) and all of the rules that are defined for the ACL.

mode dvlan-tunnel

This command is available in the Interface Port Channel Config mode.
See [mode dvlan-tunnel on page 153](#) in the VLAN chapter.

mtu (LAG)

This command sets the maximum transmission unit (MTU) size (in bytes) for the selected LAG (port channel).

The `no` version of this command resets the MTU to the default for the port channel.

Syntax `mtu 1518-9216`

For the standard implementation, the range is a valid integer between 1518–9216.

Default 1518

Mode Interface Port Channel Config

**Command
History**

Version 2.5.1	Introduced in the new Interface Port Channel Config mode.
---------------	---

**Related
Commands**

mtu (port)	Sets the MTU for a selected interface (Interface Config mode)
mtu (VLAN)	Sets the MTU for a selected VLAN (VLAN mode)
ip mtu	Sets the MTU on a routing interface (Interface Config or VLAN mode)

port-channel

This command configures a new port channel (LAG) and generates a logical *unit/slot/port* number for the port channel.

**Command
History**

Version 2.5.1.0	Modified: In 2.5.1, the command syntax is changed to interface port-channel 1-128 .
-----------------	---

Related Commands	show interfaces	Displays an overview of all port channels (LAGs) on the switch or details on the selected LAG.
	port-channel	
	addport	Add a port to a LAG. LAG ports must be physical ports, not other LAGs.

port-channel enable all (global)

This command enables the administrative mode for all port channel (LAGs).

The `no` version of this command disables all port channels (LAGs).

Syntax port-channel enable all

Mode Global Config

Command History	Version 2.3	Replaced <code>adminmode</code> with <code>enable</code> .
------------------------	-------------	--

port-channel enable (interface)

This command enables the selected port channel (LAG).

The `no` version of this command disables the selected port channel (LAG).

Syntax [no] port-channel enable

Mode Interface Config

Command History	Version 2.3	Replaced <code>adminmode</code> with <code>enable</code> .
------------------------	-------------	--

Related Commands	interface	Accesses the Interface Config mode for the selected port channel (LAG).
-------------------------	---------------------------	---

port-channel linktrap

This command enables link trap notifications for all port channels (LAGs) or for a selected port channel.

The `no` version of this command disables link trap notifications for the selected port channel.

Syntax [no] port-channel linktrap {*unit/slot/port* | all}

The interface is a logical *unit/slot/port* for a configured port channel.

The option `all` sets every configured port channel with the same administrative mode setting.

Default enabled

Mode Global Config

port-channel name

This command defines a name for the port channel (LAG).

Mode	Global Config
Command History	<hr/> Version 2.5.1 Deprecated: Replaced by description (port channel) , which adds a text description of the port channel from the new Interface Port Channel Config mode. <hr/>

port-channel staticcapability

This command enables the support of port channels (static link aggregations - LAGs) on the device. By default, the static capability for all port channels is disabled.

Command History	<hr/> Version 2.5.1 Replaced by protocol static , in the new Interface Port Channel Config mode. <hr/>
------------------------	---

port lacpmode enable

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

The no version of this command disables LACP on a port.

Syntax	[no] port lacpmode enable
Default	disabled
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	<hr/> Version 2.5 Deprecated. Use protocol lacp and protocol static . <hr/> Version 2.3 Added Interface VLAN and Interface Range modes. <hr/>
Related Commands	<hr/> interface range Defines an interface range and accesses the Interface Range mode <hr/> protocol lacp Reenables LACP on a LAG. <hr/> protocol static Converts a LAG from LACP to static. <hr/>

port lacpmode enable all

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

The no version of this command disables Link Aggregation Control Protocol (LACP) on all ports.

Syntax	[no] port lacpmode enable all
Mode	Global Config

Command History	Version 2.5	Deprecated. Use protocol lacp and protocol static .
	Version 2.3	Revised from [no] port lacpmode all
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	protocol lacp	Reenables LACP on a LAG.
	protocol static	Converts a LAG from LACP to static.

port lacptimeout (global)

This command sets the Link Aggregation Control Protocol (LACP) timeout on all ports.

The no version of this command removes the Link Aggregation Control Protocol (LACP) timeout on all ports.

Syntax	[no] port lacptimeout { short all long all }	
Parameters	short all	Enter short all to select the short timeout setting (3 seconds) for all ports.
	long all	Enter long all to select the long timeout setting (90 seconds) for all ports.
Mode	Global Config	
Related Commands	port lacptimeout (interface)	Set the LACP timeout on the selected port(s).

port lacptimeout (interface)

This command sets the Link Aggregation Control Protocol (LACP) timeout on the selected port(s).

The no version of this command removes the Link Aggregation Control Protocol (LACP) timeout on the selected port(s).

Syntax	[no] port lacptimeout { short long }	
Parameters	short	Enter short to select the short timeout setting (3 seconds) for the selected ports.
	long	Enter long to select the long timeout setting (90 seconds) for the selected ports.
Mode	Interface Config; Interface Range	
Command History	Version 2.3	Added Interface Range mode.
Related Commands	interface	Accesses the Interface Config mode for the selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	port lacptimeout (global)	Set the Link Aggregation Control Protocol (LACP) timeout on ports.

port-security

This command is available in the Interface Port Channel Config mode.
See [port-security on page 183](#) in the Security Commands chapter.

port-security mac-address

This command is available in the Interface Port Channel Config mode.
See [port-security mac-address on page 184](#) in the Security Commands chapter.

port-security mac-address move

This command is available in the Interface Port Channel Config mode.
See [port-security mac-address move on page 184](#) in the Security Commands chapter.

port-security max-dynamic

This command is available in the Interface Port Channel Config mode.
See [port-security max-dynamic on page 185](#) in the Security Commands chapter.

port-security max-static

This command is available in the Interface Port Channel Config mode.
See [port-security max-static on page 185](#) in the Security Commands chapter.

protocol lacp

This command reenables the LACP on the selected LAG.

Syntax	protocol lacp		
Default	enabled		
Mode	Interface Port Channel Config		
Usage	By default, LACP is enabled, but, if the LAG has been converted to static, you can use this command to revert the LAG to LACP mode.		
Command History	<hr/> <table><tr><td>Version 2.5.1</td><td>Introduced, in the new Interface Port Channel Config mode, to replace port-channel staticcapability.</td></tr></table> <hr/>	Version 2.5.1	Introduced, in the new Interface Port Channel Config mode, to replace port-channel staticcapability .
Version 2.5.1	Introduced, in the new Interface Port Channel Config mode, to replace port-channel staticcapability .		
Related Commands	<hr/> <table><tr><td>interface port-channel</td><td>Accesses the Interface Port Channel Config mode for the selected port channel.</td></tr></table> <hr/>	interface port-channel	Accesses the Interface Port Channel Config mode for the selected port channel.
interface port-channel	Accesses the Interface Port Channel Config mode for the selected port channel.		

interface range	Defines an interface range and accesses the Interface Range mode
protocol static	Convert the LAG to static mode.

protocol static

This command converts the selected LAG (port channel) from LACP mode to static.

Syntax	protocol static	
Default	disabled	
Mode	Interface Port Channel Config	
Usage	LAGs are in LACP mode by default. After you use this command to convert a LAG to static, if you want to revert the LAG to LACP mode, you would use the protocol lacp command.	
Command History	Version 2.5.1	Introduced, in the new Interface Port Channel Config mode, to replace port-channel staticcapability .
Related Commands	interface port-channel	Accesses the Interface Port Channel Config mode for the selected port channel.
	interface range	Defines an interface range and accesses the Interface Range mode
	protocol lacp	Revert the LAG to LACP mode.

rate-interval

This command is available in the Interface Port Channel Config mode. See [rate-interval on page 98](#) in the System Configuration chapter.

service-policy

This command is available in the Interface Port Channel Config mode. See [service-policy on page 357](#) in the System Configuration chapter.

set garp timer join

This command is available in the Interface Port Channel Config mode. See [set garp timer join on page 251](#) in the GARP Commands chapter.

set garp timer leave

This command is available in the Interface Port Channel Config mode. See [set garp timer leaveall on page 253](#) in the GARP Commands chapter.

set garp timer leaveall

This command is available in the Interface Port Channel Config mode.
See [set garp timer leaveall on page 253](#) in the GARP Commands chapter.

show interfaces port-channel

This command displays details about the designated LAG (port channel) or a summary of all LAGs.

Syntax show interfaces port-channel {1–128 | brief}

Parameters	1–128	Enter the number of the port channel, as defined in interface port-channel on page 295 .
	brief	Enter brief to display the static capability of all port channels (LAGs) on the device, as well as a summary of individual LAGs.

Mode Privileged Exec

Command History Version 2.5.1 Introduced, replacing [show port-channel](#)

Example 1 **Figure 18-109. Example of Output from show interface port-channel brief Command**

```
Forcel0#show interface port-channel brief
Codes: L - LACP Port-channel
LAG Status Ports
-----
1   Down   1/0/20 (Down)
      1/0/21 (Down)
      1/0/22 (Down)
```

Report Fields LAG — port channel number
Status — enabled/disabled
Ports — member ports

Example 2 Figure 18-110. Example of Output from show interface port-channel Command

```

Forcel0#show interface port-channel 1

Description..... wills_po20-21-22
MAC Address..... 00:01:E8:D5:A0:81
MTU..... 1518

Packets RX and TX 64 Octets..... 0
Packets RX and TX 65-127 Octets..... 0
Packets RX and TX 128-255 Octets..... 0
Packets RX and TX 256-511 Octets..... 0
Packets RX and TX 512-1023 Octets..... 0
Packets RX and TX 1024-1518 Octets..... 0
Packets RX and TX 1519-1522 Octets..... 0
Packets RX and TX 1523-2047 Octets..... 0
Packets RX and TX 2048-4095 Octets..... 0
Packets RX and TX 4096-9216 Octets..... 0

Jabbers Received..... 0
Fragments Received..... 0
Undersize Received..... 0
Alignment Errors..... 0
FCS Errors..... 0
Overruns..... 0
Unicast Packets Received..... 0
--More-- or (q)uit
Multicast Packets Received..... 0
Broadcast Packets Received..... 0
Single Collision Frames..... 0
Multiple Collision Frames..... 0
Excessive Collision Frames..... 0
Port Membership Discards..... 0

Time Since Counters Last Cleared..... 0 day 0 hr 46 min 38 sec

Link
Adm. Trap STP Mbr Port Port
LAG Link Mode Mode Mode Type Ports Speed Active
-----
1 Down En. En. Dis. Static 1/0/20 Auto False
1/0/21 Auto False
1/0/22 Auto False

```

**Related
Commands**

interface range	Defines an interface range and accesses the Interface Range mode
interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode

show port-channel

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

Syntax `show port-channel {logical_unit/slot/port | all}`

Mode Privileged Exec

**Command
History**

Version 2.5.1 Modified to [show interfaces port-channel](#).

show port-channel brief

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

Syntax	show port-channel brief
Mode	Privileged Exec and User Exec
Command History	Version 2.5.1 Modified to show interfaces port-channel .

shutdown (port channel)

This command enables or disables the port channel selected by the `interface port-channel` command. The port channel is enabled by default. Alternatively, the `no` version of this command enables the port channel.

Syntax	[no] shutdown						
Default	enabled						
Mode	Interface Port Channel Config						
Command History	Version 2.5.1 Introduced in the new Interface Port Channel Config mode						
Related Commands	<table> <tr> <td>interface range</td> <td>Defines an interface range and accesses the Interface Range mode</td> </tr> <tr> <td>interface port-channel</td> <td>Defines a port channel and invokes the Interface Port Channel Config mode</td> </tr> <tr> <td>shutdown (port)</td> <td>Enables or disables the selected port.</td> </tr> </table>	interface range	Defines an interface range and accesses the Interface Range mode	interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode	shutdown (port)	Enables or disables the selected port.
interface range	Defines an interface range and accesses the Interface Range mode						
interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode						
shutdown (port)	Enables or disables the selected port.						

snmp-server enable trap violation

This command is available in the Interface Port Channel Config mode. See [snmp-server enable trap violation on page 83](#) in the System Management Commands chapter.

snmp trap link-status (port channel)

This command enables link status traps for the port channel selected by the `interface port-channel` command.

Syntax [no] snmp trap link-status

The `no` version of this command disables link status traps by interface.



Note: This command is valid only when the Link Up/Down Flag is enabled. See [no, d6nEs bEsuEo rgEuCs dnugaonR, nE](#).

Mode Interface Port Channel Config

Command History	Version 2.5.1 Introduced in the new Interface Port Channel Config mode
------------------------	--

**Related
Commands**

interface range	Defines an interface range and accesses the Interface Range mode
interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode
snmp trap link-status (interface)	Enables link status traps by selected interface

spanning-tree (LAG)

This command sets the spanning-tree operational mode on the selected LAG (port channel).

The no version of this command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Syntax [no] spanning-tree

Default disabled

Mode Interface Port Channel Config

**Command
History**

Version 2.5.1	Introduced in the new Interface Port Channel Config mode
---------------	--

**Related
Commands**

interface range	Defines an interface range and accesses the Interface Range mode
interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode
snmp trap link-status (interface)	Enables link status traps by selected interface
spanning-tree	Sets the spanning-tree operational mode to enabled at the global level.

spanning-tree 0 cost (LAG)

This command sets/clears the CST cost for the port channel.

Syntax [no] spanning-tree 0 cost 1-65535

Defaults auto-calculated cost

Mode Interface Port Channel Config

**Command
History**

Version 2.5.1	Introduced in the new Interface Port Channel Config mode
---------------	--

**Related
Commands**

spanning-tree (LAG)	Sets the spanning-tree operational mode on the selected port channel
interface port-channel	Defines a port channel and invokes the Interface Port Channel Config mode

spanning-tree 0 priority (LAG)

This command sets/clears the CST priority for the port channel.

Syntax	[no] spanning-tree 0 priority 0-15
Default	8
Mode	Interface Port Channel Config
Command History	<hr/> Version 2.5.1 Introduced in the new Interface Port Channel Config mode <hr/>
Related Commands	<hr/> spanning-tree (LAG) Sets the spanning-tree operational mode on the selected port channel <hr/> interface port-channel Defines a port channel and invokes the Interface Port Channel Config mode <hr/> spanning-tree Sets the spanning-tree operational mode to enabled at the global level. <hr/>

spanning-tree MSTi cost (LAG)

This command associates/disassociates a multiple spanning tree instance with cost to the LAG (port channel).

Syntax	[no] spanning-tree MSTi 0-63 cost 1-2000000
	The MSTi number is an MST instance within a range of 0 to 63, corresponding to the new instance ID to be added.
	Note that the maximum cost value is 10 times less than the maximum cost value in FTOS.
	The no version of this command removes the multiple spanning tree instance from the port channel.
Defaults	auto-calculated cost
Mode	Interface Port Channel Config
Command History	<hr/> Version 2.5.1 Introduced in the new Interface Port Channel Config mode <hr/>
Related Commands	<hr/> spanning-tree (LAG) Sets the spanning-tree operational mode on the selected port channel <hr/> interface port-channel Defines a port channel and invokes the Interface Port Channel Config mode <hr/> spanning-tree Sets the spanning-tree operational mode to enabled at the global level. <hr/> spanning-tree msti <hr/>

spanning-tree MSTi priority (LAG)

This command is used to set/clear the priority associated with the multiple spanning tree instance for the port channel.

Syntax	[no] spanning-tree MSTi 0-63 priority 0-240
	The MSTi number is an MST instance within a range of 0 to 63.

Defaults	128 (priority)
Mode	Interface Port Channel Config
Command History	Version 2.5.1 Introduced in the new Interface Port Channel Config mode
Related Commands	interface port-channel Defines a port channel and invokes the Interface Port Channel Config mode spanning-tree (LAG) Sets the spanning-tree operational mode on the selected port channel spanning-tree Sets the spanning-tree operational mode to enabled at the global level.

spanning-tree mstp edge-port (LAG)

This command enables/disables spanning-tree MSTP edge-port mode.

Syntax	[no] spanning-tree mstp edge-port
Defaults	disabled
Mode	Interface Port Channel Config
Command History	Version 2.5.1 Introduced in the new Interface Port Channel Config mode
Related Commands	spanning-tree (LAG) Sets the spanning-tree operational mode on the selected port channel spanning-tree Sets the spanning-tree operational mode to enabled at the global level.

Spanning Tree (STP) Commands

This chapter provides a detailed explanation of the Spanning Tree commands. The commands are divided into two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.



Note: The SFTOS software platform STP default mode is IEEE 802.1s, but the legacy IEEE 802.1D mode is available. To change to the legacy IEEE 802.1D mode, set the STP operational mode to disabled, then enable the IEEE 802.1D mode. With the IEEE 802.1D mode operationally enabled, the rapid configuration and multiple instances features are not available. If the rapid configuration and multiple instances capabilities are required, use the IEEE 802.1s mode, which is compatible with the legacy IEEE 802.1D standard.

The chapter describes the following commands:

- [show spanning-tree on page 310](#)
- [show spanning-tree interface on page 311](#)
- [show spanning-tree mst detailed on page 312](#)
- [show spanning-tree mst port detailed on page 313](#)
- [show spanning-tree mst port summary on page 314](#)
- [show spanning-tree mst summary on page 314](#)
- [show spanning-tree summary on page 315](#)
- [show spanning-tree vlan on page 315](#)
- [spanning-tree on page 315](#)
- [spanning-tree bpdumigrationcheck on page 316](#)
- [spanning-tree configuration name on page 316](#)
- [spanning-tree configuration revision on page 316](#)
- [spanning-tree edgeport on page 317](#)
- [spanning-tree forceversion on page 317](#)
- [spanning-tree forward-time on page 317](#)
- [spanning-tree hello-time on page 318](#)
- [spanning-tree max-age on page 318](#)
- [spanning-tree max-hops on page 319](#)
- [spanning-tree msti on page 323](#)
- [spanning-tree msti instance on page 324](#)
- [spanning-tree msti priority on page 324](#)
- [spanning-tree msti vlan on page 325](#)
- [spanning-tree port mode enable on page 326](#)
- [spanning-tree port mode enable all on page 326](#)

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree.

Syntax `show spanning-tree [brief]`

Mode Privileged Exec and User Exec

Example 1 **Figure 19-111. Example Output from show spanning-tree Command**

```
Forcel0#show spanning-tree
Bridge Priority..... 32768
Bridge Identifier..... 80:00:00:01:E8:D5:A2:19
Time Since Topology Change..... 0 day 0 hr 46 min 23 sec
Topology Change Count..... 0
Topology Change in progress..... FALSE
Designated Root..... 80:00:00:01:E8:D5:A2:19
Root Path Cost..... 0
Root Port Identifier..... 00:00
Bridge Max Age..... 20
Bridge Max Hops..... 20
Bridge Forwarding Delay..... 15
Hello Time..... 2
Bridge Hold Time..... 3
CST Regional Root..... 80:00:00:01:E8:D5:A2:19
Regional Root Path Cost..... 0

    Associated FIDs          Associated VLANs
    -----
    1                        1
```

When the optional keyword `brief` is not included in the command, the following details are displayed:

Report Fields Bridge Priority—Specifies the bridge priority for the spanning tree.

Bridge Identifier—The bridge identifier for the selected instance.

Time Since Topology Change—The time in seconds since the topology last changed.

Topology Change Count—Number of times the topology has changed.

Topology Change in progress—Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.

Designated Root—The bridge identifier of the root bridge. It is derived from the bridge priority and the base MAC address of the bridge.

Root Path Cost—Value of the Root Path Cost parameter for the common and internal spanning tree.

Root Port Identifier—Port to access the Designated Root.

Bridge Max Age—Specifies the bridge maximum age for the spanning tree.

Bridge Forwarding Delay—Specifies the time spent in “Listening and Learning” mode before forwarding packets. Bridge Forwarding Delay must be greater or equal to “(Bridge Max Age/2) + 1”. The time range is from 4 seconds to 30 seconds. The default value is 15.

Hello Time—Configured value of the parameter for common spanning tree.

Bridge Hold Time—Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

CST Regional Root—Bridge Identifier of the common spanning tree regional root. It is derived using the bridge priority and the base MAC address of the bridge.

Regional Root Path Cost—Path cost to the common spanning tree Regional Root.

Associated FIDs—List of forwarding database identifiers currently associated with this instance.

Associated VLANs—List of VLAN IDs currently associated with this instance.

Example 2 **Figure 19-112. Example of Output from show spanning-tree brief Command**

```
Forcel0#show show spanning-tree brief
Bridge Priority..... 32768
Bridge Identifier..... 80:00:00:01:E8:D5:A2:19
Bridge Max Age..... 20
Bridge Max Hops..... 20
Bridge Hello Time..... 2
Bridge Forward Delay..... 15
Bridge Hold Time..... 3
```

When the brief optional keyword is included, this command displays spanning tree settings for the bridge. In this case, the following details are displayed:

Report Fields

Bridge Priority—Specifies the bridge priority for the spanning tree.

Bridge Identifier—The bridge identifier for the selected instance.

Bridge Max Age—Specifies the bridge maximum age for the spanning tree.

Hello Time—Configured value of the parameter for the common spanning tree.

Bridge Forward Delay—Specifies the time spent in “Listening and Learning” mode before forwarding packets. Bridge Forward Delay must be greater or equal to “(Bridge Max Age/2) + 1”. The time range is from 4 seconds to 30 seconds. The default value is 15.

Bridge Hold Time—Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

Related Commands

spanning-tree hello-time	Sets the Admin Hello Time for the selected port in the common and internal spanning tree.
--	---

show spanning-tree interface

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

Syntax show spanning-tree interface *unit/slot/port*

Mode Privileged Exec and User Exec

Report Fields Port mode—Enabled or disabled.

Port Up Time Since Counters Last Cleared—Time since port was reset, displayed in days, hours, minutes, and seconds.

Hello Time—Configured value of the parameter for common spanning tree.

STP BPDUs Transmitted—Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received—Spanning Tree Protocol Bridge Protocol Data Units received.

RST BPDUs Transmitted—Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RST BPDUs Received—Rapid Spanning Tree Protocol Bridge Protocol Data Units received.

MSTP BPDUs Transmitted—Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received—Multiple Spanning Tree Protocol Bridge Protocol Data Units received

Related Commands

spanning-tree hello-time	Sets the Admin Hello Time for the selected port in the common and internal spanning tree.
--	---

show spanning-tree mst detailed

This command displays settings and parameters for the specified multiple spanning tree instance.

Syntax show spanning-tree mst detailed *mstid*

The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance ID.

Mode Privileged Exec and User Exec

Report Fields MST Instance ID—The ID of the MST being created.

MST Bridge Priority—The bridge priority for the MST instance selected.

Time Since Topology Change—The time since the topology changed.

Topology Change Count—Number of times the topology has changed for this multiple spanning tree instance.

Topology Change in Progress—Value of the Topology Change parameter for the multiple spanning tree instance.

Designated Root—Identifier of the Regional Root for this multiple spanning tree instance.

Root Path Cost—Path Cost to the Designated Root for this multiple spanning tree instance.

Root Port Identifier—Port to access the Designated Root for this multiple spanning tree instance.

Associated FIDs—List of forwarding database identifiers associated with this instance.

Associated VLANs—List of VLAN IDs associated with this instance.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific port within a particular multiple spanning tree instance.

Syntax show spanning-tree mst port detailed *mstid unit/slot/port*

The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

The *unit/slot/port* is the desired switch port.

Mode Privileged Exec and User Exec

Report Fields MST Instance ID—The ID of the MST instance.

Port Identifier—The port identifier for the specified port within the spanning tree.

Port Priority—The priority for a particular port within the selected MST instance.

Port Forwarding State—Current spanning tree state of this port

Port Role—Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree.

Port Path Cost—Configured value of the Internal Port Path Cost parameter

Designated Root—The Identifier of the designated root for this port.

Designated Port Cost—Path Cost offered to the LAN by the Designated Port

Designated Bridge—Bridge Identifier of the bridge with the Designated Port.

Designated Port Identifier—Port on the Designated Bridge that offers the lowest cost to the LAN.

If 0 (defined as the default CIST ID) is passed as the *mstid*, then this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *unit/slot/port* is the desired switch port. In this case, the following are displayed.

Port Identifier—The port identifier for this port within the CST.

Port Priority—The priority of the port within the CST.

Port Forwarding State—The forwarding state of the port within the CST.

Port Role—The role of the specified interface within the CST.

Port Path Cost—The configured path cost for the specified interface.

Designated Root—Identifier of the designated root for this port within the CST.

Designated Port Cost—Path Cost offered to the LAN by the Designated Port.

Designated Bridge—The bridge containing the designated port

Designated Port Identifier—Port on the Designated Bridge that offers the lowest cost to the LAN

Topology Change Acknowledgement—Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.

Hello Time—The hello time in use for this port.

Edge Port—The configured value indicating if this port is an edge port.

Edge Port Status—The derived value of the edge port status. True if operating as an edge port; false otherwise.

Point To Point MAC Status—Derived value indicating if this port is part of a point to point link

CST Regional Root—The regional root identifier in use for this port

CST Port Cost—The configured path cost for this port

Related Commands

spanning-tree hello-time	Sets the Admin Hello Time for the selected port in the common and internal spanning tree.
spanning-tree edgeport	Designates the selected port as an edge port.

show spanning-tree mst port summary

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

If 0 (defined as the default CIST ID) is passed as the *mstid*, then the status summary is displayed for one or all ports within the common and internal spanning tree.

Syntax show spanning-tree mst port summary *mstid* {*unit/slot/port* | *all*}

Mode Privileged Exec and User Exec

Report Fields Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

Type—Currently not used.

STP State—The forwarding state of the port in the specified spanning tree instance

Port Role—The role of the specified port within the spanning tree.

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Syntax show spanning-tree mst summary

Mode Privileged Exec and User Exec

Report Fields MST Instance ID List

List of multiple spanning trees IDs currently configured.

For each MSTID:

Associated FIDs—List of forwarding database identifiers associated with this instance.

Associated VLANs—List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Syntax show spanning-tree summary

Mode Privileged Exec and User Exec

Report Fields Spanning Tree Adminmode—Enabled or disabled.

Spanning Tree Version—Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1D) based upon the Force Protocol Version parameter

Configuration Name—Identifier used to identify the configuration currently being used.

Configuration Revision Level—Identifier used to identify the configuration currently being used.

Configuration Digest Key—Identifier used to identify the configuration currently being used.

MST Instances—List of all multiple spanning tree instances configured on the switch

show spanning-tree vlan

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

Syntax show spanning-tree vlan *vlanid*

Mode Privileged Exec and User Exec

Report Fields VLAN Identifier—The VLANs associated with the selected MST instance.

Associated Instance—Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree

spanning-tree

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

The `no` version of this command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Syntax [no] spanning-tree

Default disabled

Mode	Global Config
Related Commands	<hr/> spanning-tree (LAG) Sets the spanning-tree operational mode on the selected port channel <hr/> spanning-tree port mode enable all <hr/>

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs.

Syntax spanning-tree bpdumigrationcheck {*unit/slot/port* | all}

To transmit a BPDU from a specified interface, use its *unit/slot/port*.

To transmit BPDUs from all interfaces, use the **all** keyword.

This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a **no** version.

Mode	Global Config
Command History	<hr/> Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode. <hr/>

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *name* is a string of at most 32 characters.

The **no** version of this command resets the Configuration Identifier Name to its default.

Syntax [no] spanning-tree configuration name *name*

Default The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.

Mode Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

The **no** version of this command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, in other words, 0.

Syntax spanning-tree configuration revision *0-65535*

Default	0
Mode	Global Config

spanning-tree edgeport

This command specifies that this port is an edge port (portfast) within the common and internal spanning tree, allowing this port to transition to forwarding state without delay.

The **no** version of this command specifies that this port is not an edge port within the common and internal spanning tree.

Syntax	[no] spanning-tree edgeport
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	<hr/> Version 2.3 Added Interface Range mode. <hr/>
Related Commands	<hr/> interface Identifies an interface and enters the Interface Config mode. <hr/> interface range Defines an interface range and accesses the Interface Range mode <hr/>

spanning-tree forceversion

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

The **no** version of this command sets the Force Protocol Version parameter to the default value, in other words, 802.1s.

Syntax [no] spanning-tree forceversion {802.1d | 802.1w | 802.1s}

The Force Protocol Version can be one of the following:

- 802.1d - STP BPDUs are transmitted rather than MST BPDUs (IEEE 802.1D functionality supported)
- 802.1w - RST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1w functionality supported)
- 802.1s - MST BPDUs are transmitted (IEEE 802.1s functionality supported)

Default	802.1s
Mode	Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

The **no** version of this command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, in other words, 15.

Syntax	[no] spanning-tree forward-time 4-30
Default	15
Mode	Global Config

spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree.

Syntax	spanning-tree hello-time 1-10
---------------	-------------------------------

The hello time value is in whole seconds within a range of 1 to 10 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

The **no spanning-tree hello-time** command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

Default	2
----------------	---

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
-------------	--

Command History	Version 2.3	Added Interface Range mode.
------------------------	-------------	-----------------------------

Related Commands	interface	Identifies an interface and enters the Interface Config mode.
	interface range	Defines an interface range and accesses the Interface Range mode
	show spanning-tree interface	Displays the settings and parameters for a specific switch port within the common and internal spanning tree
	show spanning-tree	

spanning-tree max-age

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

The **no** version of this command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, in other words, 20.

Syntax	spanning-tree max-age 6-40
	no spanning-tree max-age

Default	20
----------------	----

Mode Global Config

spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is in a range of 1 to 127.

The **no** version of this command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Syntax spanning-tree max-hops 1-127

[no] spanning-tree max-hops

Default 20

Mode Global Config **spanning-tree max-hops**

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is in a range of 1 to 127.

Default 20

Format spanning-tree max-hops <1-127>

Mode Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value, i.e. 20.

Format no spanning-tree max-hops

Mode Global Config

spanning-tree mst

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

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

If the 'external-cost' token is specified, this command sets the external-path cost for MST instance '0' i.e. CIST instance. The external pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the external pathcost value will be set based on Link Speed.

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

<i>Default</i>	<i>cost : auto</i> <i>external-cost : auto</i> <i>port-priority : 128</i>
<i>Format</i>	spanning-tree mst <mstid> { {cost <1-200000000> auto } {external-cost <1-200000000> auto } port-pri- ority <0-240> }
Mode	Interface Config

no spanning-tree mst

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

If the 'cost' token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. a pathcost value based on the Link Speed.

If the 'external-cost' token is specified, this command sets the external path cost for this port for mst '0' instance, to the default value, i.e. a pathcost value based on the Link Speed.

If the 'port-priority' token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. 128.

<i>Format</i>	<i>no spanning-tree mst <mstid> <cost external-cost port-priority></i>
<i>Mode</i>	<i>Interface Config</i>

spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree. The hellotime <value> is in whole seconds within a range of 1 to 10 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

<i>Default</i>	<i>2</i>
<i>Format</i>	<i>spanning-tree hello-time <1-10></i>
<i>Mode</i>	<i>Interface Config</i>

no spanning-tree hello-time

This command sets the admin Hello Time parameter for the common and internal spanning tree to the default value, i.e. 2.

<i>Format</i>	<i>no spanning-tree hello-time</i>
<i>Mode</i>	<i>Interface Config</i>

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree, when the optional parameter “brief” is not included in the command. The following details are displayed.

Format	<code>show spanning-tree <brief></code>
Mode	Privileged EXEC and User EXEC
Bridge Priority	Configured value.
Bridge Identifier	
Time Since Topology Change	in seconds
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	
Root Port Max Age	Derived value
Root Port Bridge Forward Delay	Derived value
Hello Time	Configured value
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)
<i>Bridge Max Hops</i>	<i>Bridge max-hops count for the device.</i>
CST Regional Root	
Regional Root Path Cost	
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

When the “brief” optional parameter is included, this command displays spanning tree settings for the bridge. In this case, the following details are displayed.

Bridge Priority	Configured value.
Bridge Identifier	
Bridge Max Age	Configured value.
<i>Bridge Max Hops</i>	<i>Bridge max-hops count for the device.</i>
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

show spanning-tree interface

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

Format	show spanning-tree interface <unit/slot/port>
Mode	Privileged EXEC and User EXEC
<i>Hello Time</i>	<i>Admin hello time for this port</i>
Port mode	Enabled or disabled.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RST BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
RST BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <unit/slot/port> is the desired switch port.

Format	show spanning-tree mst port detailed <mstid> <unit/slot/port>
Mode	Privileged EXEC and User EXEC
MST Instance ID	
Port Identifier	
Port Priority	
Port Forwarding State	Current spanning tree state of this port
Port Role	
<i>Auto-Calculate Port Path Cost</i>	<i>This indicates whether auto calculation for port path cost is enabled or not.</i>
<i>Port Path Cost</i>	<i>Configured value of the Internal Port Path Cost parameter</i>
<i>Auto-Calculate External Port Path Cost</i>	<i>This indicates whether auto calculation for external port path cost is enabled or not.</i>
<i>External Port Path Cost</i>	<i>Configured value of the external Port Path Cost parameter</i>
Designated Root	The Identifier of the designated root for this port.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <unit/slot/port> is the desired switch port. In this case, the following are displayed.

Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Port Path Cost	The configured path cost for the specified interface.
Designated Root	Identifier of the designated root for this port within the CST.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	The bridge containing the designated port
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Port Cost	The configured path cost for this port.

spanning-tree msti

This command sets the path cost or port priority for this port within the multiple spanning tree instance (MSTi) or in the common and internal spanning tree.

Syntax	spanning-tree msti {0 {cost 1-200000000 external-cost 1-200000000 priority 0-240} 1-63 {cost 1-200000000 priority 0-240}}	
Parameters	0 or 1-63	Enter an integer between 0 and 63 to specify an instance.
	{cost 1-200000000 external-cost 1-200000000 priority 0-240}	Specify a value for either cost (port cost), external-cost (external port cost for port used by a MST), or priority (port priority value, in increments of 16 (default = 128). See below. Note that the external-cost parameter is only an option for the 0 keyword.

no spanning-tree msti sets the value of the selected option to its default.

If the *msti* parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that MSTi. If, however, 0 (defined as the default CIST ID) is passed as the *msti*, then the configurations are performed for the common and internal spanning tree instance.

If the **cost** token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *msti* parameter. The path cost is specified as a number in the range of 1 to 200000000.

If the **external-cost** token is specified, this command sets the external-path cost for MST instance “0” (in other words, the CIST instance). The external-path cost is specified as a number in the range of 1 to 200000000.

If the **priority** token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *msti* parameter. The **priority** value is a number in the range of 0 to 240, in increments of 16.

Default	cost, external-cost: based on link speed; priority: 128	
Mode	Interface Config	
Command History	Version 2.5.1 Modified: Revised syntax from <code>spanning-tree mst <i>mstid</i> {{cost 1-200000000 auto} port-priority 0-240}</code>	
Related Commands	interface	Identifies an interface and enters the Interface Config mode.
	interface range	Defines an interface range and accesses the Interface Range mode
	spanning-tree MSTi cost (LAG)	Associates or disassociates a multiple spanning tree instance with cost to the selected LAG (port channel)

spanning-tree msti instance

This command adds a multiple spanning tree instance to the switch.

Syntax `spanning-tree msti instance mstid`

[oe]`spanning-tree msti instance mstid`

The instance *mstid* is a number within a range of 0 to 63, corresponding to the new instance ID to be added. The maximum number of multiple instances supported by SFTOS is 4.

The no version of this command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Mode	Global Config	
Command History	Version 2.5.1 Modified: Revised syntax from <code>spanning-tree mst instance <i>mstid</i></code>	

spanning-tree msti priority

This command sets the bridge priority for a specific multiple spanning tree instance.

Syntax `spanning-tree msti priority mstid 0–61440`

`no spanning-tree msti priority mstid`

The instance *mstid* is a number in the range *0-63* that corresponds to the desired existing multiple spanning tree instance.

0-61440 is the priority value, representing a range of 0 to 61440 in increments of 4096.

If 0 (defined as the default CIST ID) is passed as the *mstid*, this command sets the bridge priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits will be masked, in accordance with the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

The **no** version of this command sets the bridge priority for a specific multiple spanning tree instance to the default value, in other words, 32768.

Default	32768
Mode	Global Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	Version 2.5.1 Modified: Revised syntax from spanning-tree mst priority <i>mstid</i> ; changed the range.
	Version 2.3 Added Interface Range mode.
Related Commands	interface Identifies an interface and enters the Interface Config mode.
	interface range Defines an interface range and accesses the Interface Range mode

spanning-tree msti vlan

This command adds an association between a multiple spanning tree instance and a VLAN. The VLAN will no longer be associated with the common and internal spanning tree.

Syntax [no] spanning-tree msti vlan *msti vlanid*

The *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The *vlanid* corresponds to an existing VLAN ID.

