SFTOS Configuration Guide for the S2410

Version 2.4.1.0 **Edition 2** **April 2008**

FORCE10™

New Features

This guide is specifically for the S2410 models of the S-Series line of switches running SFTOS 2.4.1. SFTOS 2.4.1 is a variant of the Layer 2 package of SFTOS 2.3.1, designed specifically for the S2410 models. This preface describes major differences in SFTOS between Version 2.4.1 and from 2.3.1. See Chapter 1, SFTOS Features, on page 25 for a list of supported features.

New Features in SFTOS 2.4.1

Ethernet Management port: The S2410 switch has an Ethernet Management port (labeled *10/100 Ethernet* on the switch faceplate) that is dedicated to managing the switch. To configure that port, SFTOS 2.4.1 includes a new set of **serviceport** commands. See Configuring the Ethernet Management Port on page 82. You also have the option of managing the switch through the console port and management VLAN, which are common to all S-Series switches.

The major differences in SFTOS 2.4.1, in comparison to SFTOS 2.3.1 are:

- **Port ID format**: Because the S2410 does not support stacking, SFTOS version 2.4.1 does not need to address ports in the *unit/slot/port* format common to other versions of SFTOS. Instead, ports are identified simply in *slot/port* format. Physical ports have IDs with the slot always designated by 0, for example, **0/10** for port 10. Logical ports — VLAN and LAG — are identified with a 1 in the slot portion of the ID, such as **1/4** for LAG 4.
- **Speed commands**: All ports in the S2410 are fixed at 10GB, except the Ethernet Management port, so the speed and auto-negotiation commands in other versions of SFTOS are not included.
- **CX4 cable configuration**: The CX4 ports in the S2410 are auto-configuring to match signal strength to the cable length, so the CX4 pre-emphasis commands in other versions of SFTOS are not needed and are not available.

SFTOS 2.4.1 contains some other changes, in comparison to SFTOS 2.3.1:

- The maximum number of LAGs is 12, with a maximum of 12 ports in a LAG (vs. 32 LAGs, with a maximum of eight members each in SFTOS 2.3.1). See Chapter 10, Link Aggregation, on page 155.
- Maximum Jumbo Frame size increased from 9216 to 10240
- ACLs, CoS, and QoS:
    - IP ACLs are not available.
    - QoS DiffServ is not supported
    - The CoS traffic class range is reduced to four. See the commands using the *trafficclass* parameter in the QoS chapter of the *SFTOS Command Reference for the S2410*.

- The *ip_dscp* parameter of the **classofservice trust** command is not supported. See Quality of Service on page 169.
- Maximum MAC ACL rules per ACL are increased from 8 to 64.
- Maximum number of ACLs increased from 100 to 1024
- Only MAC ACLs with a source MAC is supported (cannot configure with a destination MAC)

Changes in this Guide

Most importantly, because the S2410 does not support routing, SFTOS version 2.4.1 does not include the Layer 3 package, which includes IGMP Proxy, IP Multicast, IP ACLs, OSPF, RIP, LAG and VLAN Routing, and VRRP. However, some allusions might still exist to availability of routing functionality, most specifically some statements that refer to a Routing chapter, which does not exist in this book, and description of interface configuration options that are not available on the S2410.

April 2008 Update: In this edition, the Broadcast Storm Recovery section is moved from the ACL chapter to the Security chapter (Enabling Broadcast Storm Control on page 133), with the **show interface ethernet** example replaced by a note that Broadcast Storm counters are not incremented in an S2410.

August 2007 Update: As noted above, stacking is not supported, so this edition of the guide has been modified to use the new slot/port format. Other edits are:

- Replacement of “E-Series” with “S-Series” where appropriate, along with replacement of references to E-Series CLI modes with S-Series CLI modes in some procedures
- Replacement in the Troubleshooting chapter of “crossover cable” (for the console connection) with “rollover cable”
- Replacement in the Web User Interface chapter of S50 switch icon and description with S2410 icon and description. Replaced sample Web UI panels for stacking with panels for interface statistics.