The **no** version of this command removes an association between a multiple spanning tree instance and a VLAN. The VLAN will again be associated with the common and internal spanning tree. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The *vlanid* corresponds to an existing VLAN ID.

Mode	Global Config
Command History	Version 2.5.1 Modified: Revised syntax from spanning-tree mst vlan <i>mstid vlanid</i>

spanning-tree port mode enable

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

The `no` version of this command sets the Administrative Switch Port State for this port to disabled.

Syntax [no] spanning-tree port mode enable

Default disabled

Mode Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3 Modified: Added **enable** keyword. Added Interface Range and Interface VLAN modes.

Related Commands

interface	Identifies an interface and enters the Interface Config mode.
interface range	Defines an interface range and accesses the Interface Range mode
spanning-tree (LAG)	Sets the spanning-tree operational mode on the selected LAG.
spanning-tree	Enable spanning tree on the switch.
spanning-tree port mode enable all	Enable spanning tree on all ports.

spanning-tree port mode enable all

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

Syntax [no] spanning-tree port mode enable all

The `no` version of this command sets the Administrative Switch Port State for all ports to disabled.

Default disabled

Mode Global Config

Command History

Version 2.3 Modified: Added **enable** keyword.

Related Commands

spanning-tree	Enable spanning tree on the switch.
spanning-tree port mode enable	Enable spanning tree on the selected port.

Quality of Service (QoS) Commands

This chapter provides a detailed explanation of Quality of Service (QoS) commands. The chapter is divided into the following sections:

- [Class of Service \(CoS\) Commands](#)
- [Differentiated Services \(DiffServ\) Commands on page 335](#)
- [Provisioning \(IEEE 802.1p\) Commands on page 365](#)
- [Buffer Carving on page 367](#)



Note: Access Control Lists (ACLs) also factor into quality of service. For ACL commands, see [ACL Commands on page 379](#).

For details on using QoS and ACL commands, see the QoS and Access Control chapters in the *SFTOS Configuration Guide*.

Class of Service (CoS) Commands

This section provides a detailed explanation of the QoS CoS commands:

- [classofservice dot1p-mapping on page 328](#)
- [classofservice ip-dscp-mapping on page 328](#)
- [classofservice ip-precedence-mapping on page 329](#)
- [classofservice trust on page 329](#)
- [cos-queue min-bandwidth on page 330](#)
- [cos-queue strict on page 331](#)
- [traffic-shape on page 331](#)
- [show classofservice dot1p-mapping on page 331](#)
- [show classofservice ip-dscp-mapping on page 332](#)
- [show classofservice ip-precedence-mapping on page 333](#)
- [show classofservice trust on page 333](#)
- [show interfaces cos-queue on page 334](#)

By default, bandwidth is divided into 28 slices (we get 28 by adding 1 through 7—representing seven priority queues), and then it is allocated so that the highest priority queue gets the most bandwidth. When you use a CoS command to assign a priority queue, you set the priority from 0 to 6 (highest priority).



Note: Honoring 802.1p bits is enabled by default. 802.1p honoring can be disabled with `oeu` and `oetn` commands in Global Config and Interface Config modes).

Table 20-22. Default CoS Queue Prioritization

Queue	Fraction (%) of Total Bandwidth
0	1/28 (3.57%)
1	2/28 (7.14%)
2	3/28 (10.71%)
3	4/28 (14.28%)
4	5/28 (17.86%)
5	6/28 (21.43%)
6	7/28 (25%)

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class.

Syntax `classofservice dot1p-mapping userpriority trafficclass`

The *userpriority* value can range from 0-7 and *trafficclass* can range from 0-6.

The `no` form of this command is not supported.

Modes Global Config; Interface Config; Interface Port Channel Config; Interface Range, which is indicated by the `(conf-if-range-interface)#` prompt, such as `(conf-if-range-vlan 10-20)#`.

Command History

Version 2.3	Interface Range mode added
Version 2.5.1	Interface Port Channel Config mode added

Related Command

classofservice dot1p-mapping	Maps an 802.1p priority to an internal traffic class.
interface range	Defines an interface range and accesses the Interface Range mode
show classofservice dot1p-mapping	Displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface

classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class.

Syntax `classofservice ip-dscp-mapping ipdscp trafficclass`

The *ipdscp* range is from 0-63 and the *trafficclass* range is from 0-6, although the actual number of available traffic classes depends on the platform. The `no` form of this command is not supported.

Modes Global Config; Interface Config; Interface Range, which is indicated by the `(conf-if-range-interface)#` prompt, such as `(conf-if-range-vlan 10-20)#`.

Command History

Version 2.3	Interface Range mode added
-------------	----------------------------

**Related
Commands**

classofservice dot1p-mapping	Maps an 802.1p priority to an internal traffic class.
interface range	Defines an interface range and accesses the Interface Range mode

classofservice ip-precedence-mapping

This command maps an IP precedence value to an internal traffic class.

Syntax `classofservice ip-precedence-mapping ipprecedence trafficclass`

The *ipprecedence* and *trafficclass* can both range from 0-6, although the actual number of available traffic classes depends on the platform. The `no` form of this command is not supported.

Modes Global Config; Interface Config; Interface Range, which is indicated by the `(conf-if-range-interface)#` prompt, such as `(conf-if-range-vlan 10-20)#`.

**Command
History**

Version 2.3	Interface Range mode added
-------------	----------------------------

**Related
Commands**

classofservice dot1p-mapping	Maps an 802.1p priority to an internal traffic class.
interface range	Defines an interface range and accesses the Interface Range mode
show classofservice ip-dscp-mapping	Displays the current IP precedence mapping to internal traffic classes for a specific interface or for the switch

classofservice trust

Set the class of service trust mode of all interfaces or a selected interface. The mode can be set to trust one of the Dot1p (802.1p), IP Precedence, or IP DSCP packet markings.

Syntax `[no] classofservice trust { dot1p | ip-precedence | ip-dscp | untrusted }`

The `no` version of this command sets the selected interface mode to untrusted.

Parameters

<code>dot1p</code>	Sets the Class of Service Trust Mode to 802.1p.
<code>ip-precedence</code>	Sets the Class of Service Trust Mode to IP DSCP.
<code>ip-dscp</code>	Sets the Class of Service Trust Mode to IP Precedence.
<code>untrusted</code>	Sets the Class of Service Trust Mode to Untrusted.

Modes Global Config; Interface Config; Interface Range, which is indicated by the `(conf-if-range-interface)#` prompt, such as `(conf-if-range-vlan 10-20)#`.

**Command
History**

Version 2.3	Interface Range mode added
-------------	----------------------------

**Related
Commands**

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

cos-queue max-bandwidth

This command specifies the maximum transmission bandwidth limit for each interface queue. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The total number of queues supported per interface is platform specific.

Syntax `cos-queue max-bandwidth <bw-0> <bw-1> ... <bw-n>`

Modes Global Config and Interface Config

no cos-queue max-bandwidth

This command restores the default for each queue's maximum bandwidth value.

Syntax `no cos-queue max-bandwidth`

Mode Global Config and Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue.

Syntax `cos-queue min-bandwidth bw-0 bw-1 ... bw-n`

The `no cos-queue min-bandwidth` command restores the default for each queue's minimum bandwidth value.

A value from 0-100 (percentage of link rate) must be specified for each queue, with 0, for example, indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Command History

Version 2.5.1	Interface Port Channel Config mode added
---------------	--

Modes Global Config; Interface Config; Interface Port Channel Config

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the 'random-detect queue-parms' and the 'random-detect exponential-weighting-constant' commands.

The `no` version of this command disables WRED, thereby restoring the default tail drop operation for the specified queues on the interface.

Syntax `[no] cos-queue random-detect <queue-id-1> [<queue-id-2> ... <queue-id-n>]`

Modes Global Config and Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue.

The `no` version of this command restores the default weighted scheduler mode for each specified queue.

Syntax [no] `cos-queue strict queue-id-1 [queue-id-2 ... queue-id-n]`

Modes Global Config; Interface Config; Interface Port Channel Config

Command History	Version 2.5.1	Interface Port Channel Config mode added
------------------------	---------------	--

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Syntax `traffic-shape bw`

Parameters	<code>bw</code>	Enter the rate shaping bandwidth percentage from 0 to 100 in increments of 5.
-------------------	-----------------	---

Use the `no traffic-shape` command to restore the default interface rate-shaping value.

Modes Global Config; Interface Config; Interface Range, which is indicated by the `(conf-if-range-interface)#` prompt, such as `(conf-if-range-vlan 10-20)#`.

Command History	Version 2.3	Added Interface Range mode.
------------------------	-------------	-----------------------------

Related Commands	police-simple	Establish the traffic policing style for the specified class.
	interface range	Defines an interface range and accesses the Interface Range mode

Usage Information This command is only for egress (output) rate shaping. Input rate limiting is configured using a using a combination of `class-map`, `policy-map`, and `police-simple` commands. See [class-map match-all on page 338](#), [policy-map on page 354](#), and [police-simple on page 352](#).

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.

Syntax `show classofservice dot1p-mapping [unit/slot/port]`

The `unit/slot/port` parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Mode Privileged Exec

Example **Figure 20-113. Example of show classofservice dot1p-mapping Command**

```
Force10 #show classofservice dot1p-mapping 1/0/1
User Priority      Traffic Class
-----
      0              1
      1              0
      2              0
      3              1
      4              2
      5              2
      6              3
      7              3
```

The following information is repeated for each user priority.

User Priority—The 802.1p user priority value

Traffic Class—The traffic class internal queue identifier to which the user priority value is mapped

**Related
Commands**

classofservice dot1p-mapping	Maps an 802.1p priority to an internal traffic class
interface range	Defines an interface range and accesses the Interface Range mode

show classofservice ip-dscp-mapping

This command displays the current Differentiated Services Code Point (DSCP) mapping to internal traffic classes for the global configuration settings.

Syntax show classofservice ip-dscp-mapping [*unit/slot/port*]

The *unit/slot/port* parameter is optional. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Mode Privileged Exec

Example **Figure 20-114. Example of show classofservice ip-dscp-mapping Command**

```
Force10 #show classofservice ip-dscp-mapping 1/0/1
IP DSCP          Traffic Class
-----
 0(be/cs0)        1
 1                 1
 2                 1
 3                 1
 4                 1
 5                 1
 6                 1
 7                 1
 8(cs1)           0
!---output truncated -----!
```

The following information is repeated for each user priority:

IP DSCP—The IP DSCP value

Traffic Class—The traffic class internal queue identifier to which the IP Precedence value is mapped.

**Related
Commands**

classofservice	Maps an IP precedence value to an internal traffic class
ip-precedence-mapping	

show classofservice ip-precedence-mapping

This command displays the current IP precedence mapping to internal traffic classes for all interfaces or a specific interface.

Syntax show classofservice ip-precedence-mapping [*unit/slot/port*]

The *unit/slot/port* parameter is optional. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Mode Privileged Exec

Example **Figure 20-115. Example of show classofservice ip-precedence-mapping Command**

```
Forcel0 #show classofservice ip-precedence-mapping 1/0/1
User Priority      Traffic Class
-----
0                  1
1                  0
2                  0
3                  1
4                  2
5                  2
6                  3
7                  3
```

The following information is repeated for each user priority:

IP Precedence—The IP Precedence value.

Traffic Class—The traffic class internal queue identifier to which the IP Precedence value is mapped.

**Related
Commands**

classofservice	Maps an IP precedence value to an internal traffic class
ip-precedence-mapping	

show classofservice trust

This command displays the current trust mode setting for a specific interface.

Syntax show classofservice trust [*unit/slot/port*]

The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the port trust mode of the interface is displayed. If omitted, the port trust mode of each interface in the system is shown.

Mode Privileged Exec

Example **Figure 20-116. Example of show classofservice trust Command**

```
Force10 #show classofservice trust
Class of Service Trust Mode: Dot1P
```

Non-IP Traffic Class—The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP)—either 'trust ip-dscp' or 'trust ip-precedence'.

Untrusted Traffic Class—The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface.

Syntax `show interfaces cos-queue [unit/slot/port]`

The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Mode Privileged Exec

Field Descriptions **Interface**—This displays the *unit/slot/port* of the interface. If displaying the global configuration, this output line is replaced with a “Global Configuration” indication.

Interface Shaping Rate—The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface.

The following information is repeated for each queue on the interface:

Queue ID—Queue identification number

An interface supports *n* queues numbered 0 to (*n*-1). The specific *n* value is platform dependent.

Min. Bandwidth—The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort.

Scheduler Type—Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme.

Queue Management Type—The queue depth management technique used for all queues on this interface.

Differentiated Services (DiffServ) Commands

The commands in this section are:

- [diffserv on page 337](#)

Class Commands on page 337:

- [class-map match-all on page 338](#)
- [class-map rename on page 339](#)
- [match ethertype on page 340](#)
- [match any on page 340](#)
- [match class-map on page 340](#)
- [match cos on page 341](#)
- [match destination-address mac on page 341](#)
- [match dstip on page 341](#)
- [match dstl4port on page 342](#)
- [match ip dscp on page 342](#)
- [match ip precedence on page 343](#)
- [match ip tos on page 343](#)
- [match protocol on page 343](#)
- [match source-address mac on page 344](#)
- [match srcip on page 344](#)
- [match srcl4port on page 345](#)
- [match vlan on page 345](#)

Policy Commands on page 346:

- [assign-queue on page 346](#)
- [class on page 348](#)
- [conform-color on page 348](#)
- [drop on page 348](#)
- [mark cos on page 350](#)
- [mark ip-dscp on page 350](#)
- [mark ip-precedence on page 351](#)
- [police-simple on page 352](#)
- [policy-map on page 354](#)
- [policy-map rename on page 355](#)
- [redirect on page 355](#)

Service Commands on page 357:

- [service-policy on page 357](#)

Show Commands on page 358:

- [show class-map on page 358](#)
- [show diffserv on page 359](#)
- [show diffserv service on page 360](#)
- [show diffserv service brief on page 361](#)
- [show policy-map on page 362](#)
- [show policy-map interface on page 363](#)

- [show service-policy on page 364](#)

For examples of using these commands, see the DiffServ chapter in the *SFTOS Configuration Guide*.

The user configures DiffServ in several stages by specifying:

- Class:

Creating and deleting classes

Defining match criteria for a class. Note: The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

- Policy:

Creating and deleting policies

Associating classes with a policy

Defining policy statements for a policy/class combination

- Service: Adding and removing a policy to/from a directional (i.e., inbound, outbound) interface

Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

Packet processing begins by testing the match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

Note that the type of class—all, any, or acl—has a bearing on the validity of match criteria specified when defining the class. A class type of 'any' processes its match rules in an ordered sequence; additional rules specified for such a class simply extend this list. A class type of 'acl' obtains its rule list by interpreting each ACL rule definition at the time the DiffServ class is created. Differences arise when specifying match criteria for a class type 'all', since only one value for each non-excluded match field is allowed within a class definition. If a field is already specified for a class, all subsequent attempts to specify the same field fail, including the cases where a field can be specified multiple ways through alternative formats. The exception to this is when the 'exclude' option is specified, in which case this restriction does not apply to the excluded fields.

The following class restrictions are imposed by the SFTOS DiffServ design:

- Nested class support limited to:
 - 'all' within 'all'
 - no nested 'not' conditions
 - no nested 'acl' class types
 - each class contains at most one referenced class
- Hierarchical service policies not supported in a class definition
- Access list matched by reference only, and must be sole criterion in a class
 - implicit ACL 'deny all' rule also copied
 - no nesting of class type 'acl'

Regarding nested classes, referred to here as class references, a given class definition can contain at most one reference to another class, which can be combined with other match criteria. The referenced class is truly a reference and not a copy, since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes otherwise the change is rejected. A class reference may be removed from a class definition.

The user can display summary and detailed information for classes, policies and services. All configuration information is accessible via the CLI and SNMP user interfaces.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

The `no` version of this command sets the DiffServ operational mode to inactive.

Syntax [no] `diffserv`

Mode Global Config

Class Commands

The commands in this section are:

- [class-map match-all on page 338](#)
- [class-map rename on page 339](#)
- [match ethertype on page 340](#)
- [match any on page 340](#)
- [match class-map on page 340](#)
- [match cos on page 341](#)
- [match destination-address mac on page 341](#)
- [match dstip on page 341](#)
- [match dstl4port on page 342](#)
- [match ip dscp on page 342](#)
- [match ip precedence on page 343](#)
- [match ip tos on page 343](#)
- [match protocol on page 343](#)
- [match source-address mac on page 344](#)
- [match srcip on page 344](#)
- [match srcl4port on page 345](#)
- [match vlan on page 345](#)

The `class` command set is used in DiffServ to define:

- **Traffic Classification**—Specify Behavior Aggregate (BA), based on DSCP, and Multi-Field (MF) classes of traffic (name, match criteria)
- **Service Levels**—Specify the BA forwarding classes / service levels. Conceptually, DiffServ is a two-level hierarchy of classes: 1. Service/PHB, 2. Traffic Class

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic belonging to the class. Note that once a class match criterion is created for a class, it cannot be changed or deleted - the entire class must be deleted and re-created.

The CLI command root is `class-map`.

class-map match-all

This command defines a new DiffServ class of type `match-all`. The `match-all` class type indicates that all of the individual match conditions must be true for a packet to be considered a member of the class. The class type of `match-any` indicates only one of the match criteria must be true for a packet to belong to the class; multiple matching criteria are evaluated in a sequential order, with the highest precedence awarded to the first criterion defined for the class. The class type of `match-access-group` indicates the individual class match criteria are evaluated based on an access list (ACL). The `<aclid>` parameter is an integer specifying an existing ACL number (refer to the appropriate ACL documentation for the valid ACL number range). A `match-access-group` class type copies its set of match criteria from the current rule definition of the specified ACL number. All elements of a single ACL Rule are treated by DiffServ as a grouped set, similar to class type `all`. For any class, at least one class match condition must be specified for the class to be considered valid.



Note: The class match conditions are obtained from the referenced access list *at the time of class creation*. Thus, any subsequent changes to the referenced ACL definition do not affect the DiffServ class. To pick up the latest ACL definition, the DiffServ class must be deleted and re-created.

Syntax `class-map match-access-group <classmapname> <aclid>`

`class-map match-all classmapname`

`class-map existing_classmapname`



Note: The CLI mode is changed to Class Map Config when either of these commands is successfully executed. Use this mode to define or edit the class.

`class-map match-any <classmapname>`

`no class-map existing_classmapname`

The `no` version of this command eliminates an existing DiffServ class. This command may be issued at any time. If the class is currently referenced by one or more policies or by any other class, this deletion attempt shall fail.

Parameters

<code>classmapname</code>	The <code>classmapname</code> parameter is a case-sensitive alphanumeric string from 1 to 31 characters that uniquely identifies the class.
<code>existing_classmapname</code>	An existing <code>classmapname</code>



Note: The class name “default” is reserved and is not available to be defined or deleted.

Mode Global Config `class-map match-any <classmapname>`

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 enables the Class Map Config mode “(Config-classmap)#”.

The command defines how matching in the policy works. Policy statements describe what to match in the packet. For example, “class-map match-all Dallas” means “Create a policy named ‘Dallas’ that must match all statements in the policy.”

Example **Figure 20-117. Creating a Class Map**

```
!Create "Dallas" class map!
(Forcel0) (Config)#class-map match-all Dallas
(Forcel0) (Config-classmap)#match any
(Forcel0) (Config-classmap)#exit

!Further define "Dallas"!
(Forcel0) (Config)#class-map Dallas
(Forcel0) (Config-classmap)#match ip precedence 6
(Forcel0) (Config-classmap)#exit
```

Related Commands

match any	This command adds a match condition whereby all packets are considered to belong to the class.
match ip dscp	Configure the match criteria based on the DSCP value.
match ip precedence	Identify IP precedence values as match criteria.
match ip tos	This command adds a match condition based on the value of the IP TOS field in a packet
match vlan	This command adds a match condition based on the value of the Layer 2 VLAN Identifier field.
traffic-shape	ingress rate limiting

See also [Policy Commands](#) on page 346.

class-map rename

This command changes the name of a DiffServ class. The *classname* is the name of an existing DiffServ class. The *newclassname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class (Note: the class name ‘default’ is reserved and must not be used here).

Syntax class-map rename *classname newclassname*

Default none

Mode Global Config

match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The *ethertype* value is specified as one of the following keywords: `appletalk`, `arp`, `ibmsna`, `ipv4`, `ipv6`, `ipx`, `mplsmcast`, `mplsucast`, `netbios`, `novell`, `pppoe`, `rarp` or as a custom ethertype value in the range of 0x0600–0xFFFF.

Syntax `match ethertype {keyword | custom 0x0600-0xFFFF}`

Mode Class Map (The prompt is “(Config-classmap)#”.)

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Syntax `match any`

Default none

Mode Class Map (The prompt is “(Config-classmap)#”.)

match class-map

This command adds to the specified class definition the set of match conditions defined for another class.

The `no` version of this command removes from the specified class definition the set of match conditions defined for another class.

Syntax `[no] match class-map refclassname`

The *refclassname* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default none

Mode Class Map (The prompt is “(Config-classmap)#”.)

Restrictions The class types of both *classname* and *refclassname* must be identical (i.e., any vs. any, or all vs. all). A class type of `acl` is not supported by this command.

Cannot specify *refclassname* the same as *classname* (i.e., self-referencing of class name not allowed).

At most, one other class may be referenced by a class.

An attempt to delete the *refclassname* class while still referenced by a *classname* will fail.

The combined match criteria of *classname* and *refclassname* must be an allowed combination based on the class type. Any subsequent changes to the *refclassname* class match criteria must maintain this validity, or the change attempt shall fail.

The total number of class rules formed by the complete reference class chain (includes both predecessor and successor classes) must not exceed a platform-specific maximum.

In some cases, each removal of a reclass rule reduces the maximum number of available rules in the class definition by one.

match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

Syntax	match cos <i>0-7</i>
Default	none
Mode	Class Map (The prompt is “(Config-classmap)#”.)

match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet.

Syntax match destination-address mac *macaddr macmask*

The *macaddr* parameter is any Layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The *macmask* parameter is a Layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Default	none
Mode	Class Map (The prompt is “(Config-classmap)#”.)

match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet.

Syntax match dstip *ipaddr ipmask*

The *ipaddr* parameter specifies an IP address. The *ipmask* parameter specifies an IP address bit mask; note that although similar to a standard subnet mask, this bit mask need not be contiguous.

Default	none
Mode	Class Map (The prompt is “(Config-classmap)#”.)

match dstl4port

This command adds to the specified class definition a match condition based on the destination Layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

Syntax `match dstl4port {portkey | 0-65535} [0-65535]`

To specify the match condition as a single keyword, the value for *portkey* is one of the supported port name keywords. The currently supported *portkey* values are: `domain`, `echo`, `ftp`, `ftpdata`, `http`, `smtp`, `snmp`, `telnet`, `ftp`, `www`. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition using a numeric notation, one Layer 4 port number is required. The port number is an integer from 0 to 65535.

To specify the match condition using a numeric range notation, two Layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default none

Mode Class Map (The prompt is “(Config-classmap)#”.)

match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

Syntax `match ip dscp dscpval`

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: `af11`, `af12`, `af13`, `af21`, `af22`, `af23`, `af31`, `af32`, `af33`, `af41`, `af42`, `af43`, `be`, `cs0`, `cs1`, `cs2`, `cs3`, `cs4`, `cs5`, `cs6`, `cs7`, `ef`, as described in [mark ip-dscp on page 350](#)

Note: The IP DSCP, IP precedence, and IP TOS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default none

Mode Class Map (The prompt is “(Config-classmap)#”.)

match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked).



Note: The IP DSCP, IP precedence, and IP TOS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Syntax match ip precedence *0-6*

The precedence value is an integer from 0 to 6.

Default none

Mode Class Map (The prompt is “(Config-classmap)#”.)

match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header.

Syntax match ip tos *tosbits tosmask*

The value of *tosbits* is a two-digit hexadecimal number from 00 to ff. The value of *tosmask* is a two-digit hexadecimal number from 00 to ff.

The *tosmask* denotes the bit positions in *tosbits* that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a *tosbits* value of a0 (hex) and a *tosmask* of a2 (hex).



Note: The IP DSCP, IP precedence, and IP TOS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Note: In essence, this the “free form” version of the IP DSCP/Precedence/TOS match specification in that the user has complete control of specifying which bits of the IP Service Type field are checked.

Default none

Mode Class Map (The prompt is “(Config-classmap)#”.)

match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

Syntax match protocol {protocol-name | 0-255}

To specify the match condition using a single keyword notation, the value for *protocol-name* is one of the supported protocol name keywords. The currently supported values are: *icmp*, *igmp*, *ip*, *tcp*, *udp*. Note that a value of *ip* is interpreted to match all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Note: This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Mode	Class Map (The prompt is “(Config-classmap)#”.)

match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet.

Syntax	match source-address mac <i>address macmask</i>
---------------	---

The *address* parameter is any Layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff).

The *macmask* parameter is a Layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Default	none
Mode	Class Map (The prompt is “(Config-classmap)#”.)

match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Syntax	match srcip <i>ipaddr ipmask</i>
---------------	----------------------------------

The *ipaddr* parameter specifies an IP address.

The *ipmask* parameter specifies an IP address bit mask; note that although it resembles a standard subnet mask, this bit mask need not be contiguous.

Default	none
Mode	Class Map (The prompt is “(Config-classmap)#”.)

match srcl4port

This command adds to the specified class definition a match condition based on the source Layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

Syntax `match srcl4port {portkey | 0-65535} [0-65535]`

To specify the match condition as a single keyword notation, the value for *portkey* is one of the supported port name keywords. The currently supported *portkey* values are: `domain`, `echo`, `ftp`, `ftpdata`, `http`, `smtp`, `snmp`, `telnet`, `ftp`, `www`. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one Layer 4 port number is required. The port number is an integer from 0 to 65535.

To specify the match condition as a range, two Layer 4 port numbers are required, and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default None

Mode Class Map (The prompt is “(Config-classmap)#”.)

match vlan

This command adds to the specified class definition a match condition based on the value of the Layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet).

Syntax `match vlan 1-3965`

The VLAN ID is an integer from 1 to 3965.

Default None

Mode Class Map (The prompt is “(Config-classmap)#”.)

Policy Commands

The commands described in this section are:

- [assign-queue on page 346](#)
- [class on page 348](#)
- [conform-color on page 348](#)
- [drop on page 348](#)
- [mark cos on page 350](#)
- [mark ip-dscp on page 350](#)
- [mark ip-precedence on page 351](#)
- [police-simple on page 352](#)
- [policy-map on page 354](#)
- [policy-map rename on page 355](#)
- [redirect on page 355](#)

The `policy` command set is used in DiffServ to define:

- **Traffic Conditioning**—Specify traffic conditioning actions (policing, marking, shaping) to apply to traffic classes.
- **Service Provisioning**—Specify bandwidth and queue depth management requirements of service levels (EF, AF, etc.).

The policy commands are used to associate a traffic class, which was defined by the `class` command set, with one or more QoS policy attributes. This association is then assigned to an interface to form a service. The user specifies the policy name when the policy is created.

The DiffServ CLI does not necessarily require that users associate only one traffic class to one policy. In fact, multiple traffic classes can be associated with a single policy, each defining a particular treatment for packets that match the class definition. When a packet satisfies the conditions of more than one class, preference is based on the order in which the classes were added to the policy, with the foremost class taking highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes. Note that the only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

Class instances are always added to the end of an existing policy. While existing class instances may be removed, their previous location in the policy is not reused, so the number of class instance additions/removals is limited. In general, significant changes to a policy definition require that the entire policy be deleted and re-created with the desired configuration.

The CLI command root is `policy-classmap`.

assign-queue

This command modifies the queue ID to which the associated traffic stream is assigned.

Syntax `assign-queue queueid`

The *queueid* is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

Mode Policy Class (The prompt is “(Policy-classmap Config)#”.)

bandwidth kbps

This command identifies a minimum amount of bandwidth to be reserved for the specified class instance within the named policy using an absolute rate notation. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295.



Note: The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

Note: The bandwidth kbps and percent commands are alternative ways to specify the same bandwidth policy attribute.

Syntax bandwidth kbps <1-4294967295>

Mode Policy-classmap Config

Restrictions The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.

Policy Type—Out

Incompatibilities—Expedite (all forms)

bandwidth percent

This command identifies a minimum amount of bandwidth to be reserved for the specified class instance within the named policy using a relative rate notation. The committed information rate is specified as a percentage of total link capacity and is an integer from 1 to 100.



Note: The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

Note: The bandwidth kbps and percent commands are alternative ways to specify the same bandwidth policy attribute.

Syntax bandwidth percent <1-100>

Mode Policy-classmap Config

Restrictions The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.

Policy Type	Out
Incompatibilities	Expedite (all forms)

class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. Note that this command causes the specified policy to create a reference to the class definition.



Note: The CLI mode is changed to Policy Class mode (“Policy-classmap Config”) when this command is successfully executed.

The **no** version of this command deletes the instance of a particular class and its defined treatment from the specified policy. Note that this command removes the reference to the class definition for the specified policy.

Syntax [no] class *classname*

The *classname* is the name of an existing DiffServ class.

Mode Policy Map (The prompt is “(Config-policy-map)#”)

conform-color

This command is used to enable color-aware traffic policing and define the conform-color and exceed-color class maps used. Use in conjunction with the **police-simple** command where the fields for the conform level are specified.

The **no** version of this command disables the color-aware traffic policing and mapping.

Syntax conform-color *class-map-name* [exceed-color *class-map-name*]

no conform-color

The *class-map-name* parameter is the name of an existing Diffserv class map, where different ones must be used for the conform and exceed colors.

Mode Policy Class (The prompt is “(Policy-classmap Config)#”.)

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Syntax drop

Mode Policy Class (The prompt is “(Policy-classmap Config)#”.)

expedite kbps

This command identifies the maximum guaranteed amount of bandwidth to be reserved for the specified class instance within the named policy using an absolute rate notation. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The optional committed burst size is specified in kilobytes (KB) as an integer from 1 to 128, with a default of 4.

The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.



Note: The expedite kbps and percent commands are alternative ways to specify the same expedite policy attribute.

Syntax expedite kbps <1-4294967295> [1-128]

Mode Policy-classmap Config

Restrictions The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.

Policy Type Out

Incompatibilities Bandwidth (all forms), Shape Peak

expedite percent

This command identifies the maximum guaranteed amount of bandwidth to be reserved for the specified class instance within the named policy using a relative rate notation. The committed information rate is specified as a percentage of total link capacity and is an integer from 1 to 100. The optional committed burst size is specified in kilobytes (KB) as an integer from 1 to 128, with a default of 4.



Note: The actual bandwidth allocation does not occur until the policy is attached to an interface in a particular direction.

Note: The expedite kbps and percent commands are alternative ways to specify the same expedite policy attribute.

Syntax expedite percent <1-100> [1-128]

Mode Policy-classmap Config

Restrictions The sum of the committed information rate values for all bandwidth and expedite commands defined within a policy must not exceed the available link bandwidth of the interface to which that policy is assigned. Violation of this requirement shall prevent successful attachment of a policy to the interface, or shall cause this command to fail if the policy is already in service on one or more interfaces.

Policy Type Out**Incompatibilities** Bandwidth (all forms), Shape Peak

mark cos

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted.

Syntax mark cos *0-7*

The cos value is an integer from 0 to 7.

Default 1**Mode** Policy Class (The prompt is “(Config-policy-classmap)#”)**Policy Type** In

mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

Syntax mark ip-dscp *dscpval*

The *dscpval* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The Assured Forwarding (AF) and Best Effort (BE) codepoints are described in RFC 2597. The Class Selector (CS) code points are defined in RFC 2474. The Expedited Forwarding (EF) codepoint is described in RFC 2598.

Class selector DSCPs (CS0 through CS7) are values that are backward-compatible with IP precedence. When converting between IP precedence and DSCP, match the three most significant bits. For example cs5 is 101000, which is 0x28 (40 decimal in the table below).

[Table 20-23 on page 350](#) shows an example of the mapping of numeric values to keywords. Note that these numbers are base10 while the RFC refers to these in binary. For example, ef is shown below as 46, which the RFC specifies as 101110.

Table 20-23. Mapping of DSCP Keywords to Numerical Codepoints

DSCP Keywords	Numeric Codepoints
AF11	10
AF12	12
AF13	14
AF21	18

Table 20-23. Mapping of DSCP Keywords to Numerical Codepoints

DSCP Keywords	Numeric Codepoints
AF22	20
AF23	22
AF31	26
AF32	28
AF33	30
AF41	34
AF42	36
AF43	38
BE	0
CS0	0
CS1	8
CS2	16
CS3	24
CS4	32
CS5	40
CS6	48
CS7	56
EF	46

Mode Policy Class (The prompt is “(Config-policy-classmap)#”)

Policy Type In

Incompatibilities Mark IP Precedence, Police (all forms)

mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value.

Syntax mark ip-precedence *0-7*

The IP Precedence value is an integer from 0 to 7.

Mode Policy Class (The prompt is “(Config-policy-classmap)#”)

Policy Type In

Incompatibilities Mark IP DSCP, Police (all forms)

police-simple

This command establishes the traffic policing style for the specified class.

Syntax `police-simple {1-4294967295 1-128 conform-action {drop | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | set-cos-transmit 0-7 | set-secondary-cos-transmit 0-7 | transmit} [violate-action drop]}`

The simple form of the command uses a single data rate and burst size, resulting in two outcomes: conform and nonconform.

The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each conforming outcome (conform-action), the possible actions are `drop`, `set-cos-transmit`, `set-sec-cos-transmit`, `set-dscp-transmit`, `set-prec-transmit`, or `transmit`.

For `set-dscp-transmit`, a *dscpval* value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: `af11`, `af12`, `af13`, `af21`, `af22`, `af23`, `af31`, `af32`, `af33`, `af41`, `af42`, `af43`, `be`, `cs0`, `cs1`, `cs2`, `cs3`, `cs4`, `cs5`, `cs6`, `cs7`, `ef`, as described in [mark ip-dscp on page 350](#).

For `set-prec-transmit`, an IP Precedence value is required and is specified as an integer from 0-7.

In this version of SFTOS, the `violate-action` is limited to `drop`.

Defaults In this simple form of the `police` command, the conform action defaults to `transmit` and the violate action defaults to `drop`. These actions can be set with this command once the style has been configured.

Mode Policy Class (The prompt is “(Config-policy-classmap)#”)

Restrictions Only one style of the `police` command (`police-simple`) is allowed for a given class instance in a particular policy.

Policy Type In

Incompatibilities Mark IP DSCP, Mark IP Precedence

Related Commands

class-map match-all	Defines a new DiffServ class of type match-all.
class	Creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.
traffic-shape	Specifies the maximum transmission bandwidth limit for the interface as a whole. Used for egress rate shaping only.

police-single-rate

This command is used to establish the traffic policing style for the specified class. The single-rate form of the police command uses a single data rate and two burst sizes, resulting in three outcomes: conform, exceed and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) as an integer from 1 to 128. The exceeding burst size is specified in kilobytes (KB) as an integer from 1 to 128. Note that the exceeding burst size must be equal to or greater than the conforming burst size.

For each outcome, the only possible actions are **drop**, **set-cos-transmit**, **set-sec-cos-transmit**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**. In this singlerate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For **set-dscp-transmit**, a *<dscpval>* value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **ef**.

For **set-prec-transmit**, an IP Precedence value is required and is specified as an integer from 0-7.

Syntax `police-single-rate {<1-4294967295> <1-128> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | set-secondary-cos-transmit <0-7> | transmit} exceed-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | set-secondary-cos-transmit <0-7> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | set-secondary-cos-transmit <0-7> | transmit}]}`

Mode Policy-classmap Config

Restrictions Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.

Policy Type In

Incompatibilities Mark IP DSCP, Mark IP Precedence

police-two-rate

This command is used to establish the traffic policing style for the specified class. The two-rate form of the police command uses two data rates and two burst sizes, resulting in three outcomes: conform, exceed and violate. The first two data parameters are the conforming data rate and burst size. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295, while the conforming burst size is specified in kilobytes (KB) as an integer from 1 to 128. The next two data parameters are the peak data rate and burst size. The peak data rate is specified in kilobits-per-second (Kbps) as an integer from 1 to 4294967295, while the peak burst size is specified in kilobytes (KB) as an integer from 1 to 128. Note that the peak data rate must be equal to or greater than the conforming data rate.

For each outcome, the only possible actions are **drop**, **set-cos-transmit**, **set-sec-cos-transmit**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**. In this two-rate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

For set-dscp-transmit, a <dscpval> value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

Syntax police-two-rate {<1-4294967295> <1-128> <1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | set-secondary-cos-transmit <0-7> | transmit} exceed-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | set-secondary-cos-transmit <0-7> | transmit} [violate-action {drop | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | set-secondary-cos-transmit <0-7> | transmit}]}

Mode Policy-classmap Config

Restrictions Only one style of police command (simple, singlerate, tworate) is allowed for a given class instance in a particular policy.

Policy Type In

Incompatibilities Mark IP DSCP, Mark IP Precedence

policy-map

This command establishes a new DiffServ policy.

Syntax policy-map *polycyname* in

The *polycyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound direction.

The in parameter is required. SFTOS supports only the ingress direction.



Note: The policy type dictates which of the individual policy attribute commands are valid within the policy definition.

Note: The CLI mode is changed to Policy Map when this command is successfully executed.

The no policy-map *polycyname* command eliminates an existing DiffServ policy. The *polycyname* parameter is the name of an existing DiffServ policy. This command may be issued at any time; if the policy is currently referenced by one or more interface service attachments, this deletion attempt shall fail.

Mode Global Config

Command History

Version 2.5.1.0

Modified: The maximum number of policies that can be configured is changed from 64 to 128.

policy-map rename

This command changes the name of a DiffServ policy.

Syntax `policy-map rename policyname newpolicyname`

The *policyname* is the name of an existing DiffServ class. The *newpolicyname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Mode Global Config

mark secondary-cos

This command marks all packets for the associated traffic stream with the specified secondary class of service value (the inner 802.1Q tag of a double VLAN tagged packet) in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Syntax `mark secondary-cos <0-7>`

Mode Policy-Class-Map Config

redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port channel).

Syntax `redirect unit/slot/port`

Mode Policy Class (The prompt is “(Policy-classmap Config)#”.)

randomdrop

This command changes the active queue depth management scheme from the default tail drop to RED. The first two data parameters are the average queue depth minimum and maximum threshold values specified in bytes. The minimum threshold is an integer from 1 to 250000. The maximum threshold is an integer from 1 to 500000, but it must be equal to or greater than the minimum threshold. The third data parameter is the maximum drop probability and is an integer from 0 to 100. It indicates the percentage likelihood that a packet will be dropped when the average queue depth reaches the maximum threshold value.

The remaining parameters are all optional. The fourth data parameter is the sampling rate, indicating the period at which the queue is sampled for computing the average depth. Expressed in microseconds, the sampling rate is an integer from 0 to 1000000, with a default of 0 (meaning per-packet sampling). The last parameter is the decay exponent, which determines how quickly the average queue length calculation decays over time, with a higher number producing a faster rate of decay. This value is an integer from 0 to 16, with a default of 9.

The last two parameters, namely sampling rate and decay exponent, are hierarchically specified in this command. That is, in order to provide a value for the decay exponent `<0-16>`, the user is required to also specify a sampling rate `<0-1000000>` for proper command interpretation.

Syntax	<code>randomdrop <1-250000> <1-500000> <0-100> [<0-1000000> [<0-16>]]</code>
Mode	Policy-classmap Config
Policy Type	Out

shape average

This command is used to establish average rate traffic shaping for the specified class, which limits transmissions for the class to the committed information rate, with excess traffic delayed via queueing. The committed information rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295.



Note: Queue depth management defaults to tail drop, but the `randomdrop` command can be used to change to a RED scheme.

Syntax	<code>shape average <1-4294967295></code>
Mode	Policy-classmap Config
Restrictions	This shaping rate must not exceed the maximum link data rate of the interface to which the policy is applied.
Policy Type	Out

shape peak

This command is used to establish peak rate traffic shaping for the specified class, which allows transmissions for the class to exceed the committed information rate by sending excess traffic with the understanding that it could be dropped by a downstream network element. Two rate parameters are used, a committed information rate and a peak information rate. Each of these rates is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The peak rate must be specified as equal to or greater than the committed rate.



Note: Queue depth management defaults to tail drop, but the `randomdrop` command can be used to change to a RED scheme.

Syntax	<code>shape peak <1-4294967295> <1-4294967295></code>
Mode	Policy-classmap Config
Restrictions	Neither of the shaping rate parameters is allowed to exceed the maximum link data rate of the interface to which the policy is applied.
Policy Type	Out

Incompatibilities Expedite (all forms)

Service Commands

The `service` command set consists of `service-policy` and `show service`. The `service-policy` command assigns a DiffServ traffic conditioning policy (as specified by the policy commands) to an interface in the incoming direction. Only one policy may be assigned at any one time to an interface.

service-policy

This command attaches a policy to an interface in a particular direction. However, this version of SFTOS limits the direction to ingress. The command can be used in the Interface Config mode to attach a policy to a specific interface. Alternatively, the command can be used in the Global Config mode to attach the policy to all system interfaces.

Note that this command causes a service to create a reference to the policy.



Note: This command effectively enables DiffServ on an interface (in a particular direction). There is no separate interface administrative 'mode' command for DiffServ.

Note: This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition such that it would result in a violation of the interface capabilities will cause the policy change attempt to fail.

Syntax [no] `service-policy` in *policy-map-name*

The `in` parameter is required. SFTOS supports only the ingress direction.

The *policy-map-name* parameter is the name of an existing DiffServ policy.

The `no` version of this command detaches a policy from an interface in the ingress direction. The command can be used in the Interface Config mode to detach a policy from a specific interface. Alternatively, the command can be used in the Global Config mode to detach this policy from all system interfaces to which it is currently attached. Note that this command causes a service to remove its reference to the policy.



Note: This command effectively disables DiffServ on an interface (in a particular direction). There is no separate interface administrative 'mode' command for DiffServ.

Modes Global Config (for all system interfaces); Interface Config (for a specific interface); Interface Port Channel Config; Interface Range Port Channel; Interface Range Ethernet

Command History

Version 2.5.1	Added Interface Port Channel Config mode
---------------	--

Related Commands

interface	Selects an interface and accesses the Interface Config mode
policy-map	Establishes a new DiffServ policy
show service-policy	Display a summary of policy-oriented statistics information for all interfaces.

Show Commands

The commands in this section are:

- [show class-map on page 358](#)
- [show diffserv on page 359](#)
- [show policy-map on page 362](#)
- [show diffserv service on page 360](#)
- [show diffserv service brief on page 361](#)
- [show policy-map interface on page 363](#)
- [show service-policy on page 364](#)

The DiffServ **show** commands display configuration and status information for:

- Classes
- Policies
- Services

This information can be displayed in either summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled; it is suppressed otherwise.

There is also a **show** command for general DiffServ information that is available at any time.

show class-map

This command displays all configuration information for the specified class.

Syntax `show class-map [classname]`

Parameters

<i>classname</i>	(Optional) Enter an existing DiffServ class name. Class names must be composed of alphanumeric characters.
------------------	--

Mode Privileged Exec and User Exec

Example **Figure 20-118. Example of show class-map Command**

```
Force10 #show class-map
```

Class Name	Class Type	Reference Class Name
-----	-----	-----

Field Descriptions

If a class name is specified, the following fields are displayed:

Class Name—The name of this class

Class Type—The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match. For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.

Match Criteria—The Match Criteria fields are only be displayed if they have been configured. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Class of Service, Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, Source Layer 4 Port, Source MAC Address, COS, **Secondary COS**, and VLAN, **Secondary VLAN**, and **Ethertype**.

Values—This field displays the values of the Match Criteria.

Excluded—This field indicates whether or not this Match Criteria is excluded.

If the Class Name is *not* specified, this command displays a list of all defined DiffServ classes. The following fields are displayed:

Class Name—The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)

Class Type—The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match. For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.

ACL Number—The ACL number used to define the class match conditions at the time the class was created. This field is only meaningful if the class type is acl. (Note that the contents of the ACL may have changed since this class was created.)

Ref Class Name—The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Syntax show diffserv

Mode Privileged Exec

Example **Figure 20-119. Example of Output from the show diffserv Command**

```

Force10 #show diffserv
DiffServ Admin mode..... Enable
Class Table Size Current/Max..... 0 / 25
Class Rule Table Size Current/Max..... 0 / 150
Policy Table Size Current/Max..... 0 / 64
Policy Instance Table Size Current/Max..... 0 / 576
Policy Attribute Table Size Current/Max..... 0 / 1728
Service Table Size Current/Max..... 0 / 400

```

Field Descriptions

DiffServ Admin mode —The current value of the DiffServ administrative mode

Class Table Size Current — The current number of entries (rows) in the Class Table

Class Table Max — The maximum allowed entries (rows) for the Class Table

Class Rule Table Size Current — The current number of entries (rows) in the Class Rule Table

Class Rule Table Max — The maximum allowed entries (rows) for the Class Rule Table

Policy Table Size Current — The current number of entries (rows) in the Policy Table

Policy Table Max — The maximum allowed entries (rows) for the Policy Table

Policy Instance Table Size Current — The current number of entries (rows) in the Policy Instance Table

Policy Instance Table Max — The maximum allowed entries (rows) for the Policy Instance Table

Policy Attribute Table Size Current — The current number of entries (rows) in the Policy Attribute Table

Policy Attribute Table Max — The maximum allowed entries (rows) for the Policy Attribute Table

Service Table Size Current — The current number of entries (rows) in the Service Table

Service Table Max — The maximum allowed entries (rows) for the Service Table

show diffserv service

This command displays policy service information for the specified interface and direction.

Syntax `show diffserv service { unit/slot/port | 1-3965 | brief } in`

The *unit/slot/port* parameter specifies a valid port number for the system.

For *1-3965*, enter an integer between 1 and 3965, representing a valid VLAN ID. Routing must be enabled on the VLAN.

The *in* parameter indicates the ingress direction of the interface.

Mode Privileged Exec

Example **Figure 20-120. Example of Output from the show diffserv service Command**

```
Forcel0 #show diffserv service 1/0/1 in
DiffServ Admin mode..... Enable
Interface..... 1/0/1
Direction..... In
No policy is attached to this interface in this direction.
```

Report Fields

When a policy is attached to the designated interface, the fields in the report are:

DiffServ Admin Mode—The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.

Interface—Valid unit, slot and port number separated by forward slashes.

Direction—The traffic direction of this interface service, either in or out

Operational Status—The current operational status of this DiffServ service interface

Policy Name—The name of the policy attached to the interface in the indicated direction

Policy Details—Attached policy details, whose content is identical to that described for the show policy-map *polycymapname* command (content not repeated here for brevity)

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached.

Syntax show diffserv service brief [in]

This version of SFTOS only supports the ingress direction, so the report lists the same information whether or not the in direction parameter is specified.

Mode Privileged Exec

Report Fields

DiffServ Mode—The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Interface—Valid unit, slot and port number separated by forward slashes.

Direction—The traffic direction of this interface service, either in or out

OperStatus—The current operational status of this DiffServ service interface

Policy Name—The name of the policy attached to the interface in the indicated direction

show policy-map

This command displays all configuration information for the specified policy.

Syntax show policy-map [*policyname*]

The *policyname* is the name of an existing DiffServ policy.

Mode EXEC Privilege

Report Fields Mark Secondary COS—Denotes the secondary class of service value that is set in the 802.1p header of outbound packets. This is not displayed if the mark secondary-cos was not specified.

Conform COS—The action to be taken on conforming packets per the policing metrics.

Conform Secondary COS—The action to be taken on packets conforming with the secondary class of service value per the policing metrics.

Exceed COS—The action to be taken on excess packets per the policing metrics.

Exceed Secondary COS—The action to be taken on excess packets conforming with the secondary class of service value per the policing metrics.

Non-Conform COS—The action to be taken on violating packets per the policing metric.

Non-Conform Secondary COS—The action to be taken on violating packets conforming with the secondary class of service per the policing metric.

Assign Queue—Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.

Drop—Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.

Redirect—Forces a classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

If the policy name is specified, the following fields are displayed:

Policy Name—The name of this policy

Policy Type—The policy type, namely whether it is an inbound or outbound policy definition

Class Name—The name of this class. The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Mark CoS—Denotes the class of service value that is set in the 802.1p header of outbound packets. This is not displayed if the mark cos was not specified.

Mark IP DSCP—Denotes the mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if policing is in use for the class under this policy.

Mark IP Precedence—Denotes the mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if either mark DSCP or policing is in use for the class under this policy.

Policing Style—This field denotes the style of policing, if any, used (police-simple).

Committed Rate (Kbps)—This field displays the committed rate, used in simple policing.

Committed Burst Size (KB)—This field displays the committed burst size, used in simple policing.

Conform Action—The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.

Conform DSCP Value—This field shows the DSCP mark value if the conform action is markdscp.

Conform IP Precedence Value—This field shows the IP Precedence mark value if the conform action is markprec.

Exceed Action—The current setting for the action taken on a packet considered to exceed to the policing parameters. This is not displayed if policing not in use for the class under this policy.

Exceed DSCP Value—This field shows the DSCP mark value if this action is markdscp.

Exceed IP Precedence Value—This field shows the IP Precedence mark value if this action is markprec.

Non-Conform Action—The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.

Non-Conform DSCP Value—This field displays the DSCP mark value if this action is markdscp.

Non-Conform IP Precedence Value—This field displays the IP Precedence mark value if this action is markprec.

Bandwidth—This field displays the minimum amount of bandwidth reserved in either percent or kilobits-per-second.

Expedite Burst Size (KBytes)—This field displays the maximum guaranteed amount of bandwidth reserved in either percent or kilobits-per-second format.

Shaping Average—This field is displayed if average shaping is in use. Indicates whether average or peak rate shaping is in use, along with the parameters used to form the traffic shaping criteria, such as CIR and PIR. This is not displayed if shaping is not configured for the class under this policy.

Shape Committed Rate (Kbps)—This field is displayed if average or peak rate shaping is in use. It displays the shaping committed rate in kilobits-per-second.

Shape Peak Rate (Kbps)—This field is displayed if peak rate shaping is in use. It displays the shaping peak rate in kilobits-per-second.

If the policy name is not specified, this command displays a list of all defined DiffServ policies. The following fields are displayed:

Policy Name—The name of this policy. (Note that the order in which the policies are displayed is not necessarily the same order in which they were created.)

Policy Type—The policy type, namely whether it is an inbound or outbound policy definition.

Class Members—List of all class names associated with this policy.

show policy-map interface


This command displays policy-oriented statistics information for the specified interface and direction.



Note: This command is only allowed while the DiffServ administrative mode is enabled.

Syntax show policy-map interface *unit/slot/port* in

The *unit/slot/port* parameter specifies a valid interface for the system. The direction parameter indicates the interface direction of interest.

Report Fields	<p>Interface—Valid unit, slot and port number separated by forward slashes.</p> <p>Direction—The traffic direction of this interface service, either in or out. Note: SFTOS only supports a policy-map in the “in” direction.</p> <p>Operational Status—The current operational status of this DiffServ service interface.</p> <p>Policy Name—The name of the policy attached to the interface in the indicated direction.</p> <p>Interface Offered Octets/Packets—A cumulative count of the octets/packets offered to this service interface in the specified direction before the defined DiffServ treatment is applied.</p> <p>Interface Discarded Octets/Packets—A cumulative count of the octets/packets discarded by this service interface in the specified direction for any reason due to DiffServ treatment.</p> <p>Interface Sent Octets/Packets—A cumulative count of the octets/packets forwarded by this service interface in the specified direction after the defined DiffServ treatment was applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element.</p> <p>The following information is repeated for each class instance within this policy:</p> <p>Class Name—The name of this class instance.</p> <p>In Offered Octets/Packets—A count of the octets/packets offered to this class instance before the defined DiffServ treatment is applied. Only displayed for the 'in' direction.</p> <p>In Discarded Octets/Packets—A count of the octets/packets discarded for this class instance for any</p> <p> Note: None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.</p>
----------------------	--

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction (SFTOS currently only supports the ingress direction.) This command enables or disables the route reflector client. A route reflector client relies on a route reflector to re-advertise its routes to the entire AS. The possible values for this field are **enable** and **disable**.

Syntax show service-policy in

Mode Privileged Exec

The following information is repeated for each interface (only those interfaces configured with an attached policy are shown):

Report Fields	<p>Intf—Interface: Valid unit, slot and port number separated by forward slashes.</p> <p>Oper Stat—Operational Status: The current operational status of this DiffServ service interface.</p> <p>Offered Packets—A count of the total number of packets offered to all class instances in this service before their defined DiffServ treatment is applied. These are overall per-interface per-direction counts.</p>
----------------------	--

Discarded Packets—A count of the total number of packets discarded for all class instances in this service for any reason due to DiffServ treatment. These are overall per-interface per-direction counts.

Sent Packets—A count of the total number of packets forwarded for all class instances in this service after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function or an outbound link transmission element. These are overall per-interface per-direction counts.

Policy Name—The name of the policy attached to the interface.



Note: None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

Provisioning (IEEE 802.1p) Commands

The commands described in this section are:

- [classofservice dot1pmapping on page 365](#)
- [dot1p-priority on page 366](#)
- [show classofservice dot1pmapping on page 366](#)
- [vlan port priority all on page 366](#)
- [vlan priority on page 366](#)

classofservice dot1pmapping

This command maps an 802.1p priority to an internal traffic class for a device when in Global Config mode. The number of available traffic classes may vary with the platform.

Syntax `classofservice dot1pmapping userpriority trafficclass`

The *userpriority* and *trafficclass* can both be in the 0–6 range.

Mode Global Config or Interface Config

Mode Interface Config; Interface Range, which is indicated by the (conf-if-range-*interface*)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Interface Range mode added
-------------	----------------------------

Related Commands

classofservice dot1p-mapping	Maps an 802.1p priority to an internal traffic class.
--	---

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

dot1p-priority

This command configures the 802.1p port priority, from 0 to 7, assigned to untagged packets for a specific interface.

Syntax	dot1p-priority <i>0–7</i>
Default	0
Mode	Interface Port Channel Config
Command History	<hr/> Version 2.5 Introduced. Replaces vlan priority for port channel ports (LAG ports) <hr/>

show classofservice dot1pmapping

This command displays the current 802.1p priority mapping to internal traffic classes for all or specific interfaces.

Syntax	show classofservice dot1pmapping [<i>unit/slot/port</i>]
Mode	Privileged Exec and User Exec

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device.

Syntax	vlan port priority all <i>priority</i>
---------------	--

The range for *priority* is 0-6. Any subsequent per port configuration will override this configuration setting.

Mode	Global Config
-------------	---------------

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface.

Syntax	vlan priority <i>priority</i>
---------------	-------------------------------

The range for *priority* is 0-6.

Default	0
----------------	---


Mode	Interface Config	
Command History	Version 2.5	Replaced, in part, by dot1p-priority , for port channel ports.

Buffer Carving

The commands in this section are:

- [buffer dedicated \(1G and stacking ports\) on page 368](#)
- [buffer dedicated interface \(10G ports\) on page 369](#)
- [buffer dynamic \(1G and stack ports\) on page 370](#)
- [buffer dynamic interface \(S25P\) on page 372](#)
- [buffer dynamic interface system-downlink on page 372](#)
- [buffer packets interface on page 373](#)

Buffer carving (also called buffer tuning, which is manual allocation of the memory in the switch ASICs) is new in SFTOS 2.5.1. It enables the S-Series user to override the settings of the hardware dynamic and static buffers (also called dedicated buffers or fixed buffers) on a per-port and a per-queue, per-port basis. Configuration is allowed for all physical ports — 1G, 10G, and stack ports.

 **Caution:** Changing the buffer settings from their defaults can yield unpredictable results, because Dell Force10 has not tested the many combinations of possible values and port configurations. If you are using these features for the first time, contact Dell Force10 TAC (Technical Assistance Center) 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

Hardware memory in the S-Series is, by default, allocated primarily to dynamic buffers, which provides for maximum flexibility in supporting all traffic. You can use the buffer carving commands to reallocate more of that memory on certain ports to static buffers, enabling you to give higher priority to traffic on those ports. Buffer carving is especially useful to users who know their applications well and want to use S-Series switches in places where bursty traffic is common and well understood.

 **Note:** Buffer carving should be done before other configuration to ensure that no traffic is running on the stack. Buffer carving involves changing of hardware buffer settings, so a reboot (reload command) is required for changes to take effect.

buffer check

This command checks the hardware to verify that the configured buffer allocations meet the hardware requirements.

Syntax **buffer check**

Mode Global Config

Usage After you change the buffers, you should execute this command before rebooting the switch to verify that the buffer allocations meet the hardware requirements.

Command History Related Commands

Version 2.5.1	Introduced
<code>buffer dedicated (1G and stacking ports)</code>	Set buffer sizes per port and per queue for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.
<code>buffer dedicated interface (10G ports)</code>	Set buffer sizes per port and per queue for the optional 10Gb ports 49 and 50 on the S50 and the 10Gb ports on the S25P.
<code>buffer dynamic (1G and stack ports)</code>	Set dynamic buffer sizes per port for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V
<code>show buffer unit</code>	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

buffer dedicated (1G and stacking ports)

This command sets buffer sizes per port and per queue for the ASICs controlling ports 1– 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.

Syntax `[no] buffer dedicated {interface unit/slot/port | system-uplink unit} Queue-0_buffer Queue-1_buffer Queue-2_buffer Queue-3_buffer Queue-4_buffer Queue-5_buffer Queue-6_buffer`

To return buffers to their default values, use the **no buffer dedicated interface *unit/slot/port*** or **no buffer dedicated system-uplink *unit*** command syntax, depending on the target port.

Parameters

interface <i>unit/slot/port</i>	Enter the keyword interface followed by the port that you want to configure. The possible ports vary by platform: <ul style="list-style-type: none"> S50: The 1Gb ports (1 – 48) (Use <code>buffer dedicated interface (10G ports)</code> for ports 49 and 50.) S50V: 1 – 52
system-uplink <i>unit</i>	Enter the keyword system-uplink followed by the stack member number containing the stack port that you want to configure. Note: There is no system-uplink in the S25P.
<code>Queue-0_buffer, Queue-1_buffer... Queue-6_buffer</code>	For each of the seven queues, in sequence, enter a number indicating its desired buffer size, in 1KB increments (for example, 100 for 100KB). Each queue can be assigned from 0KB to any portion of the remaining total memory. Queue 7 is unavailable for buffer carving, inheriting any of the total buffer size not allocated. The total buffer size varies by platform: <ul style="list-style-type: none"> S50: 988KB S50V: 2013KB Memory measurement is the total combined dedicated and dynamic memory per 12-port group.

Defaults	Equal allocation per queue	
Mode	Global Config	
Command History	Version 2.5.1	Introduced
Usage Information	For example, to set the buffer to 50k in each buffer on port 1/0/1 in unit 1 in an S50 stack, the command would be <code>buffer dedicated interface 1/0/1 50 50 50 50 50 50 50</code> .	
Related Commands	<code>buffer check</code>	Verify that the configured buffer allocations meet the hardware requirements.
	<code>buffer dedicated interface (10G ports)</code>	Set buffer sizes per port and per queue for ASICs controlling the optional 10GB ports 49 and 50 on the S50 and the 10Gb ports on the S25P.
	<code>buffer dynamic (1G and stack ports)</code>	Set dynamic buffer sizes per port for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.
	<code>show buffer unit</code>	Display configured values for dedicated buffers, dynamic buffers, and packet limits for <i>each</i> port in an S50, S50V, or S25P, as well as the actual settings from the switch hardware.
	<code>show buffer allocation interface</code>	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

buffer dedicated interface (10G ports)

This command sets buffer sizes per port and per queue for ASICs controlling the optional 10Gb ports 49 and 50 on the S50 and the 10Gb ports on the S25P.

Syntax `[no] buffer dedicated interface unit/slot/port Queue-0_buffer Queue-1_buffer Queue-2_buffer Queue-3_buffer Queue-4_buffer Queue-5_buffer Queue-6_buffer`

Use the **no buffer dedicated interface** `unit/slot/port` command syntax to return buffers to their default values.

Parameters	interface <i>unit/slot/port</i>	Enter the keyword interface followed by the port that you want to configure, in <i>unit/slot/port</i> format. The only ports that this command configures are ports 49 and 50 on the S50. Use buffer dedicated (1G and stacking ports) for the other ports. The possible ports vary by platform: S50: The optional 10Gb ports — 49 and 50 (Use buffer dedicated (1G and stacking ports) for ports 1 – 48.) S25P: 1 through 25
	<i>Queue-0_buffer,</i> <i>Queue-1_buffer...</i> <i>...Queue-6_buffer</i>	For each of the seven queues, in sequence, enter a number indicating its desired buffer size, in 1KB increments (for example, 100 for 100KB). Each queue can be assigned from 0KB to any portion of the remaining total memory. Queue 7 is unavailable for buffer carving, inheriting any of the total buffer size not allocated. The total buffer size varies by platform: <ul style="list-style-type: none"> • S50: 342KB • S50V: 2013KB Memory measurement is the total combined dedicated and dynamic memory per 12-port group.
Defaults	Equal allocation per queue	
Mode	Global Config	
Command History	Version 2.5.1	Introduced
Usage Information	For example, to set the buffer to 20k in each buffer on port 1/0/1 in unit 1 in an S50 stack, the command would be buffer dedicated interface 1/0/1 20 20 20 20 20 20 20 . There is no dynamic buffering on these ports.	
Related Commands	buffer check	Verify that the configured buffer allocations meet the hardware requirements.
	buffer dedicated (1G and stacking ports)	Set buffer sizes per port and per queue for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.
	buffer dynamic (1G and stack ports)	Set dynamic buffer sizes per port for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.
	show buffer unit	Display configured values for dedicated buffers, dynamic buffers, and packet limits for <i>each</i> port in an S50, S50V, or S25P, as well as the actual settings from the switch hardware.
	show buffer allocation interface	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

buffer dynamic (1G and stack ports)

This command sets dynamic buffer sizes per port for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.

Syntax **[no] buffer dynamic {interface *unit/slot/port* | system-uplink *unit*} *buffer***

To return buffers to their default values, use the **no buffer dynamic interface** *unit/slot/port* or **no buffer dynamic system-uplink** *unit* command syntax, depending on the target port.

Parameters

interface <i>unit/slot/port</i>	Enter the keyword interface followed by the port that you want to configure. The possible ports vary by platform: <ul style="list-style-type: none"> • S50: The 1Gb ports (ports 1 – 48) (Dynamic buffering is not supported for the optional 10Gb ports 49 and 50. The dynamic buffer is sufficiently oversubscribed by default.) • S50V: 1 – 52
system-uplink <i>unit</i>	Enter the keyword system-uplink followed by the stack member number containing the stack port that you want to configure. Note: There is no system-uplink in the S25P.
<i>buffer</i>	Enter the desired buffer size, in 1KB increments (for example, 100 for 100KB). The available buffer size varies by platform: <ul style="list-style-type: none"> • S50: 1024KB • S50V: 2013KB

Defaults

S50: 286KB for 1Gb ports, 431KB for stack ports
S50V: 257KB for 1Gb ports, 385KB for stack ports and 10G ports
S25P: There is no switch fabric in this switch, so, therefore, there is no system-downlink.

Mode

Global Config

Command History

Version 2.5.1	Introduced
---------------	------------

Usage Information

Dynamic buffer limits can be oversubscribed; oversubscription ratio: eight times for 1Gb ports and 13 times for stack ports.

Related Commands

buffer check	Verify that the configured buffer allocations meet the hardware requirements.
buffer dedicated (1G and stacking ports)	Set buffer sizes per port and per queue for the ASICs controlling ports 1– 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V
buffer dedicated interface (10G ports)	Set buffer sizes per port and per queue for ASICs controlling the optional 10Gb ports 49 and 50 on the S50 and the 10Gb ports on the S25P.
show buffer unit	Display configured values for dedicated buffers, dynamic buffers, and packet limits for <i>each</i> port in an S50, S50V, or S25P, as well as the actual settings from the switch hardware.
show buffer allocation interface	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

buffer dynamic interface (S25P)

This command sets the dynamic buffer size for S25P ports.

Syntax	[no] buffer dynamic interface <i>unit/slot/port</i> <i>buffer</i>	
	To return buffers to their default values, use the no buffer dynamic interface <i>unit/slot/port</i> command syntax.	
Parameters	<i>unit/slot/port</i> <i>buffer</i>	Enter the S25P port to configure (ports 1 – 28) in <i>unit/slot/port</i> format, followed by a number indicating the desired dynamic buffer size, in 1KB increments (for example, 100 for 100KB). Range: 0–2013KB
Defaults	257KB for SFP ports, 385k for stack and 10G ports; oversubscription ratio: eight times for SFP ports, 12 times for stack and 10G ports	
Mode	Global Config	
Command History	Version 2.5.1	Introduced
Related Commands	buffer check	Verify that the configured buffer allocations meet the hardware requirements.
	buffer dedicated interface (10G ports)	Set buffer sizes per port and per queue for ASICs controlling the optional 10GB ports 49 and 50 on the S50 and the 10Gb ports on the S25P.
	show buffer unit	Display configured values for dedicated buffers, dynamic buffers, and packet limits for <i>each</i> port in an S50, S50V, or S25P, as well as the actual settings from the switch hardware.
	show buffer allocation interface	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

buffer dynamic interface system-downlink

This command sets the downlink buffer size for the S50 switch fabric.

Syntax	[no] buffer dynamic interface system-downlink <i>Queue-1_buffer</i> <i>Queue-2_buffer</i> <i>Queue-3_buffer</i> <i>Queue-4_buffer</i> <i>Queue-5_buffer</i> <i>Queue-6_buffer</i>	
	To return buffers to their default values, use the no buffer dynamic interface system-downlink command.	
Parameters	<i>Queue-1_buffer</i> <i>Queue-2_buffer...</i> <i>...Queue-6_buffer</i>	For each of the six queues, in sequence, enter a number indicating its desired buffer size, in 1KB increments (for example, 10 for 10KB). Range: 0 – 128KB 128KB is available per interface.
Defaults	Equal allocation per queue. No static buffering on the switch fabric	
Mode	Global Config	

Command History	Version 2.5.1	Introduced

Related Commands	buffer check	Verify that the configured buffer allocations meet the hardware requirements.
	buffer dynamic (1G and stack ports)	Set dynamic buffer sizes per port for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.
	buffer dedicated interface (10G ports)	Set buffer sizes per port and per queue for ASICs controlling the optional 10GB ports 49 and 50 on the S50 and the 10Gb ports on the S25P.
	show buffer unit	Display configured values for dedicated buffers, dynamic buffers, and packet limits for <i>each</i> port in an S50, S50V, or S25P, as well as the actual settings from the switch hardware.
	show buffer allocation interface	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

buffer packets interface

This command sets packet limits per-port/per-queue on ports 1 – 48 and the stack port on the S50, ports 1 – 52 and the stack port on the S50V, and ports 1 – 28 on the S25P.

Syntax `[no] buffer packets interface { unit/slot/port | system-uplink | system-downlink } Queue-0_buffer Queue-1_buffer Queue-2_buffer Queue-3_buffer Queue-4_buffer Queue-5_buffer Queue-6_buffer`

To return buffers to their default values, use the **no buffer packets interface *unit/slot/port***, **no buffer packets system-uplink**, or **no buffer packets system-downlink** command syntax, depending on the target port.

Parameters	<i>unit/slot/port</i>	Enter the port that you want to configure, in <i>unit/slot/port</i> format. The possible ports vary by platform: <ul style="list-style-type: none"> S50: The 1Gb ports — 1 – 48 (Use buffer dedicated interface (10G ports) for ports 49 and 50.) S50V: 1 – 52 S25P: 1 – 28
	system-uplink	For the S50 and S50V only, enter the keyword system-uplink to configure the stack ports of all stack members.
	system-downlink	For the S50 only, enter the keyword system-downlink to configure the output from the switch fabric buffer.
	<i>Queue-0_buffer</i> <i>Queue-1_buffer...</i> <i>...Queue-6_buffer</i>	For each of the seven queues, in sequence, enter a number indicating its desired buffer size, in 1KB increments (for example, 100 for 100KB). All S50, S50V, and S25P queues have a 2047 packet limit. The total number of packets cannot exceed 2047 per port. It is possible to reduce the packet limit of Queue 7 to 0 by allocating the total of 2047 packets to the other queues.

Defaults Equal allocation per queue

Mode Global Config

Command History	Version 2.5.1	Introduced

Usage Information

The total number of packets cannot exceed 2047 per port.

Related Commands

buffer check	Verify that the configured buffer allocations meet the hardware requirements.
buffer dedicated (1G and stacking ports)	Sets buffer sizes per port and per queue for the ASICs controlling ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V
buffer dedicated interface (10G ports)	Set buffer sizes per port and per queue for ASICs controlling the optional 10Gb ports 49 and 50 on the S50 and the 10Gb ports on the S25P.
show buffer unit	Display configured values for dedicated buffers, dynamic buffers, and packet limits for <i>each</i> port in an S50, S50V, or S25P, as well as the actual settings from the switch hardware.
show buffer allocation interface	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

show buffer unit

This command displays configured values for dedicated buffers, dynamic buffers, and packet limits for each ASIC in the selected S50, S50V, or S25P, as well as the actual settings from the switch hardware. Because configured values do not take effect until the stack is rebooted, the hardware values can be different.