Deprecated Commands

In SFTOS 2.4.1.0, the following VLAN commands, in the Global Config and Interface Config modes, exist in the CLI but are deprecated:

- **vlan acceptframe**
- **vlan ingressfilter**
- **vlan participation all**
- **vlan port acceptframe**
- **vlan port ingressfilter all**
- **vlan port pvid all**
- **vlan port tagging all**
- **vlan port untagging all**
- **vlan pvid**
- **vlan tagging**

- **vlan untagging**

Note: To configure VLANs, use the **interface vlan** command (Global Config mode) to access the commands in VLAN mode. See VLANs on page 175.

- [**no**] **port lacpmode enable** (Interface Config mode) and [**no**] **port lacpmode enable all** (Global Config mode): These commands create configuration elements that do not survive a reload. Instead, use [**no**] **port channel staticcapability** (Global Config mode). See Link Aggregation Control Protocol (LACP) on page 164.

Contents

New Features 3

New Features in SFTOS 2.4.1 3
Changes in this Guide 4
Deprecated Commands 4

Contents 7

List of Figures 15

About this Guide 21

Objectives 21
Audience 21
Introduction to the Guide 21
Conventions 22
Related Force10 Documents and Additional Information 22
Contact Information 23
Documentation Feedback 23
Technical Support 23
The iSupport Website 23

Chapter 1
SFTOS Features 25

Overview of SFTOS 2.4.1 Features 25
Switch Management Options 25
Basic Routing and Switching Support 26
QoS 26
VLAN 26
Multicast Protocols 27
Security and Packet Control Features 27
Management 27
Functional Details 27

Chapter 2
Getting Started 29

Setting up Management Connections to the Switch 30
Connecting to the Console Port 31
Command Line Interface (CLI) Overview 33
CLI Command Modes 33
Getting Help From the CLI 34
Controlling Pagination 34
Checking Status 34
Viewing the Software Version and Switch Numbers 34
Verifying Details about the Switch 35
Showing Network Settings 36
Displaying Supported Features and System Up Time 37
Displaying Statistics 38
User Management 38
Creating a User and Password 39
Showing and Removing Created Users 39
Setting SNMP Read/Write Access 39
Setting the Enable Password 40
Enabling Interfaces 40
Enabling Ports 40
Setting the Management IP Address 41
Enabling Telnet to the Switch 42
Enabling and Using the SFTOS Web User Interface 42
Setting up SNMP Management 43
Creating VLANS 43
Important Points to Remember — VLANs 43
Setting Up a Management VLAN 44
Creating a Simple Configuration using VLANs and STP 44
Enabling Spanning Tree Protocol 46
Managing Configuration and Software Files 47
Important Points to Remember — Files 48
Downloading and Uploading Files 48
Upgrading the Software Image 49
Managing the Configuration 55
Using Configuration Scripts 58
Displaying Logs 62

Chapter 3
Using the Web User Interface 65

Accessing the Web User Interface 65
Command Buttons 67
Enabling and Using Java Mode 69

Enabling Java Mode . . . 69
Using the Web UI for Common Functions . . . 70
Using the Web UI to Access Information . . . 70
Using the Web UI to Configure QoS . . . 72
Using the Web UI for Switch Configuration Functions . . . 72
Using the Web UI for Security Configuration . . . 76

Chapter 4
Management . . . 81

Creating and Changing Management IP Addresses . . . 81
Configuring the Ethernet Management Port . . . 82
Changing the Management VLAN from the Default . . . 83
Verifying Access to the Management VLAN . . . 84
Verifying Management Port Connectivity . . . 85
Setting Stack Management Preferences . . . 85
Setting the Host Name Prompt . . . 85
Restoring the Configuration to Factory Defaults . . . 85
Setting up SNMP Management . . . 87
Managing SNMP Traps . . . 88
Setting up Simple Network Time Protocol (SNTP) . . . 90
SNTP Overview . . . 90
SNTP CLI Examples . . . 90
Using the Web UI to Configure SNTP . . . 92