Syntax `show buffer unit`

Mode Privileged Exec

Example 1 **Figure 20-121. show buffer unit Command Output from an S50**

```
(Force10 S50) #show buffer unit 1
Broadcom ASIC 5675 (BCM unit 0)

Total Physical Buffer.....1152 kb
Interface   Dynamic Buffer   Dynamic Buffer   Pkt Limit   Pkt Limit
              (Conf)           (Actual)        (Conf)      (Actual)
Downlink    120k             128k            2030        2047

Broadcom ASIC 5695 (BCM unit 1)
Total Physical Buffer.....1024 kb
Total Dedicated Buffer......600 kb
Total Dynamic Buffer......424 kb

Interface   Fixed buffer   Fixed Buffer   Over-sub   Over-sub   Pkt limit   Pkt limit
              (Conf)         (Actual)     (Conf)     (Actual)   (Conf)      (Actual)
1/0/1       100k           100k         10          8          2047        2047
1/0/2       120k           95k          12          8          2030        2030

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

Example 2 Figure 20-122. show buffer unit Command Output from an S50V or S25P

```
(Forcel0 S50) #show buffer unit 2
Broadcom ASIC 56504 (BCM unit 0)

Total Physical Buffer.....2048 kb
Total Dedicated Buffer.....1340 kb
Total Dynamic Buffer.....708 kb

Interface    Fixed buffer    Fixed Buffer    Over-sub    Over-sub    Pkt limit    Pkt limit
              (Conf)          (Actual)       (Conf)      (Actual)   (Conf)       (Actual)
2/0/1        100k            100k           10          8          2047         2047
2/0/2        120k            95k            12          8          2030         2030
2/0/3        100k            100k           10          8          2047         2047
2/0/4        120k            95k            12          8          2030         2030
!-----output truncated-----!
```

Table 20-24. Fields of show buffer unit Command Output

Field	Description
(top row of section)	The ASIC described in this section of the output
Total Physical Buffer	Memory available per queue for the combined static and dynamic buffers
Total Dedicated Buffer	Total static memory available on that ASIC
Total Dynamic Buffer	Total dynamic memory available on that ASIC
Interface	List of ports managed by the ASIC listed at the top of the section
Dynamic Buffer (Conf)	The dynamic buffer allocation, as configured
Dynamic Buffer (Actual)	The dynamic buffer allocation, as it is before reboot sets the value to the configured value
Fixed Buffer (Conf)	The static buffer allocation, as configured
Fixed Buffer (Actual)	The static buffer allocation, as it is before reboot sets the value to the configured value
Over-sub (Conf)	Oversubscription ratio to be made available to dynamic buffering, as configured
Over-sub (Actual)	Oversubscription ratio available to dynamic buffering, as it is before reboot revises the memory allocation to static buffers
Pkt Limit (Conf)	The packet limit allocation, as configured
Pkt Limit (Actual)	The packet limit allocation, as it is before reboot sets the value to the configured value

Command History Related Commands

Version	Introduced
Version 2.5.1	Introduced
buffer check	Verify that the configured buffer allocations meet the hardware requirements.
buffer dedicated (1G and stacking ports)	Set buffer sizes per port and per queue for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.
buffer dynamic (1G and stack ports)	Set dynamic buffer sizes per port for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V
show buffer allocation interface	Display configured and actual static buffer allocation and packet allocation values per queue for the <i>selected</i> port in an S50, S50V, or S25P.

show buffer allocation interface

This command displays configured and actual static buffer allocation and packet allocation values per queue for the selected port in an S50, S50V, or S25P. Because configured values do not take effect until the stack is rebooted, the actual values can be different.

Syntax `show buffer allocation interface {unit/slot/port | system-uplink | system-downlink}`

Parameters	<i>unit/slot/port</i>	Enter the port, in unit/slot/port format, for which you want to display the buffer allocation. The possible ports vary by platform: <ul style="list-style-type: none"> • S50: 1 – 50 • S50V: 1 – 52 • S25P: 1 – 28
	system-uplink	For the S50 and S50V only, enter the keyword system-uplink to display the stack ports of all stack members.
	system-downlink	For the S50 only, enter the keyword system-downlink to display the buffer allocation for the switch fabric output.

Mode Privileged Exec

Example **Figure 20-123. show buffer unit Command Output**

```
(Force10 S50) #show buffer allocation interface 1/0/10
Interface 1/0/10
Dedicated Buffer.....100k
Dynamic Buffer.....300k
Packet Limit.....2047

Queue   Fixed Buffer   Fixed Buffer   Pkt Limit   Pkt Limit
        (Conf)       (Actual)     (Conf)      (Actual)
0       10k          15k          300         300
1       20k          20k          400         350
2       10k          15k          300         300
3       20k          20k          400         350
4       10k          15k          300         300
5       20k          20k          400         350
6       10k          10k          300         300
```

Table 20-25. Fields of show buffer unit Command Output

Field	Description
Interface	The selected port
Dedicated Buffer	The static memory to be allocated to the selected port
Dynamic Buffer	The dynamic memory to be allocated to the selected port
Packet Limit	The packet limit memory allocated to the selected port
Queue	The seven queue IDs for the selected port
Fixed Buffer (Conf)	The static buffer allocation, per queue, as configured
Fixed Buffer (Actual)	The static buffer allocation, as it is before a reboot sets the value to the configured value

Table 20-25. Fields of show buffer unit Command Output (continued)

Field	Description
Pkt Limit (Conf)	The packet limit allocation, as configured
Pkt Limit (Actual)	The packet limit allocation, as it is before reboot sets the value to the configured value

**Command
History
Related
Commands**

Version 2.5.1	Introduced
buffer check	Verify that the configured buffer allocations meet the hardware requirements.
buffer dedicated (1G and stacking ports)	Set buffer sizes per port and per queue for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V.
buffer dynamic (1G and stack ports)	Set dynamic buffer sizes per port for ports 1 – 48 and the stack port on the S50, and ports 1 – 52 and the stack port on the S50V
show buffer unit	Display configured values for dedicated buffers, dynamic buffers, and packet limits for <i>each</i> port in an S50, S50V, or S25P, as well as the actual settings from the switch hardware.

ACL Commands

SFTOS supports the following types of Access Control Lists (ACLs):

- [IP Access Control List \(IP ACL\) Commands](#)
- [MAC Access Control List \(ACL\) Commands on page 384](#)
- [Broadcast Storm Control Commands on page 389](#)

An Access Control List (ACL) ensures that only authorized users and types of traffic have access to specific resources, while blocking unwarranted attempts to reach network resources.

The following conditions pertain to ACLs in SFTOS:

- ACL configuration for IP packet fragments is not supported.
- The maximum number of rules per ACL translates into the number of hardware classifier entries used when an ACL is attached to an interface. Increasing these values in the SFTOS software increases the RAM and NVSTORE usage.
- ACLs are configured separately for Layer 2 and Layer 3. Both types of ACL can be applied to the same interface.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored.

For details on using access control commands, see the Access Control chapter in the *SFTOS Configuration Guide*. ACLs factor into quality of service. For more on quality of service (QoS), see [Quality of Service \(QoS\) Commands on page 327](#).

IP Access Control List (IP ACL) Commands

- [access-list on page 379](#)
- [ip access-group \(Interface\) on page 381](#)
- [ip access-group all on page 382](#)
- [show ip access-lists on page 382](#)

access-list

This command creates a rule for an IP access control list (ACL). The ACL is identified by the ACL number, represented in the syntax statement as *1-99* (IP Standard ACL) or *100-199* (IP Extended ACL).

Syntax IP Standard ACL:
`access-list 1-99 {deny | permit} {every | srcip srcmask} [log] [assign-queue queue-id]
 [{mirror | redirect} unit/slot/port]`



Note: The mirror option is supported in the S50V and S25P models only.

IP Extended ACL:

`access-list 100-199 {deny | permit} {every | icmp | igmp | ip | tcp | udp | protocol_number}
 {any | srcip srcmask} {any | eq {portkey | 0-65535} {any | dstip dstmask} [eq {portkey |
0-65535}] [precedence precedence | tos tos tosmask | dscp dscp] [log] [assign-queue
queue-id] [redirect unit/slot/port]`

Use the `no access-list ACLnumber` version of this command to delete an ACL (identified by a number in the range *1-199*).

Parameters

<i>1-99</i> and <i>100-199</i>	Assign an integer in the range 1 to 99 to an access list for an IP standard ACL. Use an integer in the range 100 to 199 for an IP extended ACL.
deny permit	Specify whether the IP ACL rule permits or denies an action.
every <i>srcip srcmask</i>	For an IP Standard ACL , select the source to filter. Enter either the keyword every , to match every packet, or use the <i>srcip</i> and <i>srcmask</i> parameters to specify a source IP address and source mask for a match condition of the ACL rule (<i>srcmask</i> is an inverse mask, also called a wildcard mask, as described at the beginning of this chapter).
every icmp igmp ip tcp udp <i>protocol_number</i>	For an IP Extended ACL , you have three choices for the source to filter: <ul style="list-style-type: none"> • As above, the keyword every matches every packet. • The other keywords specify the protocol to filter— ICMP, IGMP, IP, TCP, or UDP. • Otherwise, enter the protocol number to match, from 1 to 255.
any <i>srcip</i> and <i>srcmask</i>	Enter either any , to match any source IP address, or use the <i>srcip</i> and <i>srcmask</i> parameters to specify a source IP address and source mask for a match condition of the ACL rule (<i>srcmask</i> is an inverse mask, also called a wildcard mask, as described at the beginning of this chapter).
{any eq { <i>portkey</i> <i>0-65535</i> }}	For an IP Extended ACL , specify the source Layer 4 port match condition for the IP ACL rule. You can enter: <ul style="list-style-type: none"> • the keyword any, to accept any Layer 4 port ID • the keyword eq and then enter either: <ul style="list-style-type: none"> • the <i>portkey</i>, which can be one of the following keywords: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, ftp, or www. Each of these values translates into its equivalent port number, which is used as both the start and end of a port range. • the Layer 4 port number, which ranges from 0-65535
{any <i>dstip dstmask</i> }	For an IP Extended ACL , specify a destination IP address and destination mask for the match condition of the ACL rule (<i>dstmask</i> is an inverse mask, as above).
eq { <i>portkey</i> <i>0-65535</i> }	This option is available for both any and <i>dstip dstmask</i> , and the variables are as defined above.
[precedence <i>precedence</i> tos <i>tos</i> <i>tosmask</i> dscp <i>dscp</i>]	(OPTIONAL) For an IP Extended ACL , specifies the type of service (TOS) for an IP ACL rule depending on a match of precedence or DSCP values using the parameters precedence , tos/tosmask , dscp .

	log	(OPTIONAL) Specifies that hits on this rule are to be logged (For details, see the System Logs chapter in the <i>SFTOS Configuration Guide</i>). The log attribute is only for deny rules.
	assign-queue <i>queue-id</i>	(OPTIONAL) The assign-queue ID is the queue identifier to which packets matching this rule are assigned.
	{ mirror redirect } <i>unit/slot/port</i>	(OPTIONAL) Specify whether the packets matching this rule are mirrored or redirected through the specified port. A redirected packet carries the same MAC address as it would have if it had not been redirected (the MAC address of the next hop defined in the routing table). Note: These options are only for a permit rule. The mirror option is supported in the S50V and S25P models only; it is not available on S50 switches, nor for extended access lists (100–199). Source, destination, and monitor/redirect ports must be in the same VLAN.
Default	none	
Mode	Global Config	
Command History	Version 2.5.1	Modified to include log and mirror options.
Related Commands	{deny permit}	Creates a new rule for the current MAC access list.
	interface loopback	Configures a loopback interface.
	ip access-group (Interface)	Attaches a specified ACL to the selected interface.
	show ip access-lists	Displays an IP Access Control List (ACL) and all of the rules that are defined for the ACL.
	show interface loopback	Displays loopback interface configuration.

ip access-group (Interface)

This command attaches a specified IP access-control list (ACL) to an interface.

Syntax	ip access-group <i>ACLnumber</i> [<i>1-4294967295</i>] in	
Parameters	<i>ACLnumber</i>	Enter the ACL ID, which is an integer with a range of 1–199 assigned using the OOEnn6ganc and OOEnn6ganc commands.
	<i>1-4294967295</i>	(OPTIONAL) Enter an integer that indicates the order of this ACL relative to other ACLs assigned to this port channel. A lower sequence number indicates higher precedence order. If the selected number is already in use for this port channel, this ACL replaces the currently attached ACL using that sequence number. If you do not specify a number with this command, a number that is one greater than the highest sequence number currently in use for this port channel is used for this ACL.
	in	The in parameter is required. SFTOS supports only the ingress direction.
Default	none	

Mode	Interface Config (including Interface Loopback Config) and Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode.
	access-list	Creates an IP access control list.
	ip address (routed)	configures an IP address on a routed interface.
	ip access-group (port channel)	Attaches an ACL to the selected port channel.
	show ip access-lists	Displays an IP Access Control List (ACL) and all of the rules that are defined for the ACL.

ip access-group all

This command attaches a specified IP access control list to all interfaces.

Syntax ip access-group all *ACLnumber* [1 – 4294967295] in

Default none

Mode Global Config

show ip access-lists

This command displays an IP Access Control List (ACL) and all of the rules that are defined for the ACL. The *ACLnumber* is the number used to identify the ACL.

Syntax show ip access-lists [*ACLnumber*]

Parameters

<i>ACLnumber</i>	Enter the ACL ID in the range of 1 to 199.
------------------	--

Mode Privileged Exec and User Exec

Example **Figure 21-124. Command Example: show ip access-lists**

```

Force10-S50 #show ip access-lists
Current number of ACLs: 3 Maximum number of ACLs: 100
ACL ID  Rules  Direction  Interface(s)
-----  -
1       3       inbound   1/0/48
2       1
3       1

```

Example Figure 21-125. Command Example specifying ACL number: show ip access-lists

```

Forcel0-S50 #show ip access-lists 1
ACL ID: 1
Interface:1/0/48

Rule Number: 1
Action..... permit
Match All..... FALSE
Source IP Address..... 1.1.1.1
Source IP Mask..... 255.255.255.0

Rule Number: 2
Action..... permit
Match All..... FALSE
Source IP Address..... 2.2.2.2
Source IP Mask..... 255.255.255.0

Rule Number: 3
Action..... permit
Match All..... FALSE
Source IP Address..... 2.2.2.3
Source IP Mask..... 255.255.255.0
    
```

Field Descriptions

Rule Number—This displays the number identifier for each rule that is defined for the ACL.

Action—This displays the action associated with each rule. The possible values are Permit or Deny.

Match all—TRUE or FALSE

Protocol—This displays the protocol to filter for this rule.

Source IP Address—This displays the source IP address for this rule.

Source IP Mask—This field displays the source IP Mask for this rule.

Source Ports—This field displays the source port range for this rule, if any.

Destination IP Address—This displays the destination IP address for this rule, if any.

Destination IP Mask—This field displays the destination IP Mask for this rule, if any.

Destination Ports—This field displays the destination port range for this rule, if any.

Service Type Field Match—This field indicates whether an IP DSCP, IP Precedence, or IP TOS match condition is specified for this rule, if any.

Service Type Field Value—This field indicates the value specified for the Service Type Field Match (IP DSCP, IP Precedence, or IP TOS), if any.

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode.
access-list	Creates an IP access control list.
ip access-group (port channel)	Attaches an ACL to the selected port channel.
ip access-group (Interface)	Attaches an ACL to the selected interface.

MAC Access Control List (ACL) Commands

The commands in this section are:

- [{deny|permit} on page 384](#)
- [mac access-list extended on page 386](#)
- [mac access-list extended rename on page 386](#)
- [mac access-group on page 387](#)
- [show mac access-lists on page 388](#)

{deny|permit}

This command creates a new rule for the selected MAC access list. Each rule is appended to the list of configured rules for the list. Note that an implicit “deny all” MAC rule always terminates the access list.

Syntax {deny|permit} {srcmac | any} {dstmac} | any] [assign-queue *queue-id_0-6*] [cos *0-7*] [ethertypekey] [0x0600-0xFFFF] [redirect *unit/slot/port*] [vlan {eq *0-4095*}

Parameters

deny permit	A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source (<i>srcmac</i> any) and destination (<i>dstmac</i>) any) MAC value and mask pairs must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The BPDU keyword may be specified for the destination MAC value/mask pair indicating a well-known BPDU MAC value of 01-80-c2-xx-xx-xx (hex), where 'xx' indicates a don't care. The remaining command parameters are all optional.
assign-queue	(Optional) The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <i>queue-id</i> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform.
ethertypekey	(Optional) The Ethertype (<i>ethertypekey</i>) may be specified as either a keyword or a four-digit hexadecimal value from 0x0600 to 0xFFFF. The currently supported <i>ethertypekey</i> keyword values are: appletalk , arp , ibmsna , ipv4 , ipv6 , ipx , mplsmcast , mplsucast , netbios , novell , pppoe , rarp . Each of these translates into its equivalent Ethertype value(s).
redirect	(Optional) The redirect parameter redirects traffic matching this rule to the specified egress port. The redirected packet carries the same MAC address as it would have if it had not been redirected (the MAC address of the next hop defined in the routing table). Basically, it looks like a mirrored packet on the redirect port. The assign-queue and redirect parameters are only valid for a permit rule.



Note: The special command form {deny|permit} **any any** is used to match all Ethernet Layer 2 packets, and is the equivalent of the IP access list “match every” rule.



Note: The 'no' form of this command is not supported, as the rules within an ACL cannot be deleted individually. Rather, the entire ACL must be deleted and re-specified.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword **any** to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The EtherType (*etherstypekey*) may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *etherstypekey* values are: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, and **rarp**. Each of these translates into its equivalent EtherType value(s), as shown in [Table 21-26](#).

Table 21-26. EtherType Keyword and 4-digit Hexadecimal Value

EtherType Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

Mode Mac Access List Config

**Related
Commands**

interface range	Defines an interface range and accesses the Interface Range mode
mac access-group (port channel)	In the Interface Port Channel Config mode, attaches a MAC ACL to the selected port channel
mac access-group	Attaches a specific MAC Access Control List (ACL) identified by <i>name</i> to an interface in the ingress direction
mac access-list extended	Creates a MAC ACL.
show mac access-lists	Displays the rules defined for the MAC access list specified by <i>name</i> .

mac access-list extended

This command creates a MAC Access Control List (ACL) identified by *name*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame.



Note: The CLI mode is changed to Mac Access List Config (prompt is “*hostname* (Mac-Access-List Config)#”) when this command is successfully executed. If a MAC ACL by this name already exists, this command simply invokes the mode.

The `no` version of this command deletes a MAC ACL identified by *name* from the system.

Syntax	mac access-list extended <i>name</i>	
Parameters	<i>name</i>	Case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. The string may include alphabetic, numeric, dash, dot or underscore characters only. The string must start with a letter.
Mode	Global Config	
Related Commands	{deny permit}	Creates a new rule for the MAC access list selected by the <code>mac access-list extended</code> command.
	interface range	Defines an interface range and accesses the Interface Range mode
	mac access-group (port channel)	In the Interface Port Channel Config mode, attaches a MAC ACL to the selected port channel
	mac access-group	Attaches a specific MAC Access Control List (ACL) identified by <i>name</i> to an interface in the ingress direction
	mac access-list extended rename	Changes the name of an existing MAC ACL.
	show mac access-lists	Displays the rules defined for the MAC access list specified by <i>name</i> .

mac access-list extended rename

This command changes the name of an existing MAC ACL. The *name* parameter is the name of an existing MAC ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *newname* already exists.

Syntax	mac access-list extended rename <i>name newname</i>	
Parameters	<i>name</i>	The ACL name assigned during the creation of the ACL by using the <code>mac access-list extended</code> command
	<i>newname</i>	Case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. The string may include alphabetic, numeric, dash, dot or underscore characters only. The string must start with a letter.
Mode	Global Config	

**Related
Commands**

<code>{deny permit}</code>	Creates a new rule for the MAC access list selected by the mac access-list extended command.
<code>interface range</code>	Defines an interface range and accesses the Interface Range mode
<code>mac access-group (port channel)</code>	In the Interface Port Channel Config mode, attaches a MAC ACL to the selected port channel
<code>mac access-group</code>	Attaches a specific MAC Access Control List (ACL) identified by <i>name</i> to an interface in the ingress direction
<code>mac access-list extended</code>	Creates a MAC Access Control List (ACL)
<code>show mac access-lists</code>	Displays the rules defined for the MAC access list specified by <i>name</i>

mac access-group

This command attaches a specific MAC Access Control List (ACL) identified by *name* to an interface in the ingress direction. This command, when used in Interface Config mode, only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

Syntax `mac access-group name in [1-4294967295]`

The `no mac access-group name` command removes the MAC ACL identified by *name* from the interface in the ingress direction.

Parameters

<i>name</i>	The <i>name</i> must be the name of an existing MAC ACL.
<code>1-4294967295</code>	(OPTIONAL) Enter a sequence number that indicates the order of this ACL relative to other ACLs already assigned to this port channel. A lower sequence number indicates higher precedence order. If the selected number is already in use for this port channel, this ACL replaces the currently attached ACL using that sequence number. If you do not specify a number with this command, a number that is one greater than the highest sequence number currently in use for this port channel is used for this ACL.
<code>in</code>	This keyword is required. SFTOS supports only the ingress direction.

Modes

Global Config, Interface Config; Interface Range, which is indicated by the `(conf-if-range-interface)#` prompt, such as `(conf-if-range-vlan 10-20)#`.

**Command
History**

Version 2.5.1	Modified: Added the sequence option, and removed the <code>in</code> keyword. All policies are ingress only.
Version 2.3	Added Interface VLAN and Interface Range modes.

**Related
Commands**

<code>interface range</code>	Defines an interface range and accesses the Interface Range mode
<code>mac access-group (port channel)</code>	In the Interface Port Channel Config mode, attaches a MAC ACL to the selected port channel
<code>mac access-list extended</code>	Creates a MAC Access Control List (ACL) identified by name, consisting of classification fields defined for the Layer 2 header of an Ethernet frame.
<code>show mac access-lists</code>	Displays the rules defined for the MAC access list specified by <i>name</i> .

show mac access-lists

This command displays the rules defined for all MAC ACLs or the MAC ACL specified by *name*.

Syntax show mac access-lists [*name*]

Mode Privileged Exec

When the command is used with the *name* option, the report displays details for the identified MAC access list, in the following fields:

Field Descriptions

Rule Number—The ordered rule number identifier defined within the ACL.

Action—Displays the action associated with each rule. The possible values are Permit or Deny.

Match all—TRUE OR FALSE

Source MAC Address—Displays the source MAC address for this rule.

Source MAC Mask—Displays the source MAC mask for this rule.

Destination MAC Address—Displays the destination MAC address for this rule.

Destination MAC Mask—Displays the destination MAC mask for this rule.

Ethertype—Displays the Ethertype keyword or custom value for this rule.

VLAN ID—Displays the VLAN identifier value or range for this rule.

COS—Displays the COS (802.1p) value for this rule.

Secondary VLAN ID—Displays the Secondary VLAN identifier value or range for this rule.

Secondary COS—Displays the Secondary COS (802.1p) value for this rule.

Assign Queue—Displays the queue identifier to which packets matching this rule are assigned.

Redirect Interface—Displays the *unit/slot/port* to which packets matching this rule are forwarded.

When the command is used without the *name* option, the report displays a summary of all defined MAC access lists in the system, in the following fields:

Field Descriptions

Name—The name of the MAC access list

Number of Rules—The number of user-configured rules defined for this ACL

This does not include the implicit 'deny all' rule defined at the end of every MAC ACL

Interfaces—The list of interfaces (*unit/slot/port*) to which the MAC ACL is attached in a given direction

Direction—Denotes the direction in which the MAC ACL is attached to the set of interfaces listed. The only current possible value is Inbound.

Related Commands

[mac access-list extended](#)

Creates a MAC Access Control List (ACL) identified by name, consisting of classification fields defined for the Layer 2 header of an Ethernet frame.

Broadcast Storm Control Commands

This section contains the following commands:

- [show storm-control](#)
- [storm-control broadcast on page 390](#)
- [storm-control flowcontrol on page 390](#)

show storm-control

This command displays switch configuration information.

Syntax show storm-control [*unit/slot/port* | all]

Mode Privileged Exec

Defaults Broadcast Storm Recovery Mode—May be enabled or disabled. The factory default is disabled.
802.3x Flow Control Mode—May be enabled or disabled. The factory default is disabled.

Example **Figure 21-126. Command Example: show storm-control**

```
Force10-S50 #show storm-control
802.3x Flow Control Mode..... Disable
Force10-S50 #show storm-control 1/0/1
  Intf      Bcast  Bcast  Mcast  Mcast  Ucast  Ucast
           Mode   Level  Mode   Level  Mode   Level
-----
1/0/1  Disable  5      Disable  5      Disable  5
Force10-S50 #show storm-control all ?
<cr>                               Press enter to execute the command.
Force10-S50 #show storm-control all
  Intf      Bcast  Bcast  Mcast  Mcast  Ucast  Ucast
           Mode   Level  Mode   Level  Mode   Level
-----
1/0/1  Disable  5      Disable  5      Disable  5
1/0/2  Disable  5      Disable  5      Disable  5
1/0/3  Disable  5      Disable  5      Disable  5
1/0/4  Disable  5      Disable  5      Disable  5
1/0/5  Disable  5      Disable  5      Disable  5
1/0/6  Disable  5      Disable  5      Disable  5
1/0/7  Disable  5      Disable  5      Disable  5
1/0/8  Disable  5      Disable  5      Disable  5
1/0/9  Disable  5      Disable  5      Disable  5
!-----output truncated-----!
```

Related Commands

storm-control broadcast	Configure storm control.
show interface ethernet	The report generated by the show interface ethernet command contains broadcast storm statistics.

storm-control broadcast

This command enables broadcast storm recovery mode. If the mode is enabled, broadcast storm recovery with high and low thresholds is implemented.

Syntax [no] storm-control broadcast

The **no** version of this command disables broadcast storm recovery mode.

The threshold implementation follows a percentage pattern. If the broadcast traffic on any Ethernet port exceeds the high threshold percentage (as represented in the [Table 21-27](#)) of the link speed, the switch discards the broadcast's traffic until the traffic returns to the low threshold percentage or less. The full implementation is depicted in the table below.

Table 21-27. Broadcast Storm Recovery Thresholds

Link Speed	High	Low
10M	20	10
100M	5	2
1000M	5	2

Default disabled

Mode Global Config

Related Commands

show storm-control	Shows the storm control configuration.
show interface ethernet	The report generated by the show interface ethernet command contains broadcast storm statistics.

storm-control flowcontrol

This command enables 802.3x flow control for the switch.

Syntax [no] storm-control flowcontrol

The **no** version of this command disables 802.3x flow control for the switch.



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

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

Default disabled

Mode Global Config

Routing Commands

This chapter provides a detailed explanation of routing commands, in the following sections:

- [Address Resolution Protocol \(ARP\) Commands on page 391](#)
- [IP Routing on page 397](#)
- [Bootp/DHCP Relay Commands on page 407](#)
- [Router Discovery Protocol Commands on page 410 \(IRDP/ICMP\)](#)
- [Virtual LAN Routing Commands on page 413](#)
- [Virtual Router Redundancy Protocol \(VRRP\) Commands on page 414](#)

Address Resolution Protocol (ARP) Commands

This section provides a detailed explanation of the ARP commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

The commands in this section are, in order:

- [arp on page 392](#)
- [arp cachesize on page 392](#)
- [arp dynamicrenew on page 392](#)
- [arp purge on page 392](#)
- [arp resptime on page 393](#)
- [arp retries on page 393](#)
- [arp timeout on page 393](#)
- [clear arp-cache on page 394](#)
- [ip proxy-arp on page 394](#)
- [show arp on page 394](#)
- [show arp brief on page 395](#)

arp

This command creates an ARP entry.

Syntax [oe] sd *ipaddress macaddr*

The value for *ipaddress* is the IP address of a device on a subnet attached to an existing routing interface. *macaddr* is a unicast MAC address for that device. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

The **no** version of this command deletes an ARP entry.

Mode Global Config

arp cachesize

This command configures the ARP cache size. The value for *cachesize* is a platform specific integer value.

Syntax [no] arp cachesize *Platform_specific_integer_value*

Mode Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew ARP entries of type dynamic when they age out.

The **no** version of this command disables ARP component from automatically renewing ARP entries of type dynamic when they age out.

Syntax [no] arp dynamicrenew

Mode Global Config

Command History

Version 2.3

Modified: Moved from Privileged Exec mode to Global Config mode.

arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Syntax arp purge *ipaddr*

Mode Privileged Exec

arp resptime

This command configures the ARP request response timeout.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for *seconds* is between 1-10 seconds.

The no version of this command configures the default ARP request response timeout.

Syntax arp resptime *1-10*

no arp resptime

Default 1

Mode Global Config

arp retries

This command configures the ARP count of maximum request for retries.

The value for *retries* is an integer, which represents the maximum number of request for retries. The range for *retries* is an integer between 0-10 retries.

The no version of this command configures the default ARP count of maximum request for retries.

Syntax arp retries *0-10*

no arp retries

Default 4

Mode Global Config

arp timeout

This command configures the ARP entry ageout time.

The value for *seconds* is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for *seconds* is between 15-21600 seconds.

The no version of this command configures the default ARP entry ageout time.

Syntax arp timeout *15-21600*

Default 1200

Mode Global Config

clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the *gateway* parameter is specified, the dynamic entries of type gateway are purged as well.

Syntax clear arp-cache [gateway]

Mode Privileged Exec

ip proxy-arp

This command enables proxy ARP on a router interface.

Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Syntax [no] ip proxy-arp

The no version of this command disables proxy ARP on a router interface.

Default enabled

Mode Interface Config or Interface VLAN

Command History

Version 2.3 Modified: Added Interface VLAN as a mode.

show arp

This command is only available for the Layer 3 software package. It displays the Address Resolution Protocol (ARP) cache, all the ARP entries learned through the routing engine.

The displayed results are not the total ARP entries. To view the total ARP entries, combine the **show arp** results with the **show arp switch** results (That command is available in the base Layer 2 software package.)

Syntax show arp

Mode Privileged Exec

Example **Figure 22-127. show arp Command Example**

```
(Force10 ) #show arp
Age Time (seconds)..... 1200
Response Time (seconds)..... 1
Retries..... 4
Cache Size..... 1920
Dynamic Renew Mode ..... Enable
Total Entry Count Current / Peak ..... 0 / 0
Static Entry Count Configured / Active / Max .. 0 / 0 / 64

  IP Address          MAC Address          Interface          Type          Age
-----
-----
```

- Report Fields**
- Age Time (seconds)—The time, in seconds, for an ARP entry to age out, as configured into the unit.
 - Response Time (seconds)—The time, in seconds, it takes for an ARP request timeout, as configured into the unit
 - Retries—The maximum number of times an ARP request is retried, as configured into the unit
 - Cache Size—The maximum number of entries in the ARP table. This value was configured into the unit
 - Dynamic Renew Mode—Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out
 - Total Entry Count Current / Peak—The total entries in the ARP table and the peak entry count in the ARP table
 - Static Entry Count Current / Max—The static entry count in the ARP table and maximum static entry count in the ARP table
- The following are displayed for each ARP entry:
- IP Address—The IP address of a device on a subnet attached to an existing routing interface
 - MAC Address—The hardware MAC address of that device
 - Interface—The routing *unit/slot/port* associated with the device ARP entry
 - Type—The type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.
 - Age—The current age of the ARP entry since last refresh (in hh:mm:ss format)

Related Commands	show arp brief	Displays summary Address Resolution Protocol (ARP) information
	show arp switch	Displays connectivity between the switch and other devices

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

- Syntax** show arp brief
- Mode** Privileged Exec

Example **Figure 22-128. show arp Command Example**

```
(Force10 ) #show arp brief
Age Time (seconds)..... 1200
Response Time (seconds)..... 1
Retries..... 4
Cache Size..... 1920
Dynamic Renew Mode ..... Enable
Total Entry Count Current / Peak ..... 0 / 0
Static Entry Count Configured / Active / Max .. 0 / 0 / 64
```

- Report Fields**
- Age Time (seconds)—The time, in seconds, for an ARP entry to age out, as configured into the unit
 - Response Time (seconds)—The time, in seconds, it takes for an ARP request timeout, as configured into the unit
 - Retries—The maximum number of times an ARP request is retried, as configured into the unit
 - Cache Size—The maximum number of entries in the ARP table, as configured into the unit
 - Dynamic Renew Mode—Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
 - Total Entry Count Current / Peak—The total entries in the ARP table and the peak entry count in the ARP table.
 - Static Entry Count Current / Max—The static entry count in the ARP table and maximum static entry count in the ARP table.

**Related
Commands**

show arp	Displays detailed Address Resolution Protocol (ARP) information
show arp switch	Displays connectivity between the switch and other devices

IP Routing

This section provides a detailed explanation of the IP Routing commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

The commands in this section are, in order:

- [encapsulation \(interface\) on page 397](#)
- [ip address \(routed\) on page 398](#)
- [ip forwarding on page 398](#)
- [ip mtu on page 398](#)
- [ip netdirbcast on page 399](#)
- [ip route on page 399](#)
- [ip route default on page 400](#)
- [ip route distance on page 400](#)
- [ip routing on page 400](#)
- [routing on page 401](#)
- [show ip interface on page 401](#)
- [show ip route on page 404](#)
- [show ip route bestroutes on page 405](#)
- [show ip route entry on page 405](#)
- [show ip route preferences on page 406](#)
- [show ip stats on page 406](#)



Note: For ip irdp commands, see [Router Discovery Protocol Commands on page 410](#) later in this chapter.

For ip igmp commands, see the chapter [IGMP Snooping Commands on page 273](#) and [IGMP Commands on page 471](#) in the IP Multicast chapter.

For the ip mcast (multicast) command, see the chapter [IP Multicast Commands on page 457](#).

For the ip ospf commands, see the chapter [OSPF Commands on page 423](#).

encapsulation (interface)

This command configures the link layer encapsulation type for the packet. Acceptable *encapstype* values are ethernet and snap.

Syntax encapsulation {ethernet | snap}

Restrictions—Routed frames are always Ethernet encapsulated when a frame is routed to a VLAN.

Default Ethernet

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

ip address (routed)

This command configures an IP address on a routed interface. The IP address may be a secondary IP address.

Syntax [no] ip address *ipaddr subnetmask* [secondary]

The value for *ipaddr* is the IP address of the interface.

The value for *subnetmask* is a 4-digit dotted-decimal number which represents the subnet mask of the interface.

The **no** version of this command deletes an IP address from an interface.

Mode	Interface Config (including Interface Loopback Config)	
Related Commands	ip address (management)	Configures the IP address of the management interface.
	ip address (VLAN)	Assigns an IP address and subnet mask to the selected VLAN to support Layer 3 routing.

ip forwarding

This command enables forwarding of IP frames.

The **no** version of this command disables forwarding of IP frames.

Syntax [no] ip forwarding

Default enabled

Mode Global Config

ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. However, SFTOS currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the `ip mtu` command.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency unless OSPF has been instructed to ignore differences in IP MTU with the `ip ospf mtu-ignore` command.

Syntax [no] ip mtu *mtu*

The `no` version of this command resets the IP MTU to the default value.

The *mtu* range is 68 bytes to 1500 bytes.

Default 1500 bytes

Mode Interface Config or Interface VLAN

Command History Version 2.3 Modified: Added Interface VLAN as a mode.

ip netdirbcast

This command enables the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled, they are dropped.

Syntax [no] ip netdirbcast

The `no` version of this command disables the forwarding of network-directed broadcasts.

Default disabled

Mode Interface Config or Interface VLAN

Command History Version 2.3 Modified: Added Interface VLAN as a mode.

ip route

This command configures a static route. The *ip_addr* is a valid ip address. The *subnet_mask* is a valid subnet mask. The *nextHopRtr* is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255.

The `no` version of this command deletes all next hops to a destination static route. If the optional *nextHopRtr* parameter is designated, the next hop is deleted and if the optional preference value is designated, the preference value of the static route is reset to its default.

Syntax ip route *ip_addr subnet_mask nextHopRtr [preference]*
no ip route *ip_addr subnet_mask [{nextHopRtr | preference}]*

Default preference - 1

Mode Global Config

ip route default

This command configures the default route. The value for *nextHopRtr* is a valid IP address of the next hop router. The *preference* is an integer value from 1 to 255.

The **no** version of this command deletes all configured default routes. If the optional *nextHopRtr* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Syntax ip route default *nextHopRtr* [*preference*]
no ip route default [{*nextHopRtr* | *preference*}]

Default preference - 1

Mode Global Config

ip route distance

This command sets the default distance for static routes. Lower route preference values are preferred when determining the best route. The “ip route” and “ip route default” commands allow you to optionally set the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the “ip route distance” command.

The **no** version of this command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Syntax ip route distance 1-255
no ip route distance

Default 1

Mode Global Config

ip routing

This command enables the IP Router Admin Mode for the switch.

Syntax [no] ip routing

The **no** version of this command disables the IP Router Admin Mode for the switch.

Mode Global Config

routing

This command enables routing for the selected interface.

Syntax [no] routing

The **no** version of this command disables routing for an interface. The current value for this function is displayed under **show ip interface** labeled as “Routing Mode”.

Default disabled

Mode Interface Config

Related Commands	show ip interface (see below)	Sets the IP gateway of the switch.
	interface	Invokes the Interface ManagementEthernet mode, the (Config-if-ma)# prompt.

show ip interface

This command displays summary information about IP configuration settings for all ports in the router. This command takes no options.

Syntax show ip interface {brief | *unit/slot/port* | vlan 1-3965}

Mode Privileged Exec, User Exec

Example 1 **Figure 22-129. show ip interface brief output Command Example**

```
(Force10) #show ip interface brief
Interface IP Address      IP Mask      Netdir   Multi
-----  -----  -----  -----  -----
1/0/3    10.0.0.2    255.255.255.0  Disable  Disable
```

Report Fields

- Interface**—Valid unit, slot, and port number separated by forward slashes
- IP Address**—The IP address of the routing interface in 32-bit dotted decimal format
- IP Mask**—The IP mask of the routing interface in 32-bit dotted decimal format
- Netdir Bcast**—Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
- MultiCast Fwd**—Indicates the multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

Example 2 **Figure 22-130. show ip interface output Command Example**

```
(Force10) #show ip interface 1/0/1
Routing Mode..... Disable
Administrative Mode..... Disable
Forward Net Directed Broadcasts..... Disable
Proxy ARP..... Enable
Active State..... Inactive
Link Speed Data Rate..... Inactive
MAC Address..... 00:01:E8:D5:A2:1A
Encapsulation Type..... Ethernet
IP MTU..... 1500
```



Note: Example 2 (Figure 22-130 on page 402) shows the output of the command when routing is disabled.

Example 3 (Figure 22-131 on page 402) shows the output when routing is enabled.

Example 3 **Figure 22-131. show ip interface output with Routing Enabled**

```
(Force10) #show ip interface 1/0/1
Primary IP Address..... 1.1.1.10/
255.255.255.0
Routing Mode..... Enable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Disable
Proxy ARP..... Enable
Local Proxy ARP..... Disable
Active State..... Inactive
Link Speed Data Rate..... Inactive
MAC Address..... 00:01:E8:D5:A0:DB
Encapsulation Type..... Ethernet
IP MTU..... 1500
```

Report Fields

Primary IP Address—Displays the primary IP address and subnet masks for the interface. This value appears only if you configure it.

Secondary IP Address—Displays one or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.

Routing Mode—Is the administrative mode of router interface participation. The possible values are Enable or Disable. This value is configured.

Administrative Mode—Is the administrative mode of the specified interface. The possible values of this field are Enable or Disable. This value is configured.

Routing Configuration—Displays whether Routing Configuration is enabled or disabled on the system.

Interface Configuration—Status Displays whether the Interface Configuration is enabled or disabled on the system.

Forward Net Directed Broadcasts—Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value was configured into the unit.

Proxy ARP—Displays whether Proxy ARP is enabled or disabled on the system.

Local Proxy ARP—Displays whether Local Proxy ARP is enabled or disabled on the interface.

Active State—Displays whether the interface is active or inactive. An interface is considered active if its link is up and in forwarding state.

Link Speed Data Rate—Is an integer representing the physical link data rate of the specified interface. This is measured in megabits per second (Mbps).

MAC Address—Is the burned-in physical address of the specified interface. The format is six two-digit hexadecimal numbers separated by colons.

Encapsulation Type—Is the encapsulation type for the specified interface. The types are Ethernet or SNAP.

IP MTU—Displays the maximum transmission unit (MTU) size of a frame, in bytes.

**Related
Commands**

description	Provide a description of the selected interface.
routing	Enables routing for the selected interface
ip address (routed)	Configures an IP address on a routed interface

show ip brief

This command displays all the summary information of the IP. This command takes no options.

Syntax `show ip brief`

Mode Privileged EXEC and User EXEC

Default Time to Live—The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.

Router ID—Is a 32 bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.

Routing Mode—Shows whether the routing mode is enabled or disabled.

IP Forwarding Mode—Shows whether forwarding of IP frames is enabled or disabled. This is a configured value.

show ip interface

This command displays all pertinent information about the IP interface.

Syntax `show ip interface unit/slot/port`

Mode Privileged EXEC and User EXEC

IP Address—Is an IP address representing the subnet configuration of the router interface. This value was configured into the unit.

Subnet Mask—Is a mask of the network and host portion of the IP address for the router interface. This value was configured into the unit.

Routing Mode—Is the administrative mode of router interface participation. The possible values are enable or disable. This value was configured into the unit.

Administrative Mode—Is the administrative mode of the specified interface. The possible values of this field are enable or disable. This value was configured into the unit.

Forward Net Directed Broadcasts—Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value was configured into the unit.

Active State—Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.

Link Speed Data Rate—Is an integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).

MAC Address—Is the burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.

Encapsulation Type—Is the encapsulation type for the specified interface. The types are: Ethernet or SNAP.

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router. This command takes no options.

Syntax show ip interface brief

Mode Global Config

Interface—Unit/Slot/Port (Valid unit, slot and port number separated by forward slashes.) For all interfaces, including VLAN and Port-channel interfaces.

IP Address—The IP address of the interface in 32-bit dotted decimal format.

OK?—**Yes/No**. Indicates if the hardware is functioning properly—hardware and link UP/DOWN.

Method—**manual**(static)/**dynamic**/**unset**. Displays **manual** if the configuration is read from the saved configuration.

Status—**up/down**. States whether the interface is enabled (up) or disabled (administratively down).

Protocol—**up/down**. States whether IP is enabled (up) or disabled (down) on the interface.

show ip route

This command displays the entire route table. This command takes no options.

Syntax show ip route

Mode Privileged Exec

Report Fields Network Address—Is an IP address identifying the network on the specified interface.

Subnet Mask—Is a mask of the network and host portion of the IP address for the router interface.

Protocol—Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

Total Number of Routes—The total number of routes.

For each Next Hop:

Next Hop Intf—The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address—The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

**Related
Commands**

ip routing	Enables the IP Router Admin Mode for the switch
ip address (routed)	Configures an IP address on a routed interface

show ip route bestroutes

This command causes the entire route table to be displayed. This command takes no options.

Syntax show ip route bestroutes

Mode Privileged Exec

Report Fields Network Address—Is an IP route prefix for the destination.

Subnet Mask—Is a mask of the network and host portion of the IP address for the specified interface.

Protocol—Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

Total Number of Routes—The total number of routes in the route table.

For each Next Hop:

Next Hop Intf—The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address—The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

show ip route entry

This command displays the route table for the specified network.

Syntax show ip route entry *network_address*

Mode Privileged Exec

Report Fields Network Address—Is a valid network address identifying the network on the specified interface.

Subnet Mask—Is a mask of the network and host portion of the IP address for the attached network.

Protocol—Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.

For each Next Hop:

Next Hop Interface—The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address—The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Preference—The metric value that is used for this route entry.

show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

Syntax show ip route preferences

Mode Privileged Exec and User Exec

Report Fields Local—This field displays the local route preference value.

Static—This field displays the static route preference value.

OSPF Intra—This field displays the OSPF Intra route preference value.

OSPF Inter—This field displays the OSPF Inter route preference value.

OSPF Type-1—This field displays the OSPF Type-1 route preference value.

OSPF Type-2—This field displays the OSPF Type-2 route preference value.

RIP—This field displays the RIP route preference value.

show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed. This command takes no options.

Syntax show ip stats

Mode Privileged Exec and User Exec

traceroute

This command is used to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. <ipaddr> should be a valid IP address. [port] should be a valid decimal integer in the range of 0(zero) to 65535. The default value is 33434.

Format `traceroute <ipaddr> [<port>]`
Mode `Privileged EXEC`

Bootp/DHCP Relay Commands

This section provides a detailed explanation of the BootP/DHCP Relay commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

The commands in this section are, in order:

- [bootpdhcprelay cidoptmode on page 407](#)
- [bootpdhcprelay enable on page 407](#)
- [bootpdhcprelay maxhopcount on page 408](#)
- [bootpdhcprelay minwaittime on page 408](#)
- [bootpdhcprelay serverip on page 408](#)
- [show bootpdhcprelay on page 409](#)

bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

The `no` version of this command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Syntax `[no] bootpdhcprelay cidoptmode`

Default `disabled`

Mode `Global Config`

bootpdhcprelay enable

This command enables the forwarding of BootP/DHCP relay requests by the switch.

The `no` version of this command disables the forwarding of relay requests.

Syntax `[no] bootpdhcprelay enable`

Default `disabled`

Mode `Global Config`

bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops. The parameter has a range of 1 to 16.

The `no` version of this command sets the maximum allowable hops to the default.

Syntax `bootpdhcprelay maxhopcount 1-16`

`no bootpdhcprelay maxhopcount`

Default 4

Mode Global Config

bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

The `no` version of this command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Syntax `bootpdhcprelay minwaittime 0-100`

`no bootpdhcprelay minwaittime`

Default 0

Mode Global Config

bootpdhcprelay serverip

This command configures the server IP address of the DHCP server. The *ipaddr* parameter is an IP address in a 4-digit dotted decimal format.

The `no` version of this command configures the default server IP Address for BootP/DHCP Relay on the system.

Syntax `bootpdhcprelay serverip ipaddr`

`no bootpdhcprelay serverip`

Default 0.0.0.0

Mode Global Config

show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Syntax show bootpdhcprelay

Mode Privileged Exec and User Exec

Example **Figure 22-132. show bootpdhcprelay Command Example**

```
(Force10 ) #show bootpdhcprelay
Maximum Hop Count..... 4
Minimum Wait Time(Seconds)..... 0
Admin Mode..... Disable
Server IP Address..... 0.0.0.0
Circuit Id Option Mode..... Disable
Requests Received..... 0
Requests Relayed..... 0
Packets Discarded..... 0
```

- Report Fields**
- Maximum Hop Count—Is the maximum allowable relay agent hops.
 - Minimum Wait Time (Seconds)—Is the minimum wait time.
 - Admin Mode—Represents whether relaying of requests is enabled or disabled.
 - Server IP Address—Is the IP Address for the BootP/DHCP Relay server.
 - Circuit Id Option Mode—Is the DHCP circuit Id option which may be enabled or disabled.
 - Requests Received—Is the number or requests received.
 - Requests Relayed—Is the number of requests relayed.
 - Packets Discarded—Is the number of packets discarded.

Router Discovery Protocol Commands

This section provides a detailed explanation of router discovery commands using IRDP (ICMP Router Discovery Protocol) (ICMP is Internet Control Message Protocol).

The commands in this section are, in order:

- [ip irdp on page 410](#)
- [ip irdp address on page 410](#)
- [ip irdp holdtime on page 411](#)
- [ip irdp maxadvertinterval on page 411](#)
- [ip irdp minadvertinterval on page 411](#)
- [ip irdp preference on page 412](#)
- [show ip irdp on page 412](#)

ip irdp

This command enables router discovery from a selected interface or VLAN.

The `no` version of this command disables Router Discovery on an interface.

Syntax	[no] ip irdp				
Default	enabled				
Mode	Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.				
Command History	<table border="1"> <tr> <td>Version 2.3</td> <td>Added Interface VLAN and Interface Range modes.</td> </tr> </table>	Version 2.3	Added Interface VLAN and Interface Range modes.		
Version 2.3	Added Interface VLAN and Interface Range modes.				
Related Commands	<table border="1"> <tr> <td>interface range</td> <td>Defines an interface range and accesses the Interface Range mode</td> </tr> <tr> <td>interface vlan</td> <td>Defines a VLAN and accesses the Interface VLAN mode</td> </tr> </table>	interface range	Defines an interface range and accesses the Interface Range mode	interface vlan	Defines a VLAN and accesses the Interface VLAN mode
interface range	Defines an interface range and accesses the Interface Range mode				
interface vlan	Defines a VLAN and accesses the Interface VLAN mode				

ip irdp address

This command configures the address to be used to advertise the router for the interface or VLAN. The valid values for `ipaddr` are 224.0.0.1 and 255.255.255.255.

The `no` version of this command configures the default address to be used to advertise the router for the interface.

Syntax	ip irdp address <i>ipaddr</i> no ip irdp address		
Default	224.0.0.1		
Mode	Interface Config or Interface VLAN		
Command History	<table border="1"> <tr> <td>Version 2.3</td> <td>Modified: Added Interface VLAN as a mode.</td> </tr> </table>	Version 2.3	Modified: Added Interface VLAN as a mode.
Version 2.3	Modified: Added Interface VLAN as a mode.		

ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface or VLAN.

Syntax ip irdp holdtime *maxadvertinterval-9000*

The range is the maxadvertinterval to 9000 seconds.

The no ip irdp holdtime command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Default 3 * maxinterval

Mode Interface Config or Interface VLAN

Command History Version 2.3 Modified: Added Interface VLAN as a mode.

ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface or VLAN.

Syntax ip irdp maxadvertinterval *4-1800*

The range for maxadvertinterval is 4 to 1800 seconds.

The no ip irdp maxadvertinterval command reverts the maximum time to the default, in seconds.

Default 600

Mode Interface Config or Interface VLAN

Command History Version 2.3 Modified: Added Interface VLAN as a mode.

ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface or VLAN.

Syntax ip irdp minadvertinterval *3-maxadvertinterval*

The range for minadvertinterval is 3 to the value of maxadvertinterval.

The no ip irdp minadvertinterval command reverts the minimum time to the default time, in seconds.

Default 0.75 * maxadvertinterval

Mode	Interface Config or Interface VLAN
Command History	Version 2.3 Modified: Added Interface VLAN as a mode.

ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.

Syntax ip irdp preference *-2147483648-2147483647*

The range is -2147483648 to -1 to 0 to 1 to 2147483647.

The no ip irdp preference command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Default 0

Mode Interface Config or Interface VLAN

Command History	Version 2.3 Modified: Added Interface VLAN as a mode.
------------------------	--

show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Syntax show ip irdp {*unit/slot/port* | all}

Mode Privileged Exec and User Exec

Report Fields Interface — Shows the port number (*unit/slot/port*) that matches the rest of the information in the row.

Ad Mode—Displays the advertise mode which indicates whether router discovery is enabled or disabled on this interface.

Advertise Address — Displays the IP address to which the interface sends the advertisement.

Max Int—Displays the maximum advertise interval which is the maximum time allowed between sending router advertisements from the interface in seconds.

Min Int—Displays the minimum advertise interval which is the minimum time allowed between sending router advertisements from the interface in seconds.

Adv Life—Displays advertise lifetime which is the value of the lifetime field of the router advertisement sent from the interface in seconds.

Preferences—Displays the preference of the address as a default router address, relative to other router addresses on the same subnet.

Example **Figure 22-133. Example of show ip irdp Command Output**

```
Force10 #show ip irdp 1/0/1
Interface  Ad Mode  Advertise Address  Max Int  Min Int  Hold Time  Preference
-----
1/0/1      Disable  224.0.0.1          600      450     1800      0
Force10#
```

Virtual LAN Routing Commands

This section contains the Virtual LAN Routing (VLAN Routing) commands:

- [ip address \(VLAN\) on page 413](#)
- [show ip vlan on page 413](#)
- [vlan routing on page 414](#)

ip address (VLAN)

This command assigns an IP address and subnet mask to the selected VLAN to support Layer 3 routing.

Syntax `ip address ip_address subnet_mask`

The no version of this command deletes routing on the selected VLAN.

Mode Interface VLAN

Command History

Version 2.3	Introduced. Replaces <code>vlan routing</code> .
-------------	--

Related Commands

interface vlan	Creates a VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
--------------------------------	--

show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled in the system.

Syntax `show ip vlan`

Mode Privileged Exec and User Exec

Report Fields MAC Address used by Routing VLANs—Is the MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.

VLAN ID—Is the identifier of the VLAN.

Logical Interface—Indicates the logical *unit/slot/port* associated with the VLAN routing interface.

IP Address—Displays the IP Address associated with this VLAN.

Subnet Mask—Indicates the subnet mask that is associated with this VLAN.

vlan routing

Command History	Version 2.3 Deprecated. Replaced by ip address (VLAN) .
Related Commands	ip address (VLAN) Assigns an IP address and subnet mask to the selected VLAN.

Virtual Router Redundancy Protocol (VRRP) Commands

This section provides a detailed explanation of the VRRP commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a **show** command that will display the configuration setting.

The commands in this section are, in order:

- [ip vrrp \(global\) on page 414](#)
- [ip vrrp <vrID> on page 415](#)
- [ip vrrp authentication on page 415](#)
- [ip vrrp ip on page 416](#)
- [ip vrrp mode on page 416](#)
- [ip vrrp preempt on page 417](#)
- [ip vrrp priority on page 418](#)
- [ip vrrp timers advertise on page 418](#)
- [show ip vrrp interface stats on page 419](#)
- [show ip vrrp on page 420](#)
- [show ip vrrp interface on page 420](#)
- [show ip vrrp interface brief on page 420](#)

ip vrrp (global)

This command enables the administrative mode of VRRP in the router. This command also designates the configured virtual router IP address as a secondary IP address on an interface.

The **no** version of this command disables the default administrative mode of VRRP in the router.

Syntax [no] ip vrrp

Default	enabled
Mode	Global Config

ip vrrp <vrID>

This command sets the VRID (virtual router ID) on an interface for virtual router configuration in the router. This command also has options, detailed below, to designate the configured virtual router IP address, set the mode, and set authentication.

Syntax [no] ip vrrp *vrID*

The *vrID* parameter is the virtual router ID; it is an integer value with a range from 1 to 255. Pressing Enter without including a value for *ipaddress* creates the VRID on the interface.

The no version of this command removes all VRRP configuration details of the virtual router configured on a specific interface.

Default none

Mode Interface Config or Interface VLAN

Command History

Version 2.3	Modified. Added Interface VLAN mode.
-------------	--------------------------------------

Related Commands

interface vlan	Creates a VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN
ip vrrp authentication	Sets the authorization details value for the virtual router configured on a specified interface
ip vrrp ip	Sets the IP address value for a virtual router
ip vrrp mode	Enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router.
ip vrrp preempt	Sets the preemption mode value for the virtual router configured on a specified interface
ip vrrp priority	Sets the priority value for the virtual router configured on a specified interface
ip vrrp timers advertise	Sets the advertisement value for a virtual router

ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface.

Syntax [no] ip vrrp *vrID* authentication {none | simple [*key*]}

The parameter *vrID* is the virtual router ID, which has an integer value that ranges from 1 to 255.

The parameter {none | simple} specifies the authorization type for virtual router configured on the specified interface. The *key* is optional, only required when the authorization type is **simple** (text password).

The `no ip vrrp vrID authentication` command sets the default authorization details value for the virtual router configured on a specified interface.

Default	no authorization	
Mode	Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	<hr/> Version 2.3 Added Interface Range and Interface VLAN modes. <hr/>	
Related Commands	<hr/> interface range Defines an interface range and accesses the Interface Range mode <hr/> interface vlan Creates a new VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN. <hr/> ip vrrp <vrID> Sets the VRID (virtual router ID) on an interface for virtual router configuration in the router. This command also has options. <hr/>	

ip vrrp ip

This command sets the IP address value for a virtual router.

Syntax	<code>ip vrrp vrID ip addr [secondary]</code>	
	The parameter <i>vrID</i> is the virtual router ID which has an integer value range from 1 to 255.	
	The value for <i>addr</i> is the IP address to be configured on that interface for VRRP.	
	(OPTIONAL) The keyword <i>secondary</i> designates that the IP address is a secondary address on this interface.	
Default	none	
Mode	Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	<hr/> Version 2.3 Added Interface Range and Interface VLAN modes. <hr/>	
Related Commands	<hr/> interface range Defines an interface range and accesses the Interface Range mode <hr/> interface vlan Creates a new VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN. <hr/> ip vrrp <vrID> Sets the VRID (virtual router ID) on an interface for virtual router configuration in the router. This command also has options. <hr/>	

ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router.

Syntax [no] ip vrrp *vrID* mode

The parameter *vrID* is the virtual router ID, which has an integer value ranging from 1 to 255.

The no version of this command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Default disabled

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

interface vlan	Creates a VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
--------------------------------	--

ip vrrp <vrID>	Sets the VRID (virtual router ID) on an interface for virtual router configuration in the router. This command also has options.
--------------------------------------	--

ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface.

Syntax [no] ip vrrp *vrID* preempt

The parameter *vrID* is the virtual router ID which has an integer value range from 1 to 255.

The no version of this command sets the default preemption mode value for the virtual router configured on a specified interface.

Default enabled

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

interface vlan	Creates a VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
--------------------------------	--

ip vrrp <vrID>	Sets the VRID (virtual router ID) on an interface for virtual router configuration in the router. This command also has options.
--------------------------------------	--

ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface.

Syntax ip vrrp *vrID* priority 1-254

The parameter *vrID* is the virtual router ID, which is an integer that ranges from 1 to 255.

The priority of the interface is an integer from 1 to 254.

The no ip vrrp *vrID* priority command sets the default priority value for the virtual router configured on a specified interface.

Default 100

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

interface vlan	Creates a VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
--------------------------------	--

ip vrrp <vrID>	Sets the VRID (virtual router ID) on an interface for virtual router configuration in the router. This command also has options.
--------------------------------------	--

ip vrrp timers advertise

This command sets the advertisement value for a virtual router.

Syntax ip vrrp *vrID* timers advertise 1-255

The parameter *vrID* is the virtual router ID, which is an integer that ranges from 1 to 255.

The value for **advertise** interval is the time used for VRRP advertisements in seconds.

The no ip vrrp *vrID* timers advertise command sets the default advertisement value for a virtual router.

Default 1

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

<code>interface vlan</code>	Creates a VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
<code>ip vrrp <vrID></code>	Sets the VRID (virtual router ID) on an interface for virtual router configuration in the router. This command also has options.

show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the SFTOS switch.

Syntax `show ip vrrp interface stats unit/slot/port vrid`

Mode Privileged Exec and User Exec

Is the time that the virtual router has been up, in days, hours, minutes and seconds.

Report Fields State Transitioned to Master—Represents the total number of times virtual router state has changed to MASTER.

Advertisement Received—Represents the total number of VRRP advertisements received by this virtual router.

Advertisement Interval Errors—Represents the total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.

Authentication Failure—Represents the total number of VRRP packets received that don't pass the authentication check.

IP TTL errors—Represents the total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.

Zero Priority Packets Received—Represents the total number of VRRP packets received by virtual router with a priority of '0'.

Zero Priority Packets Sent—Represents the total number of VRRP packets sent by the virtual router with a priority of '0'.

Invalid Type Packets Received—Represents the total number of VRRP packets received by the virtual router with invalid 'type' field.

Address List Errors—Represents the total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.

Invalid Authentication Type—Represents the total number of VRRP packets received with unknown authentication type.

Authentication Type Mismatch—Represents the total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.

Packet Length Errors—Represents the total number of VRRP packets received with packet length less than length of VRRP header

show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the SFTOS switch. It also displays some global parameters which are required for monitoring. This command takes no options.

Syntax show ip vrrp

Mode Privileged Exec and User Exec

Report Fields VRRP Admin Mode—Displays the administrative mode for VRRP functionality on the switch.

Router Checksum Errors—Represents the total number of VRRP packets received with an invalid VRRP checksum value.

Router Version Errors—Represents the total number of VRRP packets received with Unknown or unsupported version number.

Router VRID Errors—Represents the total number of VRRP packets received with invalid VRID for this virtual router.

show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Syntax show ip vrrp interface *unit/slot/port vrid*

Mode Privileged Exec and User Exec

Report Fields IP Address—This field represents the configured IP Address for the Virtual router.

VMAC address—Represents the VMAC address of the specified router.

Authentication type—Represents the authentication type for the specific virtual router.

Priority—Represents the priority value for the specific virtual router.

Advertisement interval—Represents the advertisement interval for the specific virtual router.

Pre-Empt Mode—Is the preemption mode configured on the specified virtual router.

Administrative Mode—Represents the status (Enable or Disable) of the specific router.

State—Represents the state (Master/backup) of the specific virtual

show ip vrrp interface brief

This command displays information about each virtual router configured on the SFTOS switch. This command takes no options. It displays information about each virtual router.

Syntax show ip vrrp interface brief

Mode Privileged Exec and User Exec

Report Fields Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

VRID—Represents the router ID of the virtual router.

IP Address—Is the IP Address that was configured on the virtual router

Mode—Represents whether the virtual router is enabled or disabled.

State—Represents the state (Master/backup) of the virtual router.

OSPF Commands

This chapter provides a detailed explanation of the Open Shortest Path First (OSPF) commands. The commands are divided by functionality into the following groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

This chapter provides detail on the following commands:

- [1583compatibility on page 424](#)
- [area authentication on page 425](#)
- [area default-cost on page 425](#)
- [area nssa on page 425](#)
- [area nssa default-info-originate on page 425](#)
- [area nssa no-redistribute \(OSPF\) on page 425](#)
- [area nssa no-summary \(OSPF\) on page 426](#)
- [area nssa translator-role \(OSPF\) on page 426](#)
- [area nssa translator-stab-intv on page 426](#)
- [area range on page 426](#)
- [area stub on page 427](#)
- [area stub summarylsa on page 427](#)
- [area virtual-link on page 427](#)
- [area virtual-link authentication on page 427](#)
- [area virtual-link dead-interval on page 428](#)
- [area virtual-link hello-interval on page 428](#)
- [area virtual-link retransmit-interval on page 429](#)
- [area virtual-link transmit-delay on page 429](#)
- [default-information originate \(OSPF\) on page 430](#)
- [default-metric \(OSPF\) on page 430](#)
- [distance ospf on page 430](#)
- [distribute-list out on page 430](#)
- [enable \(OSPF\) on page 431](#)
- [exit-overflow-interval on page 431](#)
- [external-lsdb-limit on page 431](#)
- [ip ospf on page 432](#)
- [show ip ospf abr on page 440](#)
- [ip ospf areaid on page 432](#)
- [ip ospf authentication on page 433](#)

- [ip ospf authentication-key on page 433](#)
- [ip ospf cost on page 434](#)
- [ip ospf dead-interval on page 434](#)
- [ip ospf hello-interval on page 435](#)
- [ip ospf mtu-ignore on page 436](#)
- [ip ospf priority on page 436](#)
- [ip ospf retransmit-interval on page 436](#)
- [ip ospf transmit-delay on page 437](#)
- [maximum-paths on page 438](#)
- [router-id on page 438](#)
- [router-id on page 438](#)
- [redistribute on page 438](#)
- [show ip ospf on page 439](#)
- [show ip ospf abr on page 440](#)
- [show ip ospf area on page 440](#)
- [show ip ospf database on page 441](#)
- [show ip ospf interface on page 441](#)
- [show ip ospf interface brief on page 443](#)
- [show ip ospf interface stats on page 443](#)
- [show ip ospf neighbor on page 444](#)
- [show ip ospf range on page 446](#)
- [show ip ospf stub table on page 447](#)
- [show ip ospf virtual-link on page 447](#)
- [show ip ospf virtual-link brief on page 448](#)
- [trapflags on page 448](#)

1583compatibility

This command enables OSPF 1583 compatibility.

The `no` version of this command disables OSPF 1583 compatibility.



Note: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Syntax	[no] 1583compatibility
Default	enabled
Mode	Router OSPF Config

area authentication

Command History	Version 2.3	Deprecated
------------------------	-------------	------------

area default-cost

This command configures the monetary default cost for the stub area. The operator must specify the area ID and an integer value between 1-16777215.

Syntax `area areaid default-cost 1-16777215`

Mode Router OSPF Config

area nssa

This command configures the specified *areaid* to function as an NSSA (Not So Stubby Area).

The `no` version of this command disables `nssa` from the specified area ID.

Syntax `[no] area areaid nssa`

Mode Router OSPF Config

area nssa default-info-originate

This command configures the metric value and type for the default route advertised into the NSSA.

Syntax `area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

The optional *metric* parameter specifies the metric of the default route and is to be in a range of 1-16777215. If no metric is specified, the default value is `****`. The metric type can be `comparable` (`nssa-external 1`) or `non-comparable` (`nssa-external 2`).

Mode Router OSPF Config

area nssa no-redistribute (OSPF)

This command configures the NSSA ABR (Area Border Router) so that learned external routes will not be redistributed to the NSSA.

Syntax `area areaid nssa no-redistribute`

Mode Router OSPF Config

area nssa no-summary (OSPF)

This command configures the NSSA so that summary Link State Advertisements (LSAs) are not advertised into the NSSA.

Syntax `area areaid nssa no-summary`

Mode Router OSPF Config

area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of *always* will cause the router to assume the role of the translator the instant it becomes a border router and a value of *candidate* will cause the router to participate in the translator election process when it attains border router status

Syntax `area areaid nssa translator-role {always | candidate}`

Mode Router OSPF Config

area nssa translator-stab-intv

This command configures the translator stability interval of the NSSA. The stability interval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Syntax `area areaid nssa translator-stab-intv stabilityinterval`

Mode Router OSPF Config

area range

This command creates a specified area range for a specified NSSA.

Syntax `area areaid range ipaddr subnetmask {summarylink | nssaexternallink} [advertise | not-advertise]`

The *ipaddr* is a valid IP address. The *subnetmask* is a valid subnet mask. The Link-State Database (LSDB) type must be specified by either *summarylink* or *nssaexternallink*, and the advertising of the area range can be optionally allowed or suppressed.

The `no area areaid range ipaddr subnetmask` version of this command deletes a specified area range.

Mode Router OSPF Config

area stub

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

The `no` version of this command deletes a stub area for the specified area ID.

Syntax `area areaid stub`

Mode Router OSPF Config

area stub summarylsa

This command configures the Summary LSA mode for the stub area identified by *areaid*. The Summary LSA mode is configured as enabled.

The `no` version of this command configures the default Summary LSA mode for the stub area identified by *areaid*.

Syntax `[no] area areaid stub summarylsa`

Default disabled

Mode Router OSPF Config

area virtual-link

This command creates the OSPF virtual interface for the specified *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

The `no` version of this command deletes the OSPF virtual interface from the given interface, identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Syntax `[no] area areaid virtual-link neighbor`

Mode Router OSPF Config

area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by *areaid* and *neighbor*.

Syntax `area areaid virtual-link neighbor authentication {none | {simple key} | {encrypt key keyid}}`

The *neighbor* parameter is the Router ID of the neighbor.

The authentication type is either `none` (the default), `simple`, or `encrypt`.

If the authentication type is **simple**, the authentication key must be 8 bytes or less. If the type is **encrypt**, the key may be up to 256 bytes. The *key* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard.

If the type is **encrypt**, a key ID in the range of 0 and 255 must be specified for *keyid*.

Neither the default password key nor the default key ID are configured.

Unauthenticated interfaces do not need an authentication key.

The **no area *areaid* virtual-link *neighbor authentication*** command configures the default authentication type for the OSPF virtual interface identified by *areaid* and *neighbor*.

Default	none
Mode	Router OSPF Config

area virtual-link dead-interval

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 1 to 65535.

The **no** version of this command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Syntax	area <i>areaid</i> virtual-link <i>neighbor</i> dead-interval 1-65535
	no area <i>areaid</i> virtual-link <i>neighbor</i> dead-interval
Default	40
Mode	Router OSPF Config

area virtual-link hello-interval

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Syntax	area <i>areaid</i> virtual-link <i>neighbor</i> hello-interval 1-65535
---------------	--

The *neighbor* parameter is the Router ID of the neighbor.

The 1-65535 parameter is the hello interval in seconds, specified as an integer.

Range: 1 to 65535

The `no area areaid virtual-link neighbor hello-interval` command invokes the default hello interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*.

Default	10
Mode	Router OSPF Config
Related Commands	<hr/> show ip ospf interface Displays the information for the IFO object or virtual interface tables <hr/>

area virtual-link retransmit-interval

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 0 to 3600.

The `no` version of this command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Syntax `area areaid virtual-link neighbor retransmit-interval 0-3600`

`no area areaid virtual-link neighbor retransmit-interval`

Default 5

Mode Router OSPF Config

area virtual-link transmit-delay

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor. The range for *seconds* is 0 to 3600 (1 hour).

The `no` version of this command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by *areaid* and *neighbor*. The *neighbor* parameter is the Router ID of the neighbor.

Syntax `area areaid virtual-link neighbor transmit-delay 0-3600`

`no area areaid virtual-link neighbor transmit-delay`

Default 1

Mode Router OSPF Config

default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Syntax default-information originate [always] [metric *0-16777215*] [metric-type {1 | 2}]

The no default-information originate [metric] [metric-type] command sets the advertisement of routes to the default.

Default metric—unspecified; type—2

Mode Router OSPF Config

default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Syntax default-metric *1-16777215*

The no default-metric command sets a default for the metric of distributed routes.

Mode Router OSPF Config

distance ospf

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route.

Syntax distance ospf {intra | inter | type1 | type2} *0-255*

The type of OSPF can be intra, inter, type1, or type2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type1 < **type2**.

The route preference range is 0 to 255.

The no distance ospf {intra | inter | type1 | type2} command sets the default route preference value of OSPF in the router.

Default intra = 8; inter = 10; type1 = 13; type2 = 150

Mode Router OSPF Config

distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Syntax [no] distribute-list *1-199* out {rip | static | connected}

The **no** version of this command is used to specify the access list to filter routes received from the source protocol.

Mode Router OSPF Config

enable (OSPF)

This command resets the default administrative mode of OSPF in the router (active).

The **no** version of this command sets the administrative mode of OSPF in the router to inactive.

Syntax [no] enable

Default enabled

Mode Router OSPF Config

exit-overflow-interval

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering overflow state that a router will wait before attempting to leave the overflow state. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave overflow state until restarted.

Syntax exit-overflow-interval *0-2147483647*

The range for *seconds* is 0 to 2147483647 seconds.

The **no** version of this command sets the exit overflow interval for OSPF to the default.

Default 0

Mode Router OSPF Config

external-lsdb-limit

This command configures the external LSDB limit for OSPF. When the number of non-default AS-external-LSAs in a router's LSDB reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in its database. The external LSDB limit **MUST** be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.

The **no** version of this command configures the default external LSDB limit for OSPF.

Syntax external-lsdb-limit *limit*

no external-lsdb-limit

If the value of *limit* is -1, then there is no limit. The range for *limit* is -1 to 2147483647.

Default -1

Router OSPF Config

ip ospf

This command enables OSPF on a router interface.

Syntax [no] ip ospf

The **no** version of this command disables OSPF on a router interface.

Default disabled

Mode Interface Config (including Interface Loopback Config mode) or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

Command History

Version 2.5	Modified: Added Interface Loopback Config mode.
-------------	---

Version 2.3	Modified: Added Interface VLAN as a mode.
-------------	---

ip ospf areaid

This command sets the OSPF area to which the specified router interface belongs.

Syntax ip ospf areaid *areaid*

The value for *areaid* is an IP address, formatted as a 4-digit dotted-decimal number that uniquely identifies the area to which the interface connects. Assigning an area ID that does not exist on an interface causes the area to be created with default values.

Mode Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
---------------------------------	--

interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.
--------------------------------	---

ip ospf authentication

This command enables you to select either no or simple OSPF authentication for the specified interface. If simple authentication is selected, you then select a plain-text key.

Syntax ip ospf authentication {none | simple *key*}

The type is either **none** or **simple**. The *key* is composed of standard displayable, non-control keystrokes from a standard 101/102-key keyboard and must be 8 bytes or less.

The **no ip ospf authentication** command sets the OSPF authentication type for the specified interface to the default.

Default The default authentication type is **none**.

Default The default password *key* is not configured. Unauthenticated interfaces do not need an authentication key.

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes. Modified: Separated ip ospf authentication into two commands— ip ospf authentication and ip ospf authentication-key , and removed encrypt as a parameter.
-------------	--

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.
ip ospf authentication-key	Sets the OSPF authentication key for the specified interface.

ip ospf authentication-key

This command sets the OSPF MD5 authentication key and key ID for the specified interface.

Syntax ip ospf authentication-key *key keyid*

The *key* is the MD5 authentication key, which must be 8 bytes or less and composed of standard displayable, non-control keystrokes from a standard 101/102-key keyboard.

The *keyid* range is 0 to 255.

To set the OSPF MD5 authentication key for the specified interface to the default of none, use the **no ip ospf authentication-key** command.

Default The default password *key* is not configured. Unauthenticated interfaces do not need an authentication key.

Default The default *keyid* is not configured. Unauthenticated interfaces do not need an authentication key ID.

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.3	Added Interface Range and Interface VLAN modes. Modified: Separated <code>ip ospf authentication</code> into two commands— <code>ip ospf authentication</code> and <code>ip ospf authentication-key</code> , and removed <code>encrypt</code> as a parameter.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.
	ip ospf authentication	Sets the OSPF Authentication Type and Key for the specified interface.

ip ospf cost

This command configures the cost on an OSPF interface.

Syntax `ip ospf cost 1-65535`

`1-65535` represents the cost for the specified interface or VLAN.

The `no ip ospf cost` command configures the cost on an OSPF interface to the default.

Default 10

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.3	Added Interface Range and Interface VLAN modes.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode

ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface.

Syntax `ip ospf dead-interval seconds`

The *seconds* parameter is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers should declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello interval.

Range: 1 to 2147483647

The `no ip ospf dead-interval` command sets the OSPF dead interval for the specified interface to the default.

Default 40 seconds

Mode	Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Added Interface Range and Interface VLAN modes.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.
	ip ospf hello-interval	Sets the OSPF hello interval for the specified interface
	show ip ospf neighbor	Displays the OSPF neighbor table list
	show ip ospf interface	Displays the information for the IFO object or virtual interface tables

ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface.

Syntax ip ospf hello-interval *seconds*

The value for *seconds* is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network.

Range: 1 to 65535

The no ip ospf hello-interval command sets the OSPF hello interval for the specified interface to the default.

Default 10

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.3	Added Interface Range and Interface VLAN modes.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.
	ip ospf dead-interval	Sets the OSPF dead interval for the specified interface
	show ip ospf interface	Displays the information for the IFO object or virtual interface tables

ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Syntax	[no] ip ospf mtu-ignore
	The no version of this command enables the OSPF MTU mismatch detection.
Default	Enabled
Mode	Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	<hr/> Version 2.3 Added Interface Range and Interface VLAN modes. <hr/>
Related Commands	<hr/> interface range Defines an interface range and accesses the Interface Range mode <hr/> interface vlan Creates a VLAN or selects an existing one and enters the Interface VLAN mode. <hr/>

ip ospf priority

This command sets the OSPF priority for the specified router interface.

Syntax	ip ospf priority 0-255
	The priority of the interface is an integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.
	The no ip ospf priority command sets the OSPF priority to the default for the specified router interface.
Default	1 (which is the highest router priority)
Mode	Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	<hr/> Version 2.3 Added Interface Range and Interface VLAN modes. <hr/>
Related Commands	<hr/> interface range Defines an interface range and accesses the Interface Range mode <hr/> interface vlan Creates a VLAN or selects an existing one and enters the Interface VLAN mode. <hr/>

ip ospf retransmit-interval

This command sets the OSPF retransmit interval for the specified interface. The retransmit interval is specified in seconds.

Syntax `ip ospf retransmit-interval seconds`

The value for *seconds* is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database and link-state request packets.

Range: 0 to 3600 seconds (1 hour)

The `no ip ospf retransmit-interval` command sets the OSPF retransmit interval for the specified interface to the default.

Default 5 (seconds)

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip ospf transmit-delay

This command sets the OSPF transit delay for the specified interface.

Syntax `ip ospf transmit-delay seconds`

The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface.

Range: 1 to 3600 (1 hour)

The `no ip ospf transmit-delay` command sets the OSPF Transit Delay for the specified interface to the default.

Default 1

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

maximum-paths

This command sets the number of paths that OSPF can report for a given destination where `maxpaths` is platform dependent.

The `no` version of this command resets the number of paths that OSPF can report for a given destination back to its default value.

Syntax	<code>maximum-paths <i>maxpaths</i></code> <code>no maximum-paths</code>
Default	4
Mode	OSPF Router Config

router-id

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf ID. The `ipaddress` is a configured value.

Syntax	<code>router-id <i>ipaddress</i></code>
Mode	Router OSPF Config

router ospf

In the Global Config mode, enter the `router ospf` command to access Router OSPF Config mode. To exit to the Global Config mode from the Router OSPF Config mode, enter the `exit` command.

redistribute

This command configures OSPF protocol to redistribute routes from the specified source protocol/routers.

The `no` version of this command configures OSPF protocol to redistribute routes from the specified source protocol/routers.

Syntax	<code>redistribute {rip static connected} [metric <i>0-16777215</i>] [metric-type {1 2}] [tag <i>0-4294967295</i>] [subnets]</code> <code>no redistribute {rip static connected} [metric] [metric-type] [tag] [subnets]</code>
Default	metric—unspecified; type—2; tag—0
Mode	Router OSPF Config

show ip ospf

This command displays information relevant to the OSPF router. This command takes no options.

Syntax show ip ospf

Mode Privileged Exec

Example **Figure 23-134. Example Output from the show ip ospf Command**