Chapter 5
System Logs . . . 95

Logging Commands . . . 95
Configuring the System Log . . . 96
Displaying System Log Files . . . 97
Using the Persistent Event Log . . . 98
Displaying the SNMP Trap Log . . . 99
Configuring Syslog Server Host Connections . . . 100

Chapter 6
Configuring Interfaces . . . 103

Interface Support in SFTOS . . . 103
Viewing Interface Information . . . 104
Viewing Layer 3 Interface Information . . . 108
Configuring Physical Interfaces . . . 108
Bulk Configuration . . . 113
Using Interface Range Mode . . . 113
Bulk Configuration Examples . . . 114

Chapter 7
DHCP 115

DHCP Commands 115
Protocol Overview 115
Configuring the Switch as a DHCP Server 116
Important Points to Remember 116
Configuration Task List 116
Verifying the DHCP Server Configuration 118
Using the Switch as a BootP/DHCP Relay Agent 118
DHCP Relay Agent Overview 118
Configuring the Switch as a DHCP Relay Agent 119
Verifying the DHCP Relay Agent Configuration 119
Configuration Example — DHCP Server and Relay Agent 120

Chapter 8
Providing User Access Security 121

Choosing a TACACS+ Server and Authentication Method 121
Configuring TACACS+ Server Connection Options 124
Configuring a RADIUS Connection 124
Using the CLI to Configure Access through RADIUS 125
Using the Web UI to Configure Access through RADIUS 128
Enabling Secure Management with SSH or SSL 128
Enabling SSH 129
Enabling SSL/HTTPS 131
Enabling Broadcast Storm Control 133

Chapter 9
Spanning Tree 135

SFTOS STP Features 135
Forwarding, Aging, and Learning 135
Spanning Tree Protocol (IEEE 802.1d) 136
STP CLI Management 136
CLI Port Management 137
Spanning Tree Configuration Tasks 137
Setting the STP Version Parameter 137
Enabling STP 138
Example of Configuring STP 138
Changing Spanning Tree Global Parameters 140
Enabling an Edge Port 141
Multiple Spanning-Tree Protocol (MSTP, IEEE 802.1s) 141
Important Points to Remember 141
MSTP Implementation 142
MST Regions 142

MST Interactions 142
MSTP Standards 142
MST CLI Management 143
Rapid Spanning Tree Protocol (RSTP) 146
RSTP Implementation 146
Configuration Task List for RSTP 148
Display Spanning Tree Configuration 148
Displaying STP, MSTP, and RSTP Operation 153

Chapter 10
Link Aggregation 155

Link Aggregation—IEEE 802.3 155
LAG Load Distribution 156
LAG Implementation Restrictions 156
Static LAG Requirements 157
Link Aggregation Group (LAG) Commands 157
Static LAG CLI Management 158
Configuring a LAG 158
LAG Configuration Example 160
Adding a LAG to a VLAN 162
Using the Interface Range Mode 163
Link Aggregation Control Protocol (LACP) 164
LACP Configuration 164
Displaying LAGs (Port Channels) 166
MAC Addresses Displayed 166
Display LACP Configuration 167

Chapter 11
Quality of Service. 169

Chapter 12
Access Control Lists 171

SFTOS Support for Access Control Lists 171
Implementation Notes 171
Using ACL Commands 172
ACL Configuration Example 174

Chapter 13
VLANs 175

Introduction to VLAN Configuration 175
Important Points to Remember 176
Implementing VLANs 176
VLAN Mode Commands 177
Configuration Task List for VLANs 178

Creating the VLAN and Adding Ports . . . 178
Clearing/Resetting a VLAN . . . 182
Adding a LAG to a VLAN . . . 182
GARP and GVRP . . . 185
GARP VLAN Registration Protocol (GVRP) . . . 185
GARP Timers . . . 186
GARP Commands . . . 186
Using GVRP . . . 187
Enabling Dynamic VLANs with GVRP . . . 187
Displaying GARP, GVRP, GMRP Properties . . . 189
Using the Web User Interface for VLAN Configuration . . . 189
VLAN-Stack (DVLAN) Configuration . . . 190
DVLAN Tagging Considerations . . . 190
DVLAN Configuration Sequence . . . 190
Displaying VLAN Configuration Information . . . 194