```
S50V-1#show ip ospf
Router ID..... 0.0.0.0
OSPF Admin Mode..... Disable
ASBR Mode..... Disable
RFC 1583 Compatibility..... Enable

OSPF must first be initialized for the switch.
```

Report Fields Router ID—Is a 32-bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.

OSPF Admin Mode—The administrative mode of OSPF in the router. This is a configured value.

ASBR Mode—Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).

RFC 1583 Compatibility—Reflects whether 1583 compatibility is enabled or disabled. This is a configured value.

The information below is only displayed if OSPF is enabled:

ABR Status—Reflects the whether or not the router is an OSPF Area Border Router

Exit Overflow Interval—The number of seconds that, after entering OverflowState, a router will attempt to leave OverflowState

External LSA count—The number of external (LS type 5) link-state advertisements in the link-state database

External LSA Checksum—A number representing the sum of the LS checksums of external link-state advertisements contained in the link-state database

New LSAs Originated—The number of new link-state advertisements that have been originated

LSAs Received—The number of link-state advertisements received determined to be new instantiations

External LSDB Limit—The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database

Default-metric—Default value for redistributed routes

Source—Source protocol/routes that are being redistributed

Metric-value—Metric of the routes being redistributed

Type-value—External Type 1 or External Type 2 routes

Tag-value—Decimal value attached to each external route

Subnets—For redistributing routes into OSPF, the scope of redistribution for the specified protocol

Distribute-list—The access list used to filter redistributed routes

Default-info originate—Indicates whether the default routes received from other source protocols are advertised or not

Max Paths—Maximum number of paths that OSPF can report for a given destination

show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR).

Syntax show ip ospf abr

Mode Privileged Exec and User Exec

Report Fields Type—The type of the route to the destination. It can be either:

- intra — Intra-area route
- inter — Inter-area route

Router ID—Router ID of the destination

Cost—Cost of using this route

Area ID—The area ID of the area from which this route is learned

Next Hop—Next hop toward the destination

Next Hop Intf—The outgoing router interface to use when forwarding traffic to the next hop

show ip ospf area

This command displays information about the area. The *areaid* identifies the OSPF area that is being displayed.

Syntax show ip ospf area *areaid*

Mode Privileged Exec and User Exec

Report Fields AreaID—The area ID of the requested OSPF area

Aging Interval—A number representing the aging interval for this area

External Routing—A number representing the external routing capabilities for this area

Authentication Type—The configured authentication type to use for this area

Spf Runs—Number of times that the intra-area route table has been calculated using this area's link-state database

Area Border Router Count—Total number of area border routers reachable within this area

Area LSA Count—Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.

Area LSA Checksum—A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.

Stub Mode—Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.

**Import Summary
LSAs**

Metric Value—A number representing the Metric Value for the specified area

Metric Type—The Default Metric Type for the specified area

show ip ospf database

This command displays the link state database. This command takes no options. The information below will only be displayed if OSPF is enabled.

Syntax show ip ospf database

Mode Privileged Exec and User Exec

Report Fields Router ID—Is a 32 bit dotted decimal number representing the LSDB interface.

Area ID—Is the IP address identifying the router ID.

LSA Type—The types are: router, network, ipnet sum, asbr sum, as external, group member, tmp 1, tmp 2, opaque link, opaque area.

LS ID—Is a number that “uniquely identifies an LSA that a router originates from all other self originated LSA's of the same LS type.”

Age—Is a number representing the age of the link state advertisement in seconds.

Sequence—Is a number that represents which LSA is more recent.

Checksum—Is to total number LSA checksum.

Options—This is an integer. It indicates that the LSA receives special handling during routing calculations.

show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Syntax show ip ospf interface *unit/slot/port*

Mode Privileged Exec and User Exec

Figure 23-135. Example of Output from the show ip ospf interface Command on an S50V

```

S50V-1#show ip ospf interface 1/0/24

IP Address..... 10.168.3.2
Subnet Mask..... 255.255.255.0
OSPF Admin Mode..... Enable
OSPF Area ID..... 0.0.0.0
Router Priority..... 1
Retransmit Interval..... 5
Hello Interval..... 10
Dead Interval..... 40
LSA Ack Interval..... 1
Iftransit Delay Interval..... 1
Authentication Type..... None
Metric Cost..... 1 (computed)
OSPF Mtu-ignore..... Disable
OSPF Interface Type..... broadcast
State..... designated-router
Designated Router..... 10.168.3.2
Backup Designated Router..... 10.168.2.1
Number of Link Events..... 2

```

Report Fields IP Address—Represents the IP address for the specified interface. This is a configured value.

Subnet Mask—Is a mask of the network and host portion of the IP address for the OSPF interface. This value was configured into the unit. This is a configured value.

OSPF Admin Mode—States whether OSPF is enabled or disabled on a router interface. This is a configured value.

OSPF Area ID—Represents the OSPF Area Id for the specified interface. This is a configured value.

Router Priority—A number representing the OSPF Priority for the specified interface. This is a configured value.

Retransmit Interval—A number representing the OSPF Retransmit Interval for the specified interface. This is a configured value.

Hello Interval—A number representing the OSPF Hello Interval for the specified interface. This is a configured value.

Dead Interval—A number representing the OSPF Dead Interval for the specified interface. This is a configured value.

LSA Ack Interval—A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

Transit Delay Interval—A number representing the OSPF Transit Delay for the specified interface. This is a configured value.

Authentication Type—The OSPF Authentication Type for the specified interface are: none, simple, and encrypt. This is a configured value.

The information below will only be displayed if OSPF is enabled.

OSPF Interface Type—Broadcast LANs, such as Ethernet and IEEE 802.5, take the value 'broadcast'. The OSPF Interface Type will be 'broadcast'.

State—The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.

Designated Router—Is the router ID representing the designated router.

Backup Designated Router—Is the router ID representing the backup designated router.

Number of Link Event—The number of link events.

Metric Cost—Is the cost of the ospf interface. This is a configured value.

show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables. This command takes no options.

Syntax show ip ospf interface brief

Mode Privileged Exec and User Exec

Report Fields Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

OSPF Admin Mode—States whether OSPF is enabled or disabled on a router interface. This is a configured value.

OSPF Area ID—Represents the OSPF Area Id for the specified interface. This is a configured value.

Router Priority—A number representing the OSPF Priority for the specified interface. This is a configured value.

Hello Interval—A number representing the OSPF Hello Interval for the specified interface. This is a configured value.

Dead Interval—A number representing the OSPF Dead Interval for the specified interface. This is a configured value.

Retransmit Interval—A number representing the OSPF Retransmit Interval for the specified interface. This is a configured value.

Transit Delay Interval—A number representing the OSPF Transit Delay for the specified interface. This is a configured value.

LSA Ack Interval—A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

Syntax	show ip ospf interface stats <i>unit/slot/port</i>
Mode	Privileged Exec and User Exec
Report Fields	<p>OSPF Area ID—The area ID of this OSPF interface.</p> <p>Spf Runs—The number of times that the intra-area route table has been calculated using this area's link-state database.</p> <p>Area Border Router Count—The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.</p> <p>AS Border Router Count—The total number of Autonomous System border routers reachable within this area.</p> <p>Area LSA Count—The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.</p> <p>IP Address—The IP address associated with this OSPF interface.</p> <p>OSPF Interface Events—The number of times the specified OSPF interface has changed its state, or an error has occurred.</p> <p>Virtual Events—The number of state changes or errors that occurred on this virtual link.</p> <p>Neighbor Events—The number of times this neighbor relationship has changed state, or an error has occurred.</p> <p>External LSA Count—The number of external (LS type 5) link-state advertisements in the link-state database.</p> <p>LSAs Received—The number of LSAs received.</p> <p>Originate New LSAs—The number of LSAs originated.</p>

show ip ospf neighbor

This command displays the OSPF neighbor table list.

Syntax show ip ospf neighbor [interface *unit/slot/port* [0-7]] [*ip-addr* [0-7]]

When no options are specified, this command displays the OSPF neighbor table list.

When a particular port is identified by interface *unit/slot/port*, detailed information about its neighbor is given, but only if OSPF is enabled and the interface has a neighbor.

Alternatively, if the optional *ip-addr* is used, for a neighbor's Router ID, detailed information about the neighbor displays.

For either the switch interface or the neighbor's Router ID, you can also specify a VLAN ID, represented by 0-7.

Mode Privileged Exec and User Exec

Example Figure 23-136. Example Output from the show ip ospf neighbor interface Command

```
S50V-1#show ip ospf neighbor interface 1/0/24
Router ID      Priority  IP Address    Interface    State        Dead Time
-----
192.168.2.1    1        192.168.3.1   1/0/24      Full/BACKUP-DR 31
```

Report Fields

If you do not specify an IP address, a table with the following columns displays for all neighbors or the neighbor associated with the interface that you specify:

Interface—Valid unit, slot and port number separated by forward slashes.

Router Id—Is a 4-digit dotted-decimal number identifying neighbor router.

Options—An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Priority—Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

State—The types are:

- Down—initial state of the neighbor conversation - no recent information has been received from the neighbor.
- Attempt—no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.
- Init—an Hello packet has recently been seen from the neighbor, but bi-directional communication has not yet been established.
- 2 way—communication between the two routers is bi-directional.
- Exchange start—the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.
- Exchange—the router is describing its entire link state database by sending Database Description packets to the neighbor.
- Full—the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
- Loading—Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.

Dead Time—The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

If you specify an IP address for the neighbor router, the following fields display:

Interface—Valid unit, slot, and port number separated by forward slashes

Neighbor IP Address—The IP address of the neighbor router

Interface Index—The interface ID of the neighbor router

Area ID—The area ID of the OSPF area associated with the interface

Options—An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Router Priority—The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

Dead Timer Due—The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable

State—The state of the neighboring routers

Events—The number of times this neighbor relationship has changed state, or an error has occurred

Retransmission Queue Length—An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface

show ip ospf neighbor brief

This command displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled.

Syntax `show ip ospf neighbor [neighbor-id] [unit/slot/port | all]`

Mode Privileged Exec and User Exec

Report Fields Router ID—A 4 digit dotted decimal number representing the neighbor interface.

IP Address—An IP address representing the neighbor interface.

Neighbor Interface Index—Is a *unit/slot/port* identifying the neighbor interface index.

show ip ospf range

This command displays information about the area ranges for the specified *areaid*.

Syntax `show ip ospf range areaid`

The *areaid* identifies the OSPF area whose ranges are being displayed.

Mode Privileged Exec and User Exec

Report Fields Area ID—The area ID of the requested OSPF area

IP Address—An IP Address which represents this area range

Subnet Mask—A valid subnet mask for this area range

Lsdb Type—The type of link advertisement associated with this area range

Advertisement—The status of the advertisement. Advertisement has two possible settings: enabled or disabled.

show ip ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Syntax show ip ospf stub table

Mode Privileged Exec and User Exec

Report Fields Area ID—Is a 32-bit identifier for the created stub area.

Type of Service—Is the type of service associated with the stub metric. SFTOS only supports Normal TOS.

Metric Val—The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPF cost for a route is a function of the metric value.

Metric Type—Is the type of metric advertised as the default route.

Import Summary LSA—Controls the import of summary LSAs into stub areas.

show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The *areaid* parameter identifies the area and the *neighbor* parameter identifies the neighbor's Router ID.

Syntax show ip ospf virtual-link *areaid neighbor*

Mode Privileged Exec and User Exec

Report Fields Area ID—The area ID of the requested OSPF area.

Neighbor Router ID—The input neighbor Router ID.

Hello Interval—The configured hello interval for the OSPF virtual interface.

Dead Interval—The configured dead interval for the OSPF virtual interface.

Iftransit Delay Interval—The configured transit delay for the OSPF virtual interface.

Retransmit Interval—The configured retransmit interval for the OSPF virtual interface.

Authentication Type—The configured authentication type of the OSPF virtual interface.

State—The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.

Neighbor State—The neighbor state.

show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

Syntax show ip ospf virtual-link brief

Mode Privileged Exec and User Exec

Report Fields Area Id—Is the area ID of the requested OSPF area.

Neighbor—Is the neighbor interface of the OSPF virtual interface.

Hello Interval—Is the configured hello interval for the OSPF virtual interface.

Dead Interval—Is the configured dead interval for the OSPF virtual interface.

Retransmit Interval—Is the configured retransmit interval for the OSPF virtual interface.

Transit Delay—Is the configured transit delay for the OSPF virtual interface.

trapflags

This command enables and disables OSPF traps.

Syntax [no] trapflags

The no trapflags command disables OSPF traps.

Default enabled

Mode Router OSPF Config

Usage Information Use this command in conjunction with other SNMP management commands, described in [SNMP Management Commands on page 77](#).

RIP Commands

This chapter provides a detailed explanation of the Routing Information Protocol (RIP) commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

This chapter provides details on the following commands:

- [auto-summary on page 449](#)
- [default-information originate \(RIP\) on page 450](#)
- [default-metric \(RIP\) on page 450](#)
- [distance rip on page 450](#)
- [distribute-list out on page 450](#)
- [enable \(RIP\) on page 451](#)
- [ip rip on page 451](#)
- [ip rip authentication on page 451](#)
- [ip rip receive version on page 452](#)
- [ip rip send version on page 452](#)
- [hostroutesaccept on page 453](#)
- [split-horizon on page 453](#)
- [redistribute on page 453](#)
- [show ip rip on page 454](#)
- [show ip rip interface brief on page 455](#)
- [show ip rip interface on page 455](#)

auto-summary

This command enables the RIP auto-summarization mode.

Syntax [oe] WCe6nW,, sl

The oe version of this command disables the RIP auto-summarization mode.

Default enabled

Mode Router RIP Config

default-information originate (RIP)

This command is used to control the advertisement of default routes.

The **no** version of this command is used to control the advertisement of default routes.

Syntax [no] default-information originate

Mode Router RIP Config

default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

The **no** version of this command is used to reset the default metric of distributed routes to its default value.

Syntax default-metric <0-15>

no default-metric

Mode Router RIP Config

distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route.

The **no** version of this command sets the default route preference value of RIP in the router.

Syntax distance rip <0-255>

no distance rip

Default 15

Mode Router RIP Config

distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

The **no** version of this command is used to specify the access list to filter routes received from the source protocol.

Syntax [no] distribute-list <1-199> out {ospf | static | connected}

Default 0
Mode Router RIP Config

enable (RIP)

This command resets the default administrative mode of RIP in the router (active).

The `no` version of this command sets the administrative mode of RIP in the router to inactive.

Syntax [no] enable
Default enabled
Mode Router RIP Config

ip rip

This command enables RIP on a router interface.

The `no` version of this command disables RIP on a router interface.

Syntax [no] ip rip
Default disabled
Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.3	Added Interface Range and Interface VLAN modes.
	<hr/>	
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip rip authentication

This command sets the RIP Version 2 authentication type and key for the specified interface or VLAN.

Syntax ip rip authentication {none | simple *key* | encrypt *key keyid*}

The type is either none, simple, or encrypt.

The value for the authentication *key* must be 16 bytes or less. The *key* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the type is encrypt, a *keyid* in the range of 0 and 255 must be specified to be used for MD5 encryption.

The `no ip rip authentication` command sets the default RIP Version 2 Authentication Type.

Default	The default authentication type is none.	
Default	The default password key is an empty string. Unauthenticated interfaces do not need an authentication key.	
Default	The default <i>keyid</i> is not defined. Unauthenticated interfaces do not need an authentication key ID.	
Mode	Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Added Interface Range and Interface VLAN modes.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip rip receive version

This command configures the interface to allow RIP control packets of the specified version(s) to be received.

Syntax ip rip receive version {1 | 2 | both | none}

The mode is either **1** to receive only RIP version 1 formatted packets, **2** for RIP version 2, **both** to receive packets from either format, or **none** to not allow any RIP control packets to be received.

To revert to the default of allowing RIP control packets of both version(s) to be received, use the **no ip rip receive version** command.

Default both

Mode Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History	Version 2.3	Added Interface Range and Interface VLAN modes.
		Modified: Replaced rip1 rip2 keywords with 1 2 .
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip rip send version

This command configures the interface to allow RIP control packets of the specified version to be sent.

The mode is either **1** to broadcast RIP version 1 formatted packets, **rip1c** (RIP version 1 compatibility mode) to send RIP version 2 formatted packets using broadcast, **2** to send RIP version 2 using multicast, or **none** to not allow any RIP control packets to be sent.

Syntax	ip rip send version {1 rip1c 2 none}	
	To revert to the default of sending RIP version 2 using multicast, use the no ip rip send version command.	
Default	2	
Mode	Interface Config; Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	<hr/> Version 2.3 Added Interface Range and Interface VLAN modes. Modified: Replaced rip1 rip2 keywords with 1 2. <hr/>	
Related Commands	<hr/> interface range Defines an interface range and accesses the Interface Range mode <hr/> interface vlan Creates a VLAN or selects an existing one and enters the Interface VLAN mode. <hr/>	

hostroutesaccept

This command enables the RIP hostroutesaccept mode.

The no version of this command disables the RIP hostroutesaccept mode.

Syntax	[no] hostroutesaccept
Default	enabled
Mode	Router RIP Config

split-horizon

This command sets the RIP split horizon mode.

The no version of this command sets the default RIP split horizon mode.

Syntax	[no] split-horizon {none simple poison}
Default	simple
Mode	Router RIP Config

redistribute

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match <match-type> the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

The no version of this command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Syntax for OSPF as source protocol	redistribute ospf [metric <0-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]] no redistribute {ospf static connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]
Syntax for other source protocol	redistribute {static connected} [metric <0-15>]
Default	metric—not-configured; match—internal
Mode	Router RIP Config

show ip rip

This command displays information relevant to the RIP router.

The **no** version of this command

Syntax show ip rip

Mode Privileged Exec and User Exec

RIP Admin Mode—Select enable or disable from the pulldown menu. If you select enable RIP will be enabled for the switch. The default is disable.

Split Horizon Mode—Select none, simple or poison reverse from the pulldown menu. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None - no special processing for this case. Simple - a route will not be included in updates sent to the router from which it was learned. Poisoned reverse - a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity. The default is simple

Auto Summary Mode—Select enable or disable from the pulldown menu. If you select enable groups of adjacent routes will be summarized into single entries, in order to reduce the total number of entries The default is enable.

Host Routes Accept Mode—Select enable or disable from the pulldown menu. If you select enable the router will be accept host routes. The default is enable.

Global Route Changes—The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.

Global queries—The number of responses sent to RIP queries from other systems.**Default Metric**

Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 15)

Default Metric—Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 15)

Default Route Advertise—The default route.

show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

Syntax show ip rip interface brief

Mode Privileged Exec and User Exec

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

IP Address—The IP source address used by the specified RIP interface.

Send Version—The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2.

Receive Version—The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both

RIP Mode—RIP administrative mode of router RIP operation; enable activates, disable de-activates it.

Link State—The mode of the interface (up or down).

show ip rip interface

This command displays information related to a particular RIP interface.

Syntax show ip rip interface *<unit/slot/port>*

Mode Privileged Exec and User Exec

Interface—Valid unit, slot and port number separated by forward slashes. This is a configured value.

IP Address—The IP source address used by the specified RIP interface. This is a configured value.

Send version—The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.

Receive version—The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.

Both RIP Admin Mode—RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.

Link State—Indicates whether the RIP interface is up or down. This is a configured value.

Authentication Type—The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.

Default Metric—A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value.

The following information will be invalid if the link state is down.

Bad Packets Received—The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.

Bad Routes Received—The number of routes contained in valid RIP packets that were ignored for any reason.

Updates Sent—The number of triggered RIP updates actually sent on this interface.

IP Multicast Commands

This chapter provides a detailed explanation of the IP Multicast commands that are available in the SFTOS Layer 3 software IP Multicast module. The chapter contains three sections:

- [Basic IP Multicast Commands on page 457](#)
- [Distance Vector Multicast Routing Protocol \(DVMRP\) on page 465](#)
- [IGMP Commands on page 471](#)

Basic IP Multicast Commands

This section contains the following commands:

- [ip mcast boundary on page 458](#)
- [ip multicast on page 458](#)
- [ip multicast staticroute on page 458](#)
- [ip multicast ttl-threshold on page 459](#)
- [disable ip multicast mdebug mtrace on page 459](#)
- [mrinfo on page 460](#)
- [mstat on page 460](#)
- [mtrace on page 460](#)
- [no ip mcast mroute on page 461](#)
- [show ip mcast on page 461](#)
- [show ip mcast boundary on page 462](#)
- [show ip mcast interface on page 462](#)
- [show ip mcast mroute on page 462](#)
- [show ip mcast mroute group on page 463](#)
- [show ip mcast mroute source on page 463](#)
- [show ip mcast mroute static on page 464](#)
- [show mrinfo on page 464](#)
- [show mstat on page 465](#)
- [show mtrace on page 465](#)

ip mcast boundary

This command adds an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable.

Syntax `groupipaddr mask`

groupipaddr is a group IP address and *mask* is a group IP mask.

The `no ip mcast boundary groupipaddr mask` command deletes an administrative scope multicast boundary specified by *groupipaddr* and *mask* for which this multicast administrative boundary is applicable.

Mode Interface Config or Interface VLAN

Command History

Version 2.3	Modified. Added Interface VLAN mode.
-------------	--------------------------------------

Related Commands

interface vlan	Creates a new VLAN and assigns it an ID, and then enters the Interface VLAN mode, which provides access to VLAN configuration commands for the specified VLAN.
--------------------------------	--

ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

The `no` version of this command sets the administrative mode of the IP multicast forwarder in the router to inactive. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Default disabled

Syntax `[no] ip multicast`

Mode Global Config

ip multicast staticroute

This command creates a static route which is used to perform RPF checking in multicast packet forwarding.

Syntax `ip multicast staticroute sourceipaddr mask rpfipaddr metric unit/slot/port`

The combination of the *sourceipaddr* and the *mask* fields specify the network IP address of the multicast packet source. The *groupipaddr* is the IP address of the next hop toward the source. The *metric* is the cost of the route entry for comparison with other routes to the source network and is a value in the range of 0 and 255. The *current* incoming interface is used for RPF checking for multicast packets matching this multicast static route entry.

The `no ip multicast staticroute sourceipaddr` command deletes a static route in the static mcast table. The *sourceipaddr* is the IP address of the multicast packet source.

Default none

Mode Global Config

ip multicast ttl-threshold

This command applies the given *ttlthreshold* to a routing interface.

Syntax ip multicast ttl-threshold ttlvalue

The *ttlthreshold* is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. The value for *ttlthreshold* has range from 0 to 255.

The `no ip multicast ttl-threshold` command applies the default *ttlthreshold* to a routing interface. The *ttlthreshold* is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Default 1

Mode Interface Config

disable ip multicast mdebug mtrace

This command is used to disable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Syntax •noYdisable ip multicast mdebug mtrace

The `no` version of this command is used to enable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Default none

Mode Global Config

mrinfo

This command is used to query the neighbor information of a multicast-capable router specified by [*ipaddr*]. The default value is the IP address of the system at which the command is issued. The mrinfo command can take up to 2 minutes to complete. Only one mrinfo command may be in process at a time. The results of this command will be available in the results bufferpool which can be displayed by using **show mrinfo**.

Syntax	mrinfo [<i>ipaddr</i>]
Default	none
Mode	Privileged Exec

mstat

This command is used to find the packet rate and loss information path from a source to a receiver (unicast router id of the host running mstat). The results of this command will be available in the results bufferpool which can be displayed by using **show mstat**. If a debug command is already in progress, a message is displayed and the new request fails.

Syntax	mstat <i>source</i> [<i>group</i>] [<i>receiver</i>]
---------------	--

The *source* is the IP Address of the remote multicast-capable source. The *receiver* is the IP address of the receiver. The default value is the IP address of system at which the command is issued. The *group* is a multicast address of the group to be displayed.

Default	none
Default	The default value of <i>group</i> is 224.2.0.1
Mode	Privileged Exec

mtrace

This command is used to find the multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command will be available in the results buffer pool, which can be displayed by using **show mtrace**.

If a debug command is already in execution, a message is displayed and the new request fails.

Syntax	,Cs O <i>Sourceipaddr</i> [<i>destination</i>] [<i>group</i>]
---------------	---

The *sourceipaddr* is the IP Address of the remote multicast-capable source. The *receiver* is the IP address of the receiver. The default value is the IP address of system at which the command is issued. The *group* is the multicast address of the group to be displayed.

Default	none
----------------	------

The default value of *group* is 224.2.0.1.

Mode Privileged Exec

no ip mcast mroute

This command is used to clear entries in the mroute table. The all parameters is used to clear all entries.

Syntax no ip mcast mroute {group *groupipaddr* | source *sourceipaddr* [*groupipaddr*] | all}

The *source* parameter is used to clear the routes in the mroute table entries containing the specified *sourceipaddr* or *sourceipaddr* [*groupipaddr*] pair. The source address is the source IP address of the multicast packet. The group address is the Group Destination IP address of the multicast packet.

The *group* parameter is used to clear the routes in the mroute table entries containing the specified *groupipaddr*. The group address is the Group Destination IP address of the multicast packet.

Default none

Mode Global Config

show ip mcast

This command displays the system-wide multicast information.

Syntax show ip mcast

Mode Privileged Exec and User Exec

Report Fields Admin Mode—This field displays the administrative status of multicast. This is a configured value.

Protocol State—This field indicates the current state of the multicast protocol. Possible values are Operational or Non-Operational.

Table Max Size—This field displays the maximum number of entries allowed in the multicast table.

Number Of Packets For Which Source Not Found—This displays the number of packets for which the source is not found.

Number Of Packets For Which Group Not Found—This displays the number of packets for which the group is not found.

Protocol—This field displays the multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.

Entry Count—This field displays the number of entries in the multicast table.

Highest Entry Count—This field displays the highest entry count in the multicast table.

show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Syntax show ip mcast boundary {*unit/slot/port* | all}

Mode Privileged Exec and User Exec

Report Fields Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.
Group Ip—The group IP address
Mask—The group IP mask

show ip mcast interface

This command displays the multicast information for the specified interface.

Syntax show ip mcast interface *unit/slot/port*

Mode Privileged Exec and User Exec

Report Fields Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.
TTL—This field displays the time-to-live value for this interface.

show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Syntax show ip mcast mroute {detail | summary}

Mode Privileged Exec and User Exec

Report Fields If the “detail” parameter is specified, the following fields are displayed:

Source IP Addr—This field displays the IP address of the multicast data source.

Group IP Addr—This field displays the IP address of the destination of the multicast packet.

Expiry Time—This field displays the time of expiry of this entry in seconds.

Up Time—This field displays the time elapsed since the entry was created in seconds.

RPF Neighbor—This field displays the IP address of the RPF neighbor.

Flags—This field displays the flags associated with this entry.

If the “summary” parameter is specified, the following fields are displayed:

Source IP Addr—This field displays the IP address of the multicast data source.

Group IP Addr—This field displays the IP address of the destination of the multicast packet.

Protocol—This field displays the multicast routing protocol by which this entry was created.

Incoming Interface—This field displays the interface on which the packet for this source/group arrives.

Outgoing Interface List—This field displays the list of outgoing interfaces on which this packet is forwarded.

show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *groupipaddr*.

Syntax show ip mcast mroute group groupipaddr {detail |summary}

Mode Privileged Exec and User Exec

Report Fields Source IP Addr—This field displays the IP address of the multicast data source.

Group IP Addr—This field displays the IP address of the destination of the multicast packet.

Protocol—This field displays the multicast routing protocol by which this entry was created.

Incoming Interface—This field displays the interface on which the packet for this group arrives.

Outgoing Interface List—This field displays the list of outgoing interfaces on which this packet is forwarded.

show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given *sourceipaddr* or *sourceipaddr* [*groupipaddr*] pair.

Syntax show ip mcast mroute source sourceipaddr {summary | groupipaddr}

Mode Privileged Exec and User Exec

Report Fields If the detail parameter is specified the follow fields are displayed:

Source IP Addr—This field displays the IP address of the multicast data source.

Group IP Addr—This field displays the IP address of the destination of the multicast packet.

Expiry Time—This field displays the time of expiry of this entry in seconds.

Up Time—This field displays the time elapsed since the entry was created in seconds.

RPF Neighbor—This field displays the IP address of the RPF neighbor.

Flags—This field displays the flags associated with this entry.

If the summary parameter is specified the follow fields are displayed:

Source IP Addr—This field displays the IP address of the multicast data source.

Group IP Addr—This field displays the IP address of the destination of the multicast packet.

Protocol—This field displays the multicast routing protocol by which this entry was created.

Incoming Interface—This field displays the interface on which the packet for this source arrives.

Outgoing Interface List—This field displays the list of outgoing interfaces on which this packet is forwarded.

show ip mcast mroute static

This command displays all the static routes configured in the static mcast table if is specified or displays the static route associated with the particular *sourceipaddr*.

Syntax show ip mcast mroute static [*sourceipaddr*]

Mode Privileged Exec and User Exec

Report Fields

Source Address—This field displays the IP address of the multicast packet source.

Source Mask—This field displays the mask applied to the IP address of the multicast packet source.

RPF Address—This field displays the IP address to be used as RPF for the given source and mask.

Metric—This field displays the metric value corresponding to the source address.

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

show mrinfo

This command is used to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a *mrinfo [ipaddr]* command. The results subsequent to the completion of the latest *mrinfo* will be available in the bufferpool after a maximum duration of two minutes after the completion of the ‘show mrinfo’ command. A subsequent issue ‘mrinfo’ will overwrite the contents of the buffer pool with fresh results.

Syntax show mrinfo

Mode Privileged Exec

Report Fields

Router Interface—The IP address of this neighbor

Neighbor—The neighbor associated with the router interface

Metric—The metric value associated with this neighbor

TTL—The TTL threshold associated with this neighbor

Flags—Status of the neighbor

show mstat

This command is used to display the results of packet rate and loss information from the results buffer pool of the router, subsequent to the execution/completion of a `mstat source [group] [receiver]` command. Within two minutes of the completion of the `mstat` command, the results will be available in the buffer pool. The next issuing of `mstat` would overwrite the buffer pool with fresh results.

Syntax show mstat

Mode Privileged Exec

show mtrace

This command is used to display results of multicast trace path from the results buffer pool of the router, subsequent to the execution/completion of an `mtrace source [group] [receiver]` command. The results subsequent to the completion of the `mtrace` will be available in the buffer pool within two minutes and thereafter. A subsequent `mtrace` command would overwrite the results in the buffer pool.

Syntax show mtrace

Default none

Mode Privileged Exec and User Exec

Report Fields Hops Away From Destination—The ordering of intermediate routers between the source and the destination

Intermediate Router Address—The address of the intermediate router at the specified hop distance

Mcast Protocol In Use—The multicast routing protocol used for the out interface of the specified intermediate router.

TTL Threshold—The Time-To-Live threshold of the out interface on the specified intermediate router.

Time Elapsed Between Hops (msecs)—The time between arrival at one intermediate router to the arrival at the next.

Distance Vector Multicast Routing Protocol (DVMRP)

This section provides a detailed explanation of the DVMRP commands. The commands are divided into the following different groups:

- Show commands are used to display device settings, statistics and other information.

- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.



Note: The DVMRP feature was available in SFTOS before version 2.5.1, but the commands were not tested in either 2.5.1 or 2.5.2, so the commands in this section are not supported.

This section contains the following commands:

- [ip dvmrp \(global\) on page 466](#)
- [ip dvmrp \(interface\) on page 466](#)
- [ip dvmrp metric on page 467](#)
- [ip dvmrp trapflags on page 467](#)
- [show ip dvmrp on page 467](#)
- [show ip dvmrp interface on page 468](#)
- [show ip dvmrp neighbor on page 468](#)
- [show ip dvmrp nexthop on page 469](#)
- [show ip dvmrp prune on page 470](#)
- [show ip dvmrp route on page 470](#)

ip dvmrp (global)

This command sets administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Syntax [no] ip dvmrp

The **no** version of this command sets the administrative mode of DVMRP in the router to inactive. IGMP must be enabled before DVMRP can be enabled.

Default disabled

Mode Global Config

Command History

Version 2.5.2	Unsupported: not tested in 2.5.2
Version 2.5.1	Unsupported: not tested in 2.5.1

ip dvmrp (interface)

This command sets administrative mode of DVMRP on an interface to active.

Syntax [no] ip dvmrp

The **no** version of this command sets administrative mode of DVMRP on an interface to inactive.

Default disabled

Mode Interface Config

Command History	Version 2.5.2	Unsupported: not tested in 2.5.2
	Version 2.5.1	Unsupported: not tested in 2.5.1

ip dvmrp metric

This command configures the value used in DVMRP messages as the cost to reach this network or selected VLAN.

Syntax ip dvmrp metric *value*

The *value* field has a range of 1 to 63 for a selected interface, 1 to 31 for the selected VLAN.

The **no** version of this command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Default 1

Mode Interface Config or Interface VLAN

Command History	Version 2.5.2	Unsupported: not tested in 2.5.2
	Version 2.5.1	Unsupported: not tested in 2.5.1

ip dvmrp trapflags

This command enables the DVMRP trap mode.

The **no** version of this command disables the DVMRP trap mode.

Syntax [no] ip dvmrp trapflags

Default disabled

Mode Global Config

Command History	Version 2.5.2	Unsupported: not tested in 2.5.2
	Version 2.5.1	Unsupported: not tested in 2.5.1

Usage Information Use this command in conjunction with other SNMP management commands, described in [SNMP Management Commands on page 77](#).

show ip dvmrp

This command displays the system-wide information for DVMRP.

Syntax show ip dvmrp

Mode	Privileged Exec and User Exec
Report Fields	<p>Admin Mode—This field indicates whether DVMRP is enabled or disabled. This is a configured value.</p> <p>Version String—This field indicates the version of DVMRP being used.</p> <p>Number of Routes—This field indicates the number of routes in the DVMRP routing table.</p> <p>Reachable Routes—This field indicates the number of entries in the routing table with non-infinite metrics.</p> <p>The following fields are displayed for each interface.</p> <p>Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.</p> <p>Interface Mode—This field indicates the mode of this interface. Possible values are Enabled and Disabled.</p> <p>State—This field indicates the current state of DVMRP on this interface. Possible values are Operational or Non-Operational.</p>

show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Syntax	show ip dvmrp interface <i>unit/slot/port</i>
Mode	Privileged Exec and User Exec
Report Fields	<p>Interface Mode—This field indicates whether DVMRP is enabled or disabled on the specified interface. This is a configured value.</p> <p>Metric—This field indicates the metric of this interface. This is a configured value.</p> <p>Local Address—This is the IP Address of the interface.</p> <p>This Field is displayed only when DVMRP is operational on the interface.</p> <p>Generation ID—This is the Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.</p> <p>The following fields are displayed only if DVMRP is enabled on this interface.</p> <p>Received Bad Packets—This is the number of invalid packets received.</p> <p>Received Bad Routes—This is the number of invalid routes received.</p> <p>Sent Routes—This is the number of routes that have been sent on this interface.</p>

show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Syntax	show ip dvmrp neighbor
Mode	Privileged Exec and User Exec
Report Fields	<p>IfIndex—This field displays the value of the interface used to reach the neighbor.</p> <p>Nbr IP Addr—This field indicates the IP Address of the DVMRP neighbor for which this entry contains information.</p> <p>State—This field displays the state of the neighboring router. The possible value for this field are ACTIVE or DOWN.</p> <p>Up Time—This field indicates the time since this neighboring router was learned.</p> <p>Expiry Time—This field indicates the time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.</p> <p>Generation ID—This is the Generation ID value for the neighbor.</p> <p>Major Version—This shows the major version of DVMRP protocol of neighbor.</p> <p>Minor Version—This shows the minor version of DVMRP protocol of neighbor.</p> <p>Capabilities—This shows the capabilities of neighbor.</p> <p>Received Routes—This shows the number of routes received from the neighbor.</p> <p>Rcvd Bad Pkts—This field displays the number of invalid packets received from this neighbor.</p> <p>Rcvd Bad Routes—This field displays the number of correct packets received with invalid routes.</p>

show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Syntax	show ip dvmrp nexthop
Mode	Privileged Exec and User Exec
Report Fields	<p>Source IP—This field displays the sources for which this entry specifies a next hop on an outgoing interface.</p> <p>Source Mask—This field displays the IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.</p> <p>Next Hop Interface—This field displays the interface in <i>unit/slot/port</i> format for the outgoing interface for this next hop.</p> <p>Type—This field states whether the network is a LEAF or a BRANCH.</p>

show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Syntax show ip dvmrp prune

Mode Privileged Exec and User Exec

Report Fields Group IP—This field identifies the multicast Address that is pruned.

Source IP—This field displays the IP Address of the source that has pruned.

Source Mask—This field displays the network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.

Expiry Time (secs)—This field indicates the expiry time in seconds. This is the time remaining for this prune to age out.

show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Syntax show ip dvmrp route

Mode Privileged Exec and User Exec

Report Fields Source Address—This field displays the multicast address of the source group.

Source Mask—This field displays the IP Mask for the source group.

Upstream Neighbor—This field indicates the IP Address of the neighbor which is the source for the packets for a specified multicast address.

Interface—This field displays the interface used to receive the packets sent by the sources.

Metric—This field displays the distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.

Expiry Time(secs)—This field indicates the expiry time in seconds. This is the time remaining for this route to age out.

Up Time(secs)—This field indicates the time when a specified route was learnt, in seconds.

IGMP Commands

This section provides a detailed explanation of the Internet Group Management Protocol (IGMP) commands available in the Layer 3 package.

This section contains the following commands:

- [ip igmp \(global\) on page 471](#)
- [ip igmp last-member-query-count on page 472](#)
- [ip igmp last-member-query-interval on page 472](#)
- [ip igmp-proxy on page 473](#)
- [ip igmp query-interval on page 473](#)
- [ip igmp query-max-resp-time on page 474](#)
- [ip igmp robustness on page 474](#)
- [ip igmp startup-query-count on page 474](#)
- [ip igmp startup-query-interval on page 475](#)
- [ip igmp version on page 475](#)
- [show ip igmp on page 476](#)
- [show ip igmp groups on page 476](#)
- [show ip igmp interface on page 477](#)
- [show ip igmp interface membership on page 479](#)
- [show ip igmp interface stats on page 479](#)
- [show ip igmp-proxy on page 480](#)
- [show ip igmp-proxy interface on page 481](#)
- [show ip igmp-proxy groups on page 482](#)
- [show ip igmp-proxy groups detail on page 482](#)

See also the IGMP Snooping commands in [IGMP Snooping Commands on page 273](#).

ip igmp (global)

This command enables IGMP on the router.

Syntax ip igmp

Use `no ip igmp` to set the administrative mode of IGMP in the router to inactive.

Default disabled

Mode Global Config

ip igmp (VLAN)

This command sets the administrative mode of IGMP for the selected VLAN to active.

Syntax ip igmp

Use `no ip igmp` to set the administrative mode of IGMP for the selected VLAN to inactive.

Default	disabled
Mode	Interface VLAN
Command History	Version 2.3 Introduced

ip igmp last-member-query-count

This command sets the number of group-specific queries sent before the router assumes that there are no local members on the interface or VLAN.

The `no` version of this command resets the number of Group-Specific Queries to the default value.

Syntax `ip igmp last-member-query-count count`

`no ip igmp last-member-query-count`

The range for *count* is 1 to 20.

Mode Interface Config or Interface VLAN

Command History	Version 2.3 Modified: Added Interface VLAN mode.
------------------------	---

ip igmp last-member-query-interval

This command configures the Maximum Response Time being inserted into group-specific queries sent in response to Leave Group messages on the interface or VLAN.

The `no` version of this command resets the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface to the default value.

Syntax `ip igmp last-member-query-interval seconds`

`no ip igmp last-member-query-interval`

The range for *seconds* is 0 to 255 tenths of a second.

Default 10 tenths of a second (1 second)

Mode Interface Config or Interface VLAN

Command History	Version 2.3 Modified: Added Interface VLAN mode.
------------------------	---

ip igmp-proxy

When used without parameters, this Layer 3 command enables/disables the IGMP Proxy feature on the selected port. To enable the feature, you must also enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

IGMP Proxy is used by the IGMP router to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. These commands are valid only when you first enable IGMP Proxy on the interface. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

Syntax	[no] ip igmp-proxy [reset-status] [unsolicit-report-interval 1-260]	
Parameters	reset-status	(OPTIONAL) When used with this keyword, the command resets the host interface status parameters of the IGMP Proxy router.
	unsolicit-report-interval 1-260	(OPTIONAL) When used with this keyword, the command sets the unsolicited report interval for the IGMP Proxy router. Range: 1-260 seconds
Default		
Mode	Interface Config; Interface VLAN	
Command History	Version 2.5.1	Introduced
Related Commands	show ip igmp	Displays system-wide IGMP information.
	show ip igmp-proxy	Displays a summary of the host interface status parameters.
	show ip igmp-proxy interface	Displays a detailed list of the host interface status parameters.
	show ip igmp-proxy groups detail	Displays complete information about multicast groups that IGMP Proxy reported

ip igmp query-interval

This command configures the query interval for the specified interface or VLAN. This is the frequency at which IGMP Host-Query packets are transmitted on this interface or VLAN.

Syntax ip igmp query-interval *seconds*

no ip igmp query-interval

The range for *seconds* is 1 to 3600 seconds.

The **no** version of this command resets the query interval for the specified interface to the default value.

Default 125 seconds

Mode Interface Config; Interface VLAN

Command History

 Version 2.3 Modified: Added Interface VLAN mode.

ip igmp query-max-resp-time

This command configures the maximum response time interval for the specified interface or VLAN, which is the maximum query response time advertised in IGMPv2 queries on this interface or VLAN.

Syntax ip igmp query-max-response-time *0-255*

Parameters	<i>0-255</i>	Specify the maximum response time interval in tenths of a second. Range: 0 to 255 tenths of a second
-------------------	--------------	---

To reset the maximum response time interval for the specified interface to the default value of 100 tenths of a second, use the `no ip igmp query-max-response-time` command.

Default 100 tenths of a second

Mode Interface Config; Interface VLAN

Command History

 Version 2.3 Modified: Changed from `ip igmp query-max-response-time` to `ip igmp query-max-resp-time` and added Interface VLAN mode.

ip igmp robustness

This command configures the robustness that allows tuning of the interface or VLAN. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the *robustness* variable may be increased for the interface or VLAN.

Syntax ip igmp robustness *robustness*

The range for *robustness* is 1 to 255.

The `no ip igmp robustness` command sets the robustness value to the default.

Default 2

Mode Interface Config; Interface VLAN

Command History

 Version 2.3 Modified: Added Interface VLAN mode.

ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface or VLAN.

Syntax ip igmp startup-query-count *count*

The range for *count* is 1 to 20.

The no ip igmp startup-query-count command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Default 2

Mode Interface Config; Interface VLAN

Command History

Version 2.3 Modified: Added Interface VLAN mode.

ip igmp startup-query-interval

This command sets the interval between general queries sent by a querier on startup on the interface or VLAN.

Syntax ip igmp startup-query-interval *interval*

The range for *interval* is 1 to 300 seconds.

The no ip igmp startup-query-interval command resets the interval between general queries sent by a querier on startup on the interface to the default value.

Default 31

Mode Interface Config; Interface VLAN

Command History

Version 2.3 Modified: Added Interface VLAN mode.

ip igmp version

This command configures the version of IGMP for an interface or VLAN.

Syntax [no] ip igmp version *version*

The value for *version* is either 1, 2 or 3 (for IGMP version 1, 2, or 3, respectively)

The no version of this command resets the version of IGMP for this interface. The version is reset to the default value.

Default 3

Mode Interface Config; Interface VLAN

Command History

Version 2.3 Modified: Added Interface VLAN mode.

show ip igmp

This command displays the system-wide IGMP information.

Syntax show ip igmp

Mode Privileged Exec and User Exec

Example **Figure 25-137. Example of show ip igmp Command Output**