Chapter 14
IGMP Snooping . . . 197

Enabling IGMP Snooping . . . 197
Monitoring IGMP Snooping . . . 198

Chapter 15
Port Mirroring . . . 199

Port Mirroring Features and Limitations . . . 199
Port Mirroring Commands . . . 200
Port Mirroring Configuration Examples . . . 200
Preparing to Configure Port Mirroring . . . 200
Verifying Port Mirroring . . . 202

Chapter 16
Troubleshooting . . . 205

Recovering from Flash File System Corruption . . . 205
Recovering from a Software Upgrade Failure . . . 206
Recovering from a Lost Password . . . 206
Preventing Auto-negotiation Mismatches . . . 207
Managing 10 Gigabit Interfaces . . . 207
10-GE Interfaces . . . 207
CX4 Interfaces . . . 207
Software Forwarding . . . 207
Troubleshooting No Output on the Console . . . 208

IEEE, RFCs, and SNMP . . . 211

IEEE Compliance . . . 211

RFC Compliance 212
MIBs 214
Industry MIBs Supported by SFTOS 2.4.1 214
Force10 MIBs 216
SNMP-related RFCs 216
SNMP Traps 218
Index 219

List of Figures

Figure 1 Using the Line Config Mode and the serial timeout Command 32
Figure 2 Using the show serial Command 32
Figure 3 Example of Navigating to CLI Modes 33
Figure 4 Using the show switch Command 34
Figure 5 Verifying Details about the Switch 35
Figure 6 Example of Configuring the Ethernet Management Port 36
Figure 7 Using the show network Command to Display Network Settings 36
Figure 8 Displaying All Supported Features and System Uptime 37
Figure 9 Creating a User and a Password 39
Figure 10 Showing Created Users 39
Figure 11 Creating and Displaying SNMP Access Levels 40
Figure 12 Setting the Enable Password 40
Figure 13 Enabling Ports Globally 41
Figure 14 Enabling an Individual Port 41
Figure 15 Inventory Information Panel of the SFTOS Web UI 43
Figure 16 Using the VLAN Configuration Panel of the Web UI 44
Figure 17 Using the CLI to Configure a VLAN 45
Figure 18 Spanning Tree Switch Configuration/Status Panel of the Web UI 46
Figure 19 CST Port Configuration/Status Panel of the Web UI 46
Figure 20 Example of Entering STP Commands in CLI 47
Figure 21 Downloading New Software 51
Figure 22 Displaying the Current Software Version 51
Figure 23 Saving the Current Configuration to NVRAM 52
Figure 24 Using the reload command to upgrade the OS 53
Figure 25 Example of Launching the Boot Menu to select a Code Download through Xmodem . . 54
Figure 26 Clearing the Running Configuration 56
Figure 27 Using the copy nvram:startup-config Command 56
Figure 28 Using the copy tftp Command to Download Startup-Config 56
Figure 29 Restoring the Configuration to Factory Defaults 57
Figure 30 Using the script show Command 59
Figure 31 Using the copy nvram:script Command 59
Figure 32 Using the copy tftp Command for a Script 60
Figure 33 Example of a Script Validation Error Message 61
Figure 34 Using the script apply Command 61

Figure 35 Using the script list Command 62
Figure 36 System Description Panel of the Web UI 66
Figure 37 Inventory Information Panel of the Web UI 67
Figure 38 SNMP Community Configuration Panel before Adding a Configuration 68
Figure 39 SNMP Community Configuration Panel after Adding a Configuration 68
Figure 40 Switch Navigation Icon with Service Port Configuration Panel 69
Figure 41 S2410 Switch Navigation Icon 69
Figure 42 Network Connectivity Configuration Panel of the Web UI 70
Figure 43 Port Detailed Statistics Panel of the Web UI 71
Figure 44 Port Summary Statistics Panel of the Web UI 71
Figure 45 ACL Interface Configuration Panel of the Web UI 72
Figure 46 Switch Configuration Panel of the Web UI 73
Figure 47 Port Configuration Panel of the Web UI 74
Figure 48 Spanning Tree MST Configuration/Status Panel of the Web UI 75
Figure 49 Spanning Tree MST Port Configuration/Status Panel of the Web UI 76
Figure 50 Port Security Interface Configuration Panel of the Web UI 77
Figure 51 Port Access Control Port Configuration Panel of the Web UI 77
Figure 52 RADIUS Configuration Panel of the Web UI 78
Figure 53 Secure HTTP Configuration Panel of the Web UI 78
Figure 54 Secure Shell Configuration Panel of the Web UI 79
Figure 55 Example of Configuring the Ethernet Management Port 82
Figure 56 Creating the Management Port IP Address 83
Figure 57 Changing the Management VLAN from the Default 84
Figure 58 Verifying Management Port Network 84
Figure 59 Verifying Management Port Connectivity 85
Figure 60 Setting the Host Name 85
Figure 61 Rebooting 86
Figure 62 Boot Menu 86
Figure 63 Using the show trapflags Command 89
Figure 64 Configuring SNTP Client Mode 91
Figure 65 Configuring the SNTP Client Port 91
Figure 66 Configuring the SNTP Server Connection 91
Figure 67 Using the show sntp client Command 91
Figure 68 Using the show sntp server Command 92
Figure 69 SNTP Global Configuration panel of the Web UI 92
Figure 70 SNTP Global Status Panel 93
Figure 71 SNTP Server Configuration Panel 93
Figure 72 SNTP Server Configuration Panel 94
Figure 73 SNTP Server Status Panel 94
Figure 74 Using the show logging buffered Command 97
Figure 75 Using the show logging Command 98
Figure 76 Using the show logging traplogs Command 99
Figure 77 Using the logging host Command 101

Figure 78 Using the show logging hosts Command 101
Figure 79 show running-config Command Example Showing Layer 2 Interface Information 104
Figure 80 Using the show interface switchport Command for Switch Summary Packet Information . 105
Figure 81 Using the show interface Command for Summary Packet Information for One Port . . 106
Figure 82 Using the show interface ethernet Command for Switch Detailed Packet Information 106
Figure 83 Checking Detailed Interface Counters Per Port 107
Figure 84 Using the show interfaces cos-queue Command on a Port 108
Figure 85 Interfaces Listed in the show port all Command (Partial) 109
Figure 86 Example of the show slot Command 110
Figure 87 Using the show port Command to Verify Port Settings 111
Figure 88 Clearing Counters 112
Figure 89 Using Bulk Configuration on a Single Range 114
Figure 90 Using Multiple Ranges 114
Figure 91 Using the show ip dhcp server statistics Command 118
Figure 92 Using the show bootpdhcprelay Command 119
Figure 93 Diagram of Two Switches Acting as DHCP Server and Relay Agent 120
Figure 94 Example of Configuring a Switch as a DHCP server 120
Figure 95 Example of Configuring a Switch as a DHCP relay agent 120
Figure 96 Setting the IP Address of a TACACS+ Server 122
Figure 97 Settings for Multiple TACACS+ Servers 123
Figure 98 Setting the Authentication Method 123
Figure 99 Verifying the Authentication Method Lists with the show authentication Command . . 123
Figure 100 Assigning and Verifying the Authentication Method List Assigned to Non-configured Users 123
Figure 101 RADIUS Topology 126
Figure 102 Configuration Example for RADIUS 126
Figure 103 Topology with Two RADIUS Servers 127
Figure 104 Configuration Example for Two RADIUS Servers 127
Figure 105 RADIUS Server Configuration Panel of the Web UI 128
Figure 106 Copying RSA1 Key to NVRAM for SSHv1 129
Figure 107 Copying RSA2 and DSA Keys to NVRAM for SSHv2 130
Figure 108 Using the show ip ssh Command to Show SSH Server Status 130
Figure 109 Using the show logging buffered Command to Show SSH Server Status 130
Figure 110 Copying SSL Certificates to NVRAM 131
Figure 111 Using the show ip http Command to Show HTTPS Server Status 132
Figure 112 Spanning Tree Topology Example 138
Figure 113 Using the spanning-tree Command 139
Figure 114 Using the spanning-tree port mode enable all Command 139
Figure 115 Using the spanning-tree port mode enable Command 139
Figure 116 MSTP Topology Example 144
Figure 117 MST Configuration on Switch R7 145
Figure 118 MST Configuration on R4 145