```
Forcel0 #show ip igmp
IGMP Admin Mode..... Enable

      IGMP INTERFACE STATUS
-----
Interface Interface Mode Protocol State
-----
1/0/1      Disable      Non-Operational
VLAN 4     Enable       Operational
```

Report Fields Admin Mode — This field displays the administrative status of IGMP. This is a configured value. If this field lists “Disable”, then the interface-specific fields are empty.

Interface — (Unit/Slot/Port) Valid unit, slot and port number separated by forward slashes.

Interface Mode — This field indicates whether IGMP is enabled or disabled on the interface listed on the left. This is a configured value.

Protocol State — This field indicates the current state of IGMP on this interface. Possible values are Operational or Non-Operational. For Operational to be displayed:

- The **ip igmp** command must be configured globally and at the interface.
- IP routing must be enabled globally and at the interface level.
- If IP IGMP is enabled on a VLAN interface, then at least one of the member ports of that VLAN must be active.

Related Commands

ip igmp (global)	Sets the administrative mode of IGMP in the router to active.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

show ip igmp groups

This command displays the registered multicast groups on the interface. If “detail” is specified this command displays the registered multicast groups on the interface in detail.

Syntax show ip igmp groups {*unit/slot/port* [detail] | 1-3965 [detail]}

Designate either a port (*unit/slot/port*) or VLAN number (1-3965), and then, optionally, enter detail.

Mode Privileged Exec and User Exec

Report Fields If **detail** is not specified for a specified interface, the following fields are displayed:

IP Address—This displays the IP address of the interface participating in the multicast group.

Subnet Mask—This displays the subnet mask of the interface participating in the multicast group.

Interface Mode—This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled.

Querier Status—This displays whether the interface has IGMP in querier mode or non-querier mode.

Groups—This displays the list of multicast groups that are registered on this interface.

If **detail** is specified, the following fields are displayed:

Multicast IP Address—This displays the IP Address of the registered multicast group on this interface.

Last Reporter—This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.

Up Time—This displays the time elapsed since the entry was created for the specified multicast group address on this interface.

Expiry Time—This displays the amount of time remaining to remove this entry before it is aged out.

Version1 Host Timer—This displays the time remaining until the local router will assume that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface.

**Related
Commands**

ip igmp (global)	Sets the administrative mode of IGMP in the router to active.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

show ip igmp interface

This command displays the IGMP information for the specified interface.

Syntax show ip igmp interface { *unit/slot/port* | vlan 1-3965 }

Designate a port number or a VLAN number.

Mode Privileged Exec and User Exec

Example Figure 25-138. Example of show ip igmp interface Command Output

```

Forcel0 #show ip igmp interface 1/0/1

Slot/Port..... 1/0/1
IGMP Admin Mode..... Enable
Interface Mode..... Enable
IGMP Version..... 3
Query Interval (secs)..... 125
Query Max Response Time (1/10 of a second).... 100
Robustness..... 2
Startup Query Interval (secs) ..... 31
Startup Query Count..... 2
Last Member Query Interval (1/10 of a second).. 10
Last Member Query Count..... 2