Figure 119 MST Configuration on R5 . . . 146
Figure 120 Example Output from show spanning-tree interface Command . . . 148
Figure 121 Example Output from spanning-tree brief Command . . . 149
Figure 122 Example Output from show spanning-tree Command . . . 149
Figure 123 Example Output from show spanning-tree mst port summary Command for Individual Ports 150
Figure 124 Example Output from show spanning-tree mst port summary Command for Individual Ports 150
Figure 125 Example Output from show spanning-tree mst port detailed Command for Individual Ports 151
Figure 126 Example Output from show spanning-tree mst port summary Command . . . 151
Figure 127 Example Output from show spanning-tree mst port summary Command . . . 152
Figure 128 Example Output from show spanning-tree mst port summary Command . . . 152
Figure 129 Example Output from show interface ethernet Command . . . 153
Figure 130 LAG Example in Network Diagram . . . 160
Figure 131 Adding Ports to a LAG . . . 161
Figure 132 Example of LAG Creation and Configuration . . . 162
Figure 133 Commands Available in Interface Range Mode . . . 163
Figure 134 Example of Enabling of LACP with LAG Configuration . . . 165
Figure 135 Displaying LAGs . . . 166
Figure 136 Displaying LAG Configuration by MAC Address . . . 166
Figure 137 Using show port command to display LACP Configuration . . . 167
Figure 138 Creating a Rule for a MAC Access List . . . 172
Figure 139 Sample Output from show mac access-list Command . . . 173
Figure 140 Sample Output from show mac access-lists Command . . . 173
Figure 141 ACL Configuration Example . . . 174
Figure 142 VLAN Topology . . . 179
Figure 143 Switch Connected to Other Switches through Multiple VLANs . . . 180
Figure 144 Example of Removing VLANs . . . 182
Figure 145 Adding a LAG to a VLAN . . . 183
Figure 146 Creating a LAG and learning its ID . . . 183
Figure 147 Adding ports to a LAG . . . 184
Figure 148 Adding a LAG to a VLAN . . . 184
Figure 149 Verifying a LAG in a VLAN with show vlan id and show port-channel id . . . 185
Figure 150 Diagram of VLAN between Switches . . . 188
Figure 151 Enabling GVRP on Switch and Interface on Switch 1 . . . 188
Figure 152 Setting up the VLAN and GVRP on Switch 2 . . . 188
Figure 153 Using the show vlan id Command . . . 188
Figure 154 Using the show garp and show gvrp configuration all Commands . . . 189
Figure 155 Example of Use of show dvlan-tunnel l2pdu-forwarding Command . . . 191
Figure 156 DVLAN Example Topology . . . 192
Figure 157 VLAN-Stack Configuration Sequence on R4 . . . 193
Figure 158 VLAN-Stack Configuration Sequence on R5 . . . 193
Figure 159 VLAN-Stack Configuration Sequence on R7 . . . 194

Figure 160 Using the show running-config and show vlan brief Commands 194
Figure 161 Example Output from show vlan Command 195
Figure 162 Example Output from show vlan id Command 195
Figure 163 Example Output from show vlan Command 196
Figure 164 Report from show igmpsnooping