Forcel0#

```

Report Fields

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

IGMP Admin Mode—This field displays the administrative status of IGMP. This is a configured value.

Interface Mode—This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.

IGMP Version—This field indicates the version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.

Query Interval—This field indicates the frequency at which IGMP Host-Query packets are transmitted on this interface. This is a configured value.

Query Max Response Time—This field indicates the maximum query response time advertised in IGMPv2 queries on this interface. This is a configured value.

Robustness—This field displays the tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface. This is a configured value.

Startup Query Interval—This value indicates the interval between general queries sent by a querier on startup. This is a configured value.

Startup Query Count—This value is the number of Queries sent out on startup, separated by the Startup Query Interval. This is a configured value.

Last Member Query Interval—This value indicates the Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This is a configured value.

Last Member Query Count—This value is the number of Group-Specific Queries sent before the router assumes that there are no local members. This is a configured value.

Related Commands

ip igmp (global)	Set the administrative mode of IGMP in the router to active.
ip igmp version	Set the version of IGMP for an interface or VLAN.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

show ip igmp interface membership

This command displays the list of interfaces that have registered in the specified multicast group.

- Syntax** show ip igmp interface membership *multiipaddr* [*detail*]
- Mode** Privileged Exec
- Report Fields** Interface—Valid unit, slot and port number separated by forward slashes.
- Interface IP—This displays the IP address of the interface participating in the multicast group.
- State—This displays whether the interface has IGMP in querier mode or non-querier mode.
- Group Compatibility Mode—The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
- Source Filter Mode—The source filter mode (Include/Exclude) for the specified group on this interface. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.
- If **detail** is specified, the following fields are displayed:
- Interface—Valid unit, slot and port number separated by forward slashes.
- Group Compatibility Mode—The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
- Source Filter Mode—The source filter mode (Include/Exclude) for the specified group on this interface. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.
- Source Hosts—This displays the list of unicast source IP Addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP Address. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.
- Expiry Time—This displays the amount of time remaining to remove this entry before it is aged out. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.

Related Commands

ip igmp (global)	Sets the administrative mode of IGMP in the router to active.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

show ip igmp interface stats

This command displays the IGMP statistical information for the given interface. The statistics are only displayed when the interface is enabled for IGMP.

- Syntax** show ip igmp interface stats *unit/slot/port*
- Mode** Privileged Exec and User Exec

Report Fields	<p>Querier Status—This field indicates the status of the IGMP router, whether it is running in querier mode or non-querier mode.</p> <p>Querier IP Address—This field displays the IP Address of the IGMP querier on the IP subnet to which this interface is attached.</p> <p>Querier Up Time—This field indicates the time since the interface querier was last changed.</p> <p>Querier Expiry Time—This field displays the amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.</p> <p>Wrong Version Queries—This field indicates the number of queries received whose IGMP version does not match the IGMP version of the interface.</p> <p>Number of Joins—This field displays the number of times a group membership has been added on this interface.</p> <p>Number of Groups—This field indicates the current number of membership entries for this interface.</p>
----------------------	---

Related Commands

ip igmp (global)	Sets the administrative mode of IGMP in the router to active.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

show ip igmp-proxy

If you first you enable IGMP Proxy, this command displays a summary of the host interface status parameters.

Syntax show ip igmp-proxy

Mode Privileged Exec and User Exec

Command History

Version 2.5.1	Introduced
---------------	------------

Report Fields	<p>Interface index — The interface number of the IGMP Proxy.</p> <p>Admin Mode — Displays the IGMP administrative status (enabled/disabled). This is a configured value. If this field lists “Disable”, then the interface-specific fields are empty.</p> <p>Operational Mode — States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.</p> <p>Version — The present IGMP host version that is operational on the proxy interface.</p> <p>Number of Multicast Groups — States the number of multicast groups that are associated with the IGMP Proxy interface.</p> <p>Unsolicited Report Interval — The time interval at which the IGMP Proxy interface sends unsolicited group membership report.</p>
----------------------	--

Querier IP Address on Proxy Interface — The IP address of the querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).

Older Version 1 Querier Timeout — The interval used to time out the older version 1 queriers.

Older Version 2 Querier Timeout — The interval used to time out the older version 2 queriers.

Proxy Start Frequency — The number of times the IGMP Proxy has been stopped and started.

**Related
Commands**

ip igmp (global)	Sets the administrative mode of IGMP in the router to active.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

show ip igmp-proxy interface

If you first you enable IGMP Proxy, this command displays a detailed list of the host interface status parameters.

Syntax show ip igmp-proxy interface

Mode Privileged Exec and User Exec

**Command
History**

Version 2.5.1	Introduced
---------------	------------

Report Fields Interface index — The unit/slot/port of the IGMP proxy

The column headings of the table associated with the interface are as follows:

Ver — IGMP version

Query Rcvd — Number of IGMP queries received

Report Rcvd — Number of IGMP reports received

Report Sent — Number of IGMP reports sent

Leaves Rcvd — Number of IGMP leaves received

Leaves Sent — Number of IGMP leaves sent

**Related
Commands**

ip igmp (global)	Sets the administrative mode of IGMP in the router to active.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

show ip igmp-proxy groups

This command displays information about the subscribed multicast groups that IGMP Proxy reported.

Syntax	show ip igmp-proxy groups						
Mode	Privileged Exec and User Exec						
Command History	<table border="1"> <tr> <td>Version 2.5.1</td> <td>Introduced</td> </tr> </table>	Version 2.5.1	Introduced				
Version 2.5.1	Introduced						
Report Fields	<p>Interface index — The interface number of the IGMP Proxy</p> <p>Group Address — The IP address of the multicast group</p> <p>Last Reporter — The IP address of host that last sent a membership report</p> <p>Up Time (in secs) — The time elapsed since last created</p> <p>Member State — The status of the entry. Possible values are:</p> <p>IDLE_MEMBER — The interface has responded to the latest group membership query for this group.</p> <p>DELAY_MEMBER — The interface is going to send a group membership report to respond to a group membership query for this group.</p> <p>Filter Mode — The possible values are Include or Exclude.</p> <p>Sources — The number of sources attached to the multicast group</p>						
Related Commands	<table border="1"> <tr> <td>ip igmp (global)</td> <td>Sets the administrative mode of IGMP in the router to active.</td> </tr> <tr> <td>ip igmp (VLAN)</td> <td>Sets the administrative mode of IGMP for the selected VLAN to active</td> </tr> <tr> <td>ip igmp-proxy</td> <td>When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval, this command sets the unsolicited report interval for the IGMP Proxy router.</td> </tr> </table>	ip igmp (global)	Sets the administrative mode of IGMP in the router to active.	ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active	ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.
ip igmp (global)	Sets the administrative mode of IGMP in the router to active.						
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active						
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.						

show ip igmp-proxy groups detail

This command displays complete information about multicast groups that IGMP Proxy reported.

Syntax	show ip igmp-proxy groups detail		
Mode	Privileged Exec and User Exec		
Command History	<table border="1"> <tr> <td>Version 2.5.1</td> <td>Introduced</td> </tr> </table>	Version 2.5.1	Introduced
Version 2.5.1	Introduced		
Report Fields	Interface index — The interface number of the IGMP Proxy		

Group Address — The IP address of the multicast group

Last Reporter — The IP address of host that last sent a membership report for the current group, on the network attached to the IGMP-Proxy interface (upstream interface)

Up Time (in secs) — The time elapsed since last created

Member State — The status of the entry. Possible values are:

IDLE_MEMBER — The interface has responded to the latest group membership query for this group.

DELAY_MEMBER — The interface is going to send a group membership report to respond to a group membership query for this group.

Filter Mode — The possible values are Include or Exclude.

Sources — The number of sources attached to the multicast group

Group Source List — The list of IP addresses of the sources attached to the multicast group

Expiry Time — Time left before a source is deleted

**Related
Commands**

ip igmp (global)	Sets the administrative mode of IGMP in the router to active.
ip igmp (VLAN)	Sets the administrative mode of IGMP for the selected VLAN to active
ip igmp-proxy	When used without parameters, this command enables/disables the IGMP Proxy on the router. When used with the reset-status keyword, this command resets the host interface status parameters of the IGMP Proxy router. When used with unsolicit-report-interval , this command sets the unsolicited report interval for the IGMP Proxy router.

PIM Commands

This chapter contains the following major sections:

- [PIM-DM Commands on page 485](#)
- [PIM-SM Commands on page 488](#)

PIM-DM Commands

This section provides Protocol Independent Multicast–Dense Mode (PIM-DM) command syntax. The commands are:

- [ip pimdm on page 485](#)
- [ip pimdm mode on page 486](#)
- [ip pimdm query-interval on page 486](#)
- [show ip pimdm on page 486](#)
- [show ip pimdm interface on page 487](#)
- [show ip pimdm interface stats on page 487](#)
- [show ip pimdm neighbor on page 488](#)



Note: The PIM-DM feature was available in SFTOS before version 2.5.1, but the commands were not tested in either 2.5.1 or 2.5.2, so the commands in this section are not supported.

ip pimdm

This command enables the administrative mode of PIM-DM in the router.

Syntax [oe] aduda,..

The **oe** version of this command disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

Default disabled

Mode Global Config

Command History

Version 2.5.2	Unsupported: not tested in 2.5.2
Version 2.5.1	Unsupported: not tested in 2.5.1

ip pimdm mode

This command sets administrative mode of PIM-DM on an interface to enabled.

Syntax [no] aduda,..,u,e.E *unit/slot/port*

The **no** version of this command sets administrative mode of PIM-DM on an interface to disabled.

Default disabled

Mode Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.2	Unsupported: not tested in 2.5.2
Version 2.5.1	Unsupported: not tested in 2.5.1
Version 2.3	Added Interface Range and Interface VLAN modes.

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip pimdm query-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

Syntax ip pimdm query-interval *seconds*

no ip pimdm query-interval

The **no** version of this command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Default 30

Mode Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.5.2	Unsupported: not tested in 2.5.2
Version 2.5.1	Unsupported: not tested in 2.5.1
Version 2.3	Added Interface Range and Interface VLAN modes.

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

show ip pimdm

This command displays the system-wide information for PIM-DM.

Syntax show ip pimdm

Mode Privileged Exec and User Exec

PIM-DM Admin Mode—This field indicates whether PIM-DM is enabled or disabled. This is a configured value.

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

Interface Mode—This field indicates whether PIM-DM is enabled or disabled on this interface. This is a configured value.

State—This field indicates the current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

show ip pimdm interface

This command displays the interface information for PIM-DM on the specified interface.

Syntax show ip pimdm interface *unit/slot/port*

The no version of this command

Mode Privileged Exec and User Exec

Interface Mode—This field indicates whether PIM-DM is enabled or disabled on the specified interface. This is a configured value.

PIM-DM Interface Hello Interval—This field indicates the frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

show ip pimdm interface stats

This command displays the statistical information for PIM-DM on the specified interface.

Syntax show ip pimdm interface stats {*unit/slot/port* | all}

The no version of this command

Mode Privileged Exec and User Exec

Interface—Valid unit, slot and port number separated by forward slashes.

IP Address—This field indicates the IP Address that represents the PIM-DM interface.

Nbr Count—This field displays the neighbor count for the PIM-DM interface.

Hello Interval—This field indicates the time interval between two hello messages sent from the router on the given interface.

Designated Router—This indicates the IP Address of the Designated Router for this interface.

show ip pimdm neighbor

This command displays the neighbor information for PIM-DM on the specified interface.

Syntax show ip pimdm neighbor {*unit/slot/port* | all}

The **no** version of this command

Mode Privileged Exec and User Exec

Neighbor Address—This field displays the IP Address of the neighbor on an interface.

Interface—Valid unit, slot and port number separated by forward slashes.

Up Time—This field indicates the time since this neighbor has become active on this interface.

Expiry Time—This field indicates the expiry time of the neighbor on this interface.

PIM-SM Commands

This section provides a detailed explanation of the Protocol Independent Multicast - Sparse Mode (PIM-SM) commands in SFTOS. The commands are:

- [ip pimsm cbsrpreference on page 489](#)
- [ip pimsm cbsrhashmasklength on page 489](#)
- [ip pimsm crppreference on page 490](#)
- [ip pimsm datathreshrate on page 490](#)
- [ip pimsm message-interval on page 490](#)
- [ip pimsm on page 491](#)
- [ip pimsm mode on page 491](#)
- [ip pimsm query-interval on page 492](#)
- [ip pimsm spt-threshold on page 492](#)
- [ip pim-trapflags on page 492](#)
- [ip pimsm staticrp on page 493](#)
- [show ip pimsm rphash on page 493](#)
- [show ip pimsm staticrp on page 493](#)
- [show ip pimsm on page 493](#)
- [show ip pimsm candrptable on page 494](#)
- [show ip pimsm componenttable on page 494](#)
- [show ip pimsm interface on page 495](#)
- [show ip pimsm interface stats on page 495](#)
- [show ip pimsm neighbor on page 496](#)
- [show ip pimsm rp on page 497](#)
- [show ip pimsm rphash on page 497](#)

ip pimsm cbsrpreference

This command is used to configure the CBSR preference for a particular PIM-SM interface. The range of CBSR preference is -1 to 255.

Syntax ip pimsm cbsrpreference 1-255

no ip pimsm cbsrpreference

The **no** version of this command is used to reset the CBSR preference for a particular PIM-SM interface to the default value.

Default 0

Mode Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip pimsm cbsrhashmasklength

This command is used to configure the CBSR hash mask length to be advertised in bootstrap messages for a particular PIM-SM interface. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid range is 0 - 32. The default value is 30.

Syntax ip pimsm cbsrhashmasklength 0-32

no ip pimsm cbsrhashmasklength

The **no** version of this command is used to reset the CBSR hash mask length for a particular PIM-SM interface to the default value.

Default 30

Mode Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip pimsm crppreference

This command is used to configure the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface. The valid values are from (1 to 255), and the value of -1 is used to indicate that the local interface is not a Candidate RP interface.

The active router interface, with the highest IP Address and crppreference greater than -1, is chosen as the CRP for the router. The default value is 0.

In the CRP advertisements sent to the bootstrap router (BSR), the router interface advertises itself as the CRP for the group range 224.0.0.0 mask 240.0.0.0.

Syntax ip pimsm crppreference *-1-255*

no ip pimsm crppreference

The **no** version of this command is used to reset the Candidate Rendezvous Point (CRP) for a particular PIM-SM interface to the default value.

Default 0

Mode Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip pimsm datathreshrate

This command is used to configure the data Threshold rate for the PIM-SM router. The rate is specified in Kilobytes per second. The possible values are 0 to 2000.

Syntax ip pimsm datathreshrate *0-2000*

no ip pimsm datathreshrate

The **no** version of this command is used to reset the data Threshold rate for the PIM-SM router to the default value.

Default 50

Mode Global Config

ip pimsm message-interval

This command is used to configure the global join/prune interval for PIM-SM router.

Syntax ip pimsm message-interval *10-3600*

The join/prune interval is specified in seconds. This parameter can be configured to a value from 10 to 3600.

The `no ip pimsm message-interval` command resets the global join/prune interval for PIM-SM router to the default value.

Default 60

Mode Global Config

ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to enabled. IGMP must be enabled before PIM-SM can be enabled.

Syntax [no] ip pimsm

The `no` version of this command sets administrative mode of PIM-SM multicast routing across the router to disabled. IGMP must be enabled before PIM-SM can be enabled.

Default disabled

Mode Global Config

ip pimsm mode

This command sets administrative mode of PIM-SM multicast routing on a routing interface to enabled.

Syntax [no] ip pimsm mode

The `no` version of this command sets administrative mode of PIM-SM multicast routing on a routing interface to disabled.

Default disabled

Mode Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.

Command History

Version 2.3	Added Interface Range and Interface VLAN modes.
-------------	---

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip pimsm query-interval

This command configures the transmission frequency of hello messages in seconds between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

Syntax	ip pimsm query-interval <i>10-3600</i>	
	The no ip pimsm query-interval command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.	
Default	30	
Mode	Interface Config or Interface VLAN; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Added Interface Range and Interface VLAN modes.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	interface vlan	Creates a VLAN or selects an existing one and enters the Interface VLAN mode.

ip pimsm spt-threshold

This command is used to configure the Threshold rate for the RP router to switch to the shortest path. The rate is specified in Kilobytes per second. The possible values are 0 to 2000.

Syntax	ip pimsm spt-threshold <i>0-2000</i>	
	The no ip pimsm spt-threshold command is used to reset the Threshold rate for the RP router to switch to the shortest path to the default value.	
Default	50	
Mode	Global Config	

ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Syntax	[no] ip pim-trapflags	
	The no version of this command disables the PIM trap mode.	
Default	disabled	
Mode	Global Config	
Usage Information	Use this command in conjunction with other SNMP management commands, described in SNMP Management Commands on page 77 .	

ip pimsm staticrp

This command is used to create the RP IP address for the PIM-SM router.

Syntax [no] ip pimsm staticrp *ipaddress groupaddress groupmask*

The *ipaddress* is the IP address of the RP. The *groupaddress* is the group address supported by the RP. The *groupmask* is the group mask (regular form) for the group address.

The **no** version of this command is used to delete the RP IP address for the PIM-SM router.

Default disabled

Mode Global Config

show ip pimsm rphash

This command displays the RP router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

Syntax show ip pimsm rphash *groupaddress*

Mode Privileged Exec and User Exec

RP IP Address—This field displays the IP address of the RP.

Group Mask—This field displays the group mask for the group address.

show ip pimsm staticrp

This command displays the static RP information for the PIM-SM router.

Syntax show ip pimsm staticrp

Mode Privileged Exec and User Exec

RP IP Address—This field displays the IP address of the RP.

Group Address—This field displays the group address supported by the RP.

Group Mask—This field displays the group mask for the group address.

show ip pimsm

This command displays the system-wide information for PIM-SM.

Syntax show ip pimsm

The **no** version of this command

Mode Privileged Exec and User Exec

PIM-SM Admin Mode—This field indicates whether PIM-SM is enabled or disabled. This is a configured value.

Join/Prune Interval (secs)—This field shows the interval at which periodic PIM-SM Join/Prune messages are to be sent. This is a configured value.

Data Threshold Rate (K bits/sec)—This field shows the data threshold rate for the PIM-SM router. This is a configured value.

Register Threshold Rate (K bits/sec)—This field indicates the threshold rate for the RP router to switch to the shortest path. This is a configured value.

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

Interface Mode—This field indicates whether PIM-SM is enabled or disabled on the interface. This is a configured value.

Protocol State—This field indicates the current state of the PIM-SM protocol on the interface. Possible values are Operational or Non-Operational.

show ip pimsm candrptable

This command displays the IP multicast groups for which the local router is to advertise itself as a Candidate-RP when the value of hold time is non-zero.

Syntax show ip pimsm candrptable

Mode Privileged Exec and User Exec

Group Address—This field specifies the IP multicast group address.

Group Mask—This field specifies the multicast group address subnet mask.

Address—This field specifies the unicast address of the interface that will be advertised as a Candidate-RP.

show ip pimsm componenttable

This command displays the table containing objects specific to a PIM domain. One row exists for each domain to which the router is connected.

Syntax show ip pimsm componenttable

Mode Privileged Exec and User Exec

Component Index—This field displays a number which uniquely identifies the component.

Component BSR Address—This field displays the IP address of the bootstrap router (BSR) for the local PIM region.

Component BSR Expiry Time—This field displays the minimum time remaining before the BSR in the local domain will be declared down.

Component CRP Hold Time—This field displays the hold time of the component when it is a candidate.

show ip pimsm interface

This command displays the interface information for PIM-SM on the specified interface.

Syntax show ip pimsm interface *unit/slot/port*

Mode Privileged Exec and User Exec

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

IP Address—This field indicates the IP address of the specified interface.

Subnet Mask—This field indicates the Subnet Mask for the IP address of the PIM interface.

Mode—This field indicates whether PIM-SM is enabled or disabled on the specified interface. This is a configured value. By default it is disabled.

Hello Interval—This field indicates the frequency at which PIM hello messages are transmitted on this interface. This is a configured value. By default, the value is 30 seconds.

CBSR Preference—This field shows the preference value for the local interface as a candidate bootstrap router. This is a configured value.

CRP Preference—This field shows the preference value as a candidate rendezvous point on this interface.

CBSR Hash Mask Length—This field shows the hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. The value is used in the hash algorithm for selecting the RP for a particular group.

show ip pimsm interface stats

This command displays the statistical information for PIM-SM on the specified interface.

Syntax show ip pimsm interface stats {*unit/slot/port* | all}

The no version of this command

Mode Privileged Exec and User Exec

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

IP Address—This field indicates the IP Address that represents the PIM-SM interface.

Subnet Mask—This field indicates the Subnet Mask of this PIM-SM interface.

Designated Router—This indicates the IP Address of the Designated Router for this interface.

Neighbor Count—This field displays the number of neighbors on the PIM-SM interface.

show ip pimsm neighbor

This command displays the neighbor information for PIM-SM on the specified interface.

Syntax show ip pimsm neighbor {*unit/slot/port* | all}

Mode Privileged Exec and User Exec

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

IP Address—This field displays the IP Address of the neighbor on an interface.

Up Time—This field indicates the time since this neighbor has become active on this interface.

Expiry Time—This field indicates the expiry time of the neighbor on this interface.

show ip pimsm rp

This command displays the PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for the specific *groupaddress groupmask* provided in the command. The information in the table is displayed for each IP multicast group.

Syntax show ip pimsm rp {*groupaddress groupmask* | candidate | all}

Mode Privileged Exec and User Exec

Group Address—This field specifies the IP multicast group address.

Group Mask—This field specifies the multicast group address subnet mask.

Address—This field displays the IP address of the Candidate-RP.

Hold Time—This field displays the hold time of a Candidate-RP.

Expiry Time—This field displays the minimum time remaining before the Candidate-RP will be declared down.

Component—This field displays a number which uniquely identifies the component. Each protocol instance connected to a separate domain should have a different index value.

show ip pimsm rphash

This command displays the RP router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

Syntax show ip pimsm rphash *groupaddress*

Mode Privileged Exec and User Exec

RP IP Address—This field displays the IP address of the RP.

Group Mask—This field displays the group mask for the group address.

Index

Symbols

{deny|permit} 384

Numerics

1583compatibility 424

802.1p 327, 328, 332

802.1p priority 328

A

ABR (OSPF Area Border Router) 425

Access Control Lists (ACLs) 379

accessing DHCP Pool Config mode 237

access-list 379

ACL Commands 379

ACL wildcard masks 379

active image 119

addport 288

Address Aging Timeout 98

archive copy-sw 217

archive download-sw 218

area authentication 425

area default-cost 425

area nssa 425

area nssa default-info-originate 425

area nssa no-redistribute (OSPF) 425

area nssa no-summary (OSPF) 426

area nssa translator-role (OSPF) 426

area nssa translator-stab-intv 426

area range 426

area stub 427

area stub summarylsa 427

area virtual-link 427

area virtual-link authentication 427

area virtual-link dead-interval 428

area virtual-link hello-interval 428

area virtual-link retransmit-interval 429

area virtual-link transmit-delay 429

areaid 25

ARP

aging 232, 233, 234, 235, 238, 239, 240, 241, 393

cache, displaying 394, 395

response time 393

retries 393

arp 392

arp cachesize 392

arp dynamicrenew 392

arp purge 392

arp resptime 393

arp retries 393

arp timeout 393

assign-queue 346

audience 10

authentication

OSPF MD5 433

OSPF simple 433

authentication login 188

Authentication traps 83

auto-negotiate 88

auto-negotiate all 89

auto-summary 449

B

Backspace 26

backup image 108

bandwidth division 327

bandwidth kbps 347

bandwidth percent 347

b-node (Broadcast) 238

boot system 119

bootfile 232

bootpdhcrelay cidoptmode 407

bootpdhcrelay enable 407

bootpdhcrelay maxhopcount 408

bootpdhcrelay minwaittime 408

bootpdhcrelay serverip 408

BPDU tunneling 151

bp dumigrationcheck, spanning-tree 316

bridge aging-time 89

broadcasts

broadcast storm recovery mode 390

broadcast storm trap 467, 492

buffer check 367

buffer dedicated (1G and stacking ports) 368, 369, 370

buffer dedicated interface (10G ports) 369

buffer dynamic (1G and stacking ports) 370

buffer dynamic interface (S25P) 372

buffer dynamic interface system-downlink 372

buffer packets interface 373

buffer tuning 367

buffered log 172

bulk configuration. See interface range. 91

C

card types 227

class 348

class command 31, 32

Class Commands, DiffServ 337

Class Map Mode 33

- Class Map mode 30
 - class-map 337, 338
 - class-map command 30
 - class-map match-all 338
 - class-map rename 339
 - classofservice dot1p-mapping 290, 328
 - classofservice dot1p-mapping 365
 - classofservice ip-dscp-mapping 328
 - classofservice ip-precedence-mapping 329
 - classofservice trust 329
 - clear arp-cache 394
 - clear commands
 - clear config 105
 - clear pass 106
 - clear traplog 106
 - clear vlan 127
 - clear config 22, 105
 - clear counters 106
 - clear dot1x statistics 189
 - clear igmpsnooping 106
 - clear ip dhcp binding 232
 - clear ip dhcp conflict 232
 - clear ip dhcp server statistics 232
 - clear lldp neighbors 159
 - clear pass 106
 - clear port-channel 290
 - clear radius statistics 189
 - clear traplog 106
 - clear vlan 127
 - CLI banner 109
 - client-identifier 233
 - client-name 233
 - clock time 243
 - Command Modes, Using 28
 - Command Syntax Conventions 23
 - Common Command Parameters 25
 - config commands
 - config arp agetime 232, 233, 234, 235, 238, 239, 240, 241, 393
 - config arp resptime 393
 - config arp retries 393
 - config lags adminmode 298
 - config lags create 293, 295, 297
 - config lags deleteport 291
 - config lags linktrap 298
 - config lags name 299
 - config loginsession 179
 - config port admin-mode 103, 305
 - config port linktrap 84, 85, 305
 - config port physical-mode 104
 - config switchconfig broadcast 390
 - config switchconfig flowcontrol 390
 - config trapflags bcaststorm 467, 492
 - config users add 19, 180
 - config users passwd 19, 180, 181
 - config vlan add 91
 - config vlan delete 91, 129
 - config vlan garp gvarp 88, 254
 - config vlan garp jointime 251
 - config vlan garp leavealltime 253
 - config vlan garp leavetime 252
 - config vlan interface acceptframe 141, 144
 - config vlan makestatic 130, 413
 - config vlan name 130, 131
 - config vlan participation 143, 144
 - config vlan ports gvrp 254, 255
 - config vlan ports ingressfilter 141, 142, 143, 144
 - config vlan ports pvid 144, 146
 - config vlan ports tagging 139, 140, 145, 147
 - Config Interface Vlan mode 33
 - Config router ospf area externrouting 425
 - Config router rip interface version receive 451
 - config users delete 181
 - config users passwd 181
 - config vlan ports ingressfilter 144
 - configuration guide 10
 - configuration reset 105
 - Configuration Scripting 122
 - configure 90
 - configure command 30
 - conform-color 348
 - Contact and Patents Information 11
 - control characters 26
 - copy 20, 21, 106
 - copy (clibanner) 109
 - copy system 19
 - CoS Queue Prioritization 328
 - cos-queue max-bandwidth 290, 330
 - cos-queue min-bandwidth 290, 330
 - cos-queue random-detect 291, 330
 - cos-queue strict 291, 331
 - cqueue min-bandwidth 290
 - Ctrl characters 26
 - current-active 121
 - CX4 cable length 36
- ## D
- dedicated buffers 367
 - default-information originate (OSPF) 430, 450

- default-information originate (RIP) 450
- defaultList (default log-in list) 188
- default-metric (OSPF) 430
- default-metric (RIP) 450
- Delete 27
- delete (software image) 120
- deleteport (global config) 291
- deleteport (interface config) 291
- description (port channel) 292
- description (port or VLAN) 127
- description (VLAN) 127
- destination port 95, 96
- device configuration commands 99, 100, 253, 260, 475–479
- DHCP client 233
- DHCP Pool Config 233
- DHCP Pool Config mode 30
- DHCP Pool Config mode, accessing 237
- DHCP Pool Configuration Mode 32
- DHCP Server 231
- Differentiated Services Code Point (DSCP) 332
- diffserv 337
- DiffServ Code Point (DSCP) 342
- dir 37
- disable ip multicast mdebug mtrace 459
- disconnect 179
- distance ospf 430
- distance rip 450
- distribute-list out 430, 450
- dns-server 234
- document conventions 23
- domain-name 234
- Dot1p (802.1p) 328, 329, 331
- dot1p-priority 293, 366
- dot1x defaultlogin 189
- dot1x initialize 189
- dot1x login 190
- dot1x max-req 190
- dot1x port-control 190
- dot1x port-control all 191
- dot1x re-authenticate 191
- dot1x re-authentication 191
- dot1x system-auth-control 192
- dot1x timeout 192
- dot1x user 193
- Double VLAN tagging 150
- drop 348
- DSCP 342
- DSCP (Differentiated Services Code Point) 332

- Dual Image Commands 119
- Dual Image Support 15
- duplex settings 104
- dvlan-tunnel etherType 152
- dvlan-tunnel l2pdu-forwarding enable 151
- dvlan-tunnel l2pdu-forwarding mac-address 151
- dynamic buffers 367
- Dynamic Host Configuration Protocol (DHCP) 231

E

- ECMP 16
- edge port, STP 317
- egress rate shaping 331
- enable 90
- enable (OSPF) 431
- enable (RIP) 451
- enable command 30
- enable passwd 110
- encapsulation 431
- encapsulation (interface) 397
- encapsulation (VLAN) 128
- Encapsulation Type 403
- encrypted OSPF authentication 433
- error log 175
- EtherChannel 287
- Ethernet Encapsulation Type 403
- Ethernet Range mode 30, 92
- Ethernet Range mode prompt 93
- Ethernet trunk 287
- event log 175
- Exit 27
- exit-overflow-interval 431
- expansion modules 227
- expedite kbps 349
- expedite percent 349
- external-lsdb-limit 431

F

- filedescr (software image) 120
- fixed buffers 367
- flow control 390
- Force10 Networks TAC 367
- frame acceptance mode 141, 144

G

- GARP commands 251
- General Attribute Registration Protocol (GARP) 251
- Global Config Mode 32
- Global Config mode 30

gmrp adminmode 257
 GMRP commands 251
 gmrp interfacemode all 258
 gmrp interfacemode enable (LAG) 294
 GVRP
 enabling or disabling 88, 254, 255
 join time 251
 leave time 252
 gvrp adminmode enable 254
 GVRP command 251
 gvrp interfacemode enable 254

H

hardware installation guide 10
 Hardware installation guides 11
 hardware-address 234
 history table 172
 h-node (hybrid) 238
 host 235
 hostname 37
 hostname, setting 37
 hostroutesaccept 453
 how router route table 415
 How to Use This Document 10

I

ICMP 410
 IEEE 802.1Q 141, 144
 IEEE 802.1x 15
 IfIndex 62
 IGMP (Internet Group Management Protocol)
 commands 273
 igmp enable 274, 294
 igmp enable (interface) 274
 igmp fast-leave 275, 294
 igmp groupmembership-interval 294
 igmp groupmembership-interval (interface) 275
 igmp interfacemode enable all 276
 igmp maxresponse 276, 281
 igmp mcrtpiretime 277
 igmp mcrtpiretime (interface) 294
 igmp mrouter 277, 295
 igmp mrouter interface 295
 igmp mrouter interface enable 278
 IGMP Proxy 16
 IGMP Snooping 15
 IGMP Snooping commands 273, 471
 IGMP v1/v2 (RFC 1112, 2236) 16
 IGMP v3 (RFC 3376) 16
 image1 121

image2 121
 ingress filtering 141, 142, 143, 144
 inlinepower 114
 inlinepower admin 115
 inlinepower limit 116
 inlinepower priority 116
 inlinepower threshold 115
 inlinepower type 116
 input rate limiting 338
 interface 91
 interface (access Interface Config mode) 91
 interface command 30, 32
 Interface Config Mode 32
 Interface Config mode 30
 interface loopback 95
 Interface Loopback Config mode 84, 398
 interface managementethernet 20, 38
 interface managementethernet command 31
 Interface ManagementEthernet mode 31, 38, 39
 Interface Port Channel Config mode 32, 296, 297, 305,
 306, 307, 308, 366
 interface port-channel 295
 interface range 91
 interface range command 92
 Interface Range mode 92
 Interface Range mode command
 auto-negotiate 89
 classofservice dot1p-mapping 328
 classofservice dot1pmapping 365
 classofservice ip-dscp-mapping 328
 classofservice ip-precedence-mapping 329
 classofservice trust 329
 deleteport 291
 dot1x max-req 190
 dot1x port-control 191
 dot1x re-authentication 192
 dot1x timeout 193
 dvlan-tunnel ethertype 152
 encapsulation 398
 igmp groupmembership-interval 275
 igmp maxresponse 277
 igmp mcrtpiretime 277
 igmp mrouter 278
 ip access-group 382
 ip irdp 410
 ip ospf 432
 ip ospf areaid 432, 486, 489, 490, 491, 492
 ip ospf authentication 433
 ip ospf authentication-key 433
 ip ospf cost 434

- ip ospf dead-interval 435
- ip ospf hello-interval 435
- ip ospf mtu-ignore 436
- ip ospf priority 436
- ip ospf retransmit-interval 437
- ip ospf transmit-delay 437
- ip rip 451
- ip rip authentication 452
- ip rip receive version 331, 452
- ip rip send version 147, 453
- ip vrrp ip 416
- ip vrrp mode 417
- ip vrrp preempt 417
- ip vrrp priority 418
- ip vrrp timers advertise 418
- ip vrrp vrID authentication 416
- mac access-group 387
- no port-security max-dynamic 185
- port lacpmode 299
- port-security 184
- port-security mac-address 184
- port-security mac-address move 184
- port-security max-static 185
- protocol vlan group 133
- shutdown 103
- snmp trap link-status 84
- snmp-server enable trap violation 83
- spanning-tree edgeport 317
- spanning-tree hello-time 318
- spanning-tree mst priority 325
- spanning-tree port mode enable 326
- speed 104
- vlan acceptframe 141
- vlan ingressfilter 143
- vlan pvid 147
- interface vlan 28, 30, 129, 140
- interface vlan command 31, 129
- Interface VLAN mode 125, 129
- Internet Group Management Protocol (IGMP) 471
- inventory 100, 103, 188, 221, 226, 253, 255, 259, 260, 349, 382, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 479, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497
- inverse mask 380
- ip access-group (Interface) 381
- ip access-group (port channel) 295
- ip access-group all 382
- ip address 20
- ip address (management) 38
- ip address (routed) 398
- ip address (VLAN) 413
- IP Address, Management 19
- ip dhcp bootp automatic 235
- ip dhcp conflict logging 235
- ip dhcp excluded-address 235
- ip dhcp filtering (global) 236
- ip dhcp filtering (interface) 236
- ip dhcp filtering trust 236
- ip dhcp ping packets 236
- ip dhcp pool 237
- ip dhcp pool command 30
- ip dvmrp 466
- ip dvmrp metric 467
- ip dvmrp trapflags 77, 467
- ip forwarding 398
- ip http javamode enable 213
- ip http secure-port 213
- ip http secure-protocol 213
- ip http secure-server enable 214
- ip http server enable 214
- ip igmp 471
- ip igmp last-member-query-count 472
- ip igmp last-member-query-interval 472
- ip igmp query-interval 473
- ip igmp query-max-resp-time 474
- ip igmp robustness 474
- ip igmp startup-query-count 474
- ip igmp startup-query-interval 475
- ip igmp version 475
- ip igmp-proxy 473
- ip irdp 410
- ip irdp address 410
- ip irdp holdtime 411
- ip irdp maxadvertinterval 411
- ip irdp minadvertinterval 411
- ip irdp preference 412
- ip mcast boundary 458
- IP MTU 403
- ip mtu 398
- ip multicast 458
- ip multicast staticroute 458
- ip multicast ttl-threshold 459
- ip netdirbcast 399
- ip ospf 432
- ip ospf areaid 432
- ip ospf authentication 433
- ip ospf authentication-key 433

ip ospf cost 434
 ip ospf dead-interval 434
 ip ospf hello-interval 435
 ip ospf mtu-ignore 436
 ip ospf priority 436
 ip ospf retransmit-interval 436
 ip ospf transmit-delay 437
 ip pimdm 485
 ip pimdm mode 486
 ip pimdm query-interval 486
 ip pimsm 491
 ip pimsm cbsrhashmasklength 489
 ip pimsm cbsrpreference 489
 ip pimsm crppreference 490
 ip pimsm datathreshrate 490
 ip pimsm message-interval 490
 ip pimsm mode 491
 ip pimsm query-interval 492
 ip pimsm spt-threshold 492
 ip pimsm staticrp 493
 ip pim-trapflags 77, 492
 ip proxy-arp 394
 ip rip 451
 ip rip authentication 451
 ip rip receive version 452
 ip rip send version 452
 ip route 399
 ip route default 400
 ip route distance 400
 ip routing 400
 ip ssh maxsessions 210
 ip ssh protocol 210
 ip ssh server enable 211
 ip ssh timeout 211
 ip telnet maxsessions 71
 ip telnet server enable 72
 ip telnet timeout 71
 ip vrrp 414, 415
 ip vrrp authentication 415
 ip vrrp ip 416
 ip vrrp mode 416
 ip vrrp preempt 417
 ip vrrp priority 418
 ip vrrp timers advertise 418
 ipaddr 25
 IPv4 (RFC 1812) 16
 IPv4 Router Discovery (RFC 1256) 16
 IRDP 410
 iSupport 10, 11

J

join time 251

K

key 207
 key, tacacs-server 206
 Keyboard Shortcuts 26

L

LAG (802.3ad) 287
 LAG in VLAN 136
 LAG ports 366
 LAGs
 configuring 293, 295, 297
 deleting ports from 291
 enabling or disabling 298
 link traps 298
 name 299
 summary information 303, 304
 Layer 4 342
 lease 237
 leave time 252, 253
 Line Config Mode 32
 Line Config mode 31
 lineconfig command 31
 lineconfig command, using 75
 link aggregate group (LAG) 287
 link aggregations. See LAGs
 Link Layer Discovery Protocol (LLDP) -- IEEE
 802.1AB 157
 Link State Advertisements (LSAs) 426
 link traps
 interface 84, 85, 305
 LAG 298
 Link-State Database (LSDB) 426
 LLDP (Link Layer Discovery Protocol) 157
 lldp hello 160
 lldp mode (global) 160
 lldp mode (interface) 161
 lldp multiplier 161
 lldp notification 162
 lldp notification-interval 162
 LLDP packet 158
 lldp timers-reinit 163
 lldp transmit-mgmt 163
 lldp transmit-tlv 163
 LLDPDU 160
 Logging
 logging buffered 169
 logging buffered wrap 170

- logging cli-command 170
- logging console 170
- logging facility 171
- logging history 172
- logging host 172
- logging persistent 173
- logging port 173
- logging syslog 173
- show eventlog 175
- show logging 174
- show logging eventlog 175
- show logging history 176
- show logging hosts 177
- show logging traplogs 177
- logging history command 172
- logging history size command 176
- logging host reconfigure 172
- logging host remove 172
- logical slot/port 25
- logout 19, 110
- logout commands 110, 111
- loopback interface 95
- LSA 426
- LSDB 426

M

- Mac Access List Config mode 31, 33, 385, 386
- mac access-group 387
- mac access-group (port channel) 296
- mac access-list extended 386
- mac access-list extended command 31
- mac access-list extended rename 386
- MAC address 234
- MAC Database Commands 88
- mac-access-list extended command 33
- macaddr 25
- mac-address (management VLAN) 39
- mac-type (management VLAN) 39
- makestatic 130
- management commands 71
 - 201 commands ??-74
- Management IP Address 19
- management route default 20, 40
- mark cos 350
- mark ip-dscp 350
- mark ip-precedence 351
- mark secondary-cos 355
- mask 235
- match any 340

- match class-map 340
- match cos 341
- match destination-address mac 341
- match dstip 341
- match dstl4port 342
- match ethertype 340
- match ip dscp 342
- match ip precedence 343
- match ip tos 343
- match protocol 343
- match secondary-cos 340
- match source-address mac 344
- match srcip 344
- match srcl4port 345
- match vlan 345
- max-hops, spanning-tree 319
- maximum-paths 438
- MD5 OSPF authentication 433
- member 218
- Microsoft client identifier 233
- mirrored port 95, 96, 101
- m-node (mixed) 238
- mode
 - Ethernet Range 30
 - Interface Port Channel Config 296, 297, 305, 306, 307, 308
 - Policy Class 346
 - Port Channel 30
 - VLAN Range 30
- mode access 30
- mode dvlan-tunnel 153, 297
- Mode-based Topology 29
- modes 30, 31, 84, 398, 438
 - Interface Port Channel Config 32, 275, 277, 289, 292, 293, 294, 296
 - Router OSPF Config 438
- monitor session 95
- monitor session 1 mode 96
- monitored port 101
- movemanagement 219
- mrinfo 460
- mstat 460
- mtrace 460
- mtu (LAG) 297
- mtu (port) 97
- mtu (VLAN) 130
- MTU, IP 403
- Multicast 485
- Multi-Link Trunking (MLT) 287
- multiple spanning tree instance (MSTi) 323

N

name (VLAN) 131
 native 139, 140
 NetBIOS mapping 238
 NetBIOS node type 238
 netbios-name-server 238
 netbios-node-type 238
 network 237
 network configuration commands 71
 201 commands ??-74
 network mac-address 41
 network mac-type 41
 network mgmt_vlan 131
 network mgmt_vlan. See vlan participation.
 network parms 41
 network protocol 41
 next-active 121
 next-server 238
 NIC bonding 287
 NIC teaming 287
 no cos-queue max-bandwidth 290, 330
 no ip mcast mroute 461
 no monitor 97
 no monitor session 1 98
 Node Manager 9
 NSSA (Not So Stubby Area) 425

O

objectives 9
 Open Shortest Path First (OSPF) commands 423
 option 239
 OSPF
 hello interval 428
 OSPF (Open Shortest Path First) commands 423
 OSPF authentication
 MD5 433
 simple 433
 OSPF commands 423
 OSPF MTU 436
 OSPF priority 436
 OSPF retransmit interval 436
 OSPF specification 430
 OSPF timers 426, 428, 434, 437
 OSPF transit delay 437

P

participation (VLAN) 131
 passwords
 changing user 181
 resetting all 106, 110

 setting user 19, 180
 special characters 19, 181
 user 180
 patents 11
 PDUs 251, 253
 persistent log 175
 PIM-DM commands 485
 PIM-SM commands 488
 PIM-SM-edge 16
 ping 111
 p-node (peer-to-peer) 238
 PoE (Power over Ethernet) 114
 PoE Commands 114
 PoE status 118
 PoE status types 118
 police-simple 352
 police-single-rate 353
 police-two-rate 353
 Policy Class Mode 32
 Policy Class mode 31
 Policy Commands, DiffServ 346
 policy map command 32
 Policy Map Mode 32
 Policy Map mode 31
 policy-classmap 346
 policy-map 354
 policy-map command 31
 policy-map rename 355
 port (for TACACS+) 207
 port channel 287
 port channel in VLAN 136
 Port Channel mode 30
 port channel ports 366
 Port Channel Range mode 92, 93
 port lacpmode enable 299
 port lacpmode enable all 299
 port lacpmode lacptimeout (global) 300
 port lacpmode lacptimeout (interface) 300
 port MAC locking 183
 port mirroring 95, 101
 port mode, spanning-tree 326
 port monitoring 101
 port teaming 287
 port trunking 287
 port-channel 297
 port-channel enable all (global) 298
 port-channel enable all (interface) 298
 port-channel linktrap 298
 port-channel name 299

- port-channel staticcapability 299
- portfast 317
- ports
 - administrative mode 103, 305
 - deleting from LAGs 291
 - frame acceptance mode 141, 144
 - GVRP 254, 255
 - information 101
 - ingress filtering 141, 142, 143, 144
 - link traps 84, 85, 305
 - physical mode 104
 - tagging 139, 140, 145, 147
 - VLAN IDs 144, 146
- port-security 183, 301
- port-security mac-address 184, 301
- port-security mac-address move 184, 301
- port-security max-dynamic 185, 301
- port-security max-static 185, 301
- Power over Ethernet (PoE) 114
- preemphasis, CX4 cable length 36
- priority 208
- priority (TACACS+) 208
- priority (VLAN) 132
- Private Edge VLAN 148
- Privileged Exec Mode 32
- Privileged Exec mode 30
- probe port 95
- Products and Services Liability 11
- prompt, Interface VLAN mode 129
- protected VLAN (PVLAN) 148
- protocol (management VLAN) 41
- Protocol Data Units. See PDUs
- protocol group 132
- Protocol Independent Multicast - Sparse Mode (PIM-SM)
 - commands 488
- Protocol Independent Multicast-Dense Mode (PIM-DM)
 - commands 485
- protocol lacp 301
- protocol static 302
- protocol vlan group 132
- protocol vlan group all 133
- Proxy ARP (RFC 1027) 16
- pvid (VLAN) 133
- PVLAN 148

Q

- QinQ 150
- QoS commands 327
- Quality of Service (QoS) commands 327
- Quick Reference 11

- quit 111

R

- radius accounting mode 199
- radius server host 200
- radius server key 201
- radius server msgauth 201
- radius server primary 201
- radius server retransmit 201
- radius server timeout 202
- randomdrop 355
- rate 98
- rate limiting 331
- rate shaping 331
- rate-interval 98, 302
- rate-limiting 352
- redirect 355
- redistribute 438, 453
- Related Documents 10
- release notes 10
- reload 22, 111
- reload command 367
- remotecon maxsessions 73
- remotecon timeout 74
- reset system command 111
- response time 393
- retries 393
- RFC 1700 233
- RFC 2328 430
- Router Config OSPF Mode 33
- Router Config RIP Mode 33
- router ospf 438
- router ospf command 31, 33
- Router OSPF Config mode 31, 438
- router ospf interface stats 443
- router rip command 31, 33
- Router RIP Config mode 31
- router-id 438
- routetid 25
- routing 401
- RSMLT 287

S

- S2410 documentation 9
- S25-01-GE-24P (S25P model switch) 228
- S25P 9
- S25P-DC 9
- S50 9
- S50-01-10GE-2C (10G CX4 module) 228

- S50-01-10GE-2P (10G XFP module) 228
- S50-01-12G-2S (12G stacking module) 228
- S50-01-24G-1S (24G stacking module) 228
- S50-01-GE-48T-V (S50V model) 228
- S50N 9
- S50N-DC 9
- S50V 9
- script apply 123
- script delete 123
- script list 123
- script show 124
- script validate 124
- serial baudrate 75
- serial timeout 76
- service dhcp 239
- service-policy 302, 357
- session-limit 72
- sessions
 - closing 110, 111, 179
 - displaying 179
- session-timeout 72
- set garp timer join 251, 302
- set garp timer leave 252, 302
- set garp timer leaveall 253, 303
- set gmrp adminmode 257
- set gmrp interfacemode 258
- set gmrp interfacemode all 259
- set gvrp adminmode 88, 255
- set gvrp interfacemode 255
- set gvrp interfacemode all 255
- set igmp (interface) 278
- set igmp (system) 278
- set igmp fast-leave 279
- set igmp groupmembership-interval (interface level) 279
- set igmp groupmembership-interval (system level) 279
- set igmp groupmembership-interval all 280
- set igmp interfacemode all 280
- set igmp maxresponse 280
- set igmp mcrtxpiretime (interface) 282
- set igmp mcrtxpiretime all 282
- set igmp mcrtxpiretime 281
- set igmp mrouter 283
- set igmp mrouter interface 283
- set prompt 38
- set slot disable 226
- set slot power 226
- setting the hostname 37
- SFTOS Command Reference 10
- SFTOS Configuration Guide 10
- shape average 356
- shape peak 356
- show accounting 203
- show arp 394
- show arp brief 395
- show arp switch 42
- show authentication 193
- show authentication users 194
- show bootpdhcprelay 409
- show bootvar 121, 219, 220, 221, 222
- show buffer allocation interface 376
- show class-map 358
- show classofservice dot1p-mapping 331
- show classofservice ip-dscp-mapping 332
- show classofservice ip-precedence-mapping 333
- show classofservice trust 333, 334
- show clock 243
- show commands
 - inventory 99, 100, 103, 221, 226, 253, 255, 259, 260, 382, 497
 - show arp table 394, 395
 - show inventory 100, 188, 226, 349, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 479, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496
 - show lags summary 303, 304
 - show login session 179
 - show port 101
 - show stats switch detailed 48, 51, 52, 57, 59
 - show switchconfig 389
 - show tacacs 208
 - show terminal 112
 - show users 180
 - show vlan detailed 59, 134, 136, 137
- show cx4-cable-length 43
- show diffserv 359, 360
- show diffserv service 360, 361
- show diffserv service brief 361
- show dot1q-tunnel 154
- show dot1x 194
- show dot1x all 194
- show dot1x detail 194, 195
- show dot1x statistics 194
- show dot1x summary 194
- show dot1x users 197
- show dvlan-tunnel 155
- show dvlan-tunnel l2pdu-forwarding 155
- show ethernet 43
- show eventlog command 68
- show forwardingdb agetime 98

show garp 253
 show gmrp configuration 259
 show gvrp configuration 255
 show hardware 18, 46
 show hardware Command 46
 show igmpsnooping 283
 show igmpsnooping command example 284, 285
 show igmpsnooping fast-leave 285
 show igmpsnooping interface command example 284
 show igmpsnooping mrouter interface 285
 show igmpsnooping vlan command example 284
 show inlinepower 118
 show inlinepower (stack) 117
 show inlinepower all example 118
 show interface 47, 57, 59
 show interface ethernet 50
 show interface ethernet switchport sample output 51
 show interface ethernet unit/slot/port command 49
 show interface ethernet unit/slot/port sample output 52
 show interface loopback 99
 show interface managementethernet 20
 show interface port-channel 304
 show interface port-channel brief 289, 303
 show interface port-channel brief command 303
 show interface port-channel command 304
 show interface unit/slot/port sample output 48, 49
 show interfaces 59
 show interfaces cos-queue 334
 show interfaces description 60, 128
 show interfaces description sample output 60
 show interfaces port-channel 303
 show interfaces switchport 148
 show ip access-lists 382
 show ip brief 403
 show ip dhcp binding 239
 show ip dhcp conflict 241
 show ip dhcp global configuration 240
 show ip dhcp pool configuration 240
 show ip dhcp server statistics 241
 show ip dvmrp 467
 show ip dvmrp interface 468
 show ip dvmrp neighbor 468
 show ip dvmrp nexthop 469
 show ip dvmrp prune 470
 show ip dvmrp route 470
 show ip http 215
 show ip igmp 476
 show ip igmp groups 476
 show ip igmp interface 477, 478
 show ip igmp interface membership 479
 show ip igmp interface stats 479
 show ip igmp-proxy 480
 show ip igmp-proxy groups 482
 show ip igmp-proxy groups detail 482
 show ip igmp-proxy interface 481
 show ip interface 401, 403
 show ip interface brief 404
 show ip irdp 412
 show ip mcast 461
 show ip mcast boundary 462
 show ip mcast interface 462
 show ip mcast mroute 462
 show ip mcast mroute group 463
 show ip mcast mroute source 463
 show ip mcast mroute static 464
 show ip ospf 439
 show ip ospf abr 440
 show ip ospf area 440
 show ip ospf command output 439
 show ip ospf database 441
 show ip ospf interface 441
 show ip ospf interface brief 443
 show ip ospf interface command output 442, 445
 show ip ospf interface stats 443
 show ip ospf neighbor 444
 show ip ospf neighbor brief 446
 show ip ospf range 446
 show ip ospf stub table 447
 show ip ospf virtual-link 447
 show ip ospf virtual-link brief 448
 show ip pimdm 486, 493
 show ip pimdm interface 487
 show ip pimdm interface stats 487
 show ip pimdm neighbor 488
 show ip pimsm 493
 show ip pimsm candrptable 494
 show ip pimsm componenttable 494
 show ip pimsm interface 495
 show ip pimsm interface stats 495
 show ip pimsm neighbor 496
 show ip pimsm rp 497
 show ip pimsm rphash 493, 497
 show ip pimsm staticrp 493
 show ip rip 454
 show ip rip interface 455
 show ip rip interface brief 455
 show ip route 404
 show ip route bestroutes 405

show ip route entry 405
show ip route preferences 406
show ip ssh 212
show ip stats 406
show ip vlan 413
show ip vrrp 420
show ip vrrp interface 420
show ip vrrp interface brief 420
show ip vrrp interface stats 419
show lldp interface 164, 165, 167
show lldp neighbors 165, 167
show lldp statistics 166
show logging 60
show logging buffered 174
show logging command 68
show logging history 176
show logging hosts 177
show logging hosts example 177
show logging traplogs 177
show login session 18, 179, 182
show mac access-lists 388
show mac-address-table 99
show mac-address-table gmrp 260
show mac-address-table igmpsnooping 285
show mac-address-table multicast 100
show mac-address-table stats 100
show mac-addr-table 61
show mac-addr-table all 61, 62, 63, 64, 148, 149
show mac-addr-table all sample output 61
show mac-addr-table count 62, 121, 221, 222, 332, 333, 358, 360
show mac-addr-table count sample output 62
show mac-addr-table vlan 62
show memory 63
show memory command 68
show memory sample output 63
show monitor 406
show monitor session 101
show mrfinfo 464
show msglog 63
show mstat 465
show mtrace 465
show network 64
show policy-map 362
show policy-map interface 363
show port 101
show port all 18
show port all command 68
show port protocol 103
show port-channel 304
show port-channel brief 304
show port-security 186
show port-security dynamic 187
show port-security static 187
show port-security violation 187
show process cpu 64
show process cpu command 68
show process cpu sample output 64
show radius 202
show radius accounting statistics 203
show radius statistics (authentication) 204
show running-config 65
show running-config command 68
show running-config sample output 65
show serial 76
show serial buffer unit 374
show serial sample output 76
show service-policy 364
show slot 226
show snmpcommunity 78
show snmptrap 78
show snmp 247
show snmp client 248
show snmp server 248
show spanning-tree 310, 321
show spanning-tree brief 310, 311
show spanning-tree interface 311, 321
show spanning-tree mst detailed 312
show spanning-tree mst port detailed 313, 322
show spanning-tree mst port summary 314
show spanning-tree mst summary 314
show spanning-tree summary 315
show spanning-tree vlan 315
show stack-port 219
show stack-port diag 220
show storm-control 389
show supported cardtype 227
show supported switchtype 223
show switch 221
show switchport protected 148
show sysinfo 66, 152, 365, 366, 367
show sysinfo sample output 67
show tacacs 208, 209
show tech-support 68
show telnet 73
show terminal 112
show terminal length 112
show trapflags 79

- show users 18, 180
- show users authentication 198
- show version 69
- show version command 68
- show version sample output 69
- show vlan 134
- show vlan association 134
- show vlan association subnet 136, 137
- show vlan brief 135
- show vlan id 136
- show vlan port 138, 147
- shutdown (port channel) 305
- shutdown (port) 103
- shutdown all (port) 103
- Simple Network Time Protocol (SNTP) commands 244
- simple OSPF authentication 433
- single-connection 208
- slot 229
- SMLT 287
- SNAP Encapsulation Type 403
- SNMP management commands 467
- SNMP system management commands 77
- snmp trap link-status 84, 305
- snmp trap link-status (Interface) 84
- snmp trap link-status all 85
- SNMP trap summary and trap details 177
- SNMP v3 access privileges 181
- snmp-server 79
- snmp-server community 80
- snmp-server community ipaddr 80
- snmp-server community ipmask 80
- snmp-server community mode 81
- snmp-server community ro 81
- snmp-server community rw 81
- snmp-server enable trap violation 83, 305
- snmp-server enable traps bcaststorm 81
- snmp-server enable traps linkmode 82
- snmp-server enable traps multiusers 82
- snmp-server enable traps stp mode 82
- snmp-server traps enable 83
- snmptrap 83
- snmptrap ipaddr 84
- snmptrap mode 84
- snmptrap snmpversion 85
- SNTP 3
- sntp broadcast client poll-interval 244
- sntp client mode 245
- sntp client port 245
- SNTP Commands 244
- sntp server 246
- sntp unicast client poll-interval 245
- sntp unicast client poll-retry 246
- sntp unicast client poll-timeout 246
- source port 95, 96, 101
- spanning-tree 315
- spanning-tree (LAG) 306
- spanning-tree 0 cost (LAG) 306
- spanning-tree 0 priority (LAG) 307
- spanning-tree bpdumigrationcheck 316
- spanning-tree configuration name 316
- spanning-tree configuration revision 316
- spanning-tree edgeport 317
- spanning-tree forceversion 317
- spanning-tree forward-time 317
- spanning-tree hello-time 318
- spanning-tree max-age 318
- spanning-tree max-hops 319
- spanning-tree mst 319, 324
- spanning-tree mst instance 320, 324, 325
- spanning-tree mst mst vlan 325
- spanning-tree mst priority 324
- spanning-tree msti 323
- spanning-tree MSTi cost (LAG) 307
- spanning-tree msti cost command 323
- spanning-tree msti external-cost command 323
- spanning-tree msti instance 324
- spanning-tree MSTi priority (LAG) 307
- spanning-tree msti priority command 323
- spanning-tree msti vlan 325
- spanning-tree mstp edge-port (LAG) 308
- spanning-tree port mode enable 326
- spanning-tree port mode enable all 326
- special characters 26
- speed 104
- speed all 104
- speedkeys 26
- speeds 104
- split-horizon 453
- S-Series switches 9
- SSH, enable/disable 211
- SSH2 Server 15
- sshcon maxsessions. See ip ssh maxsessions.
- sshcon timeout. See ip ssh timeout.
- stack 224
- stack command 31
- Stack Config Mode 33
- stacking commands 217
- Stacking Config mode 31
- static buffers 367

- statistics
 - switch, related 201 commands 48, 51, 52, 57, 59
- storm-control broadcast 390
- storm-control flowcontrol 390
- switch 389
 - inventory 99, 100, 103, 188, 221, 226, 253, 255, 259, 260, 349, 382, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 479, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497
 - resetting 111
 - statistics, related 201 commands 48, 51, 52, 57, 59
- switch priority 225
- switch renumber 225
- switchport protected (Global Config) 149
- switchport protected (Interface Config) 150
- syntax conventions 23
- syslog servers 60, 63
- system information and statistics commands
 - 201 commands 79
- system log 172
- system utilities ??-111217
- System Utility Commands 105

T

- Tab 27
- TAC (Technical Assistance Center) contact info 367
- TACACS
 - key 207
 - port 207
 - priority 208
 - show tacacs 208
 - single-connection 208
 - timeout 209
- TACACS Config Mode 33
- TACACS Config mode 29, 31
- tacacs-server host 205
- tacacs-server host ip-address command 31
- tacacs-server key 206
- tacacs-server timeout 207
- tagged 139
- tagged native command 140
- tagged port-channel 140
- tagging 139, 140, 145, 147
- Tech Tips and FAQ, S-Series 11
- Technical Assistance Center (TAC) 367
- telnet 73
 - enable or disable 72
 - sessions, closing 110, 111, 179

- sessions, displaying 179
- telnetcon maxsessions 73
- telnetcon maxsessions. See ip telnet maxsessions.
- telnetcon timeout. See ip telnet timeout.
- terminal length 112
- terminal length command 68, 112
- timeouts
 - ARP 232, 233, 234, 235, 238, 239, 240, 241, 393
 - TACACS 209
- TLV header 158
- TLV information string 158
- TLV Length 158
- TLV Type 158
- Topology, Mode-based 29
- TOS (type of service) 380
- traceroute 113
- traffic policing 352
- traffic-shape 331
- trap flags, broadcast storm 467, 492
- trap log, clearing 106
- trapflags 448
- trapflags (OSPF) 77
- TRAPMGR 178
- traputil.c 178
- trunks. See LAGs
- type 234
- type of service (TOS) 380

U

- unique identifier for a DHCP client 233
- show switch 222
- untagged 139, 140
- update bootcode 122
- User Account Management Commands 179
- user account management commands
 - 201 commands 179
- User Exec Mode 32
- User Exec mode 30
- user, new 180
- username 19, 180
- users
 - adding 19, 180
 - displaying 180
 - passwords 19, 106, 110, 180, 181
- users defaultlogin 198
- users login 199
- users snmpv3 accessmode 181
- users snmpv3 authentication 181
- users snmpv3 encryption 182
- Using Command Modes 28

V

- vlan 141
- vlan acceptframe 141
- vlan association mac 141
- vlan association subnet 142
- vlan commands (Global Config) 143, 144, 145, 146
- vlan ingressfilter 143
- VLAN Mode 33
- VLAN mode 31
- vlan name. See name.
- vlan participation (interface) 143
- vlan participation (management) 70
- vlan participation all 144
- vlan port acceptframe all 144
- vlan port ingressfilter all 144
- vlan port priority all 366
- vlan port pvid all 144
- vlan port tagging all 145
- vlan port untagging all 145
- vlan priority 366
- vlan protocol group 146
- vlan protocol group add protocol 146
- vlan protocol group remove 146
- vlan pvid 146
- VLAN Range mode 30, 92
- vlan routing 414
- VLAN Routing commands 413
- vlan tagging 147
- VLAN tunneling 150
- vlan untagging 147
- VLANs
 - adding 91
 - changing the name of 130, 131
 - deleting 91, 129
 - details 59, 134, 136, 137
 - frame acceptance mode 141, 144
 - GVRP 88, 254, 255
 - IDs 144, 146
 - ingress filtering 141, 142, 143, 144
 - jointime 251
 - leave all time 253
 - leave time 252
 - making static 130, 413
 - participation in 143, 144
 - resetting parameters 127
 - tagging 139, 140, 145, 147
- VRID (virtual router ID) 415
- VRRP (RFC 2338) 16
- VRRP commands 414

W

- Web connections, displaying 179
- wildcard mask 380
- wildcard masks, ACL 379
- Windows Internet Naming Service (WINS) 238
- WINS 238
- write 113
- write memory 113

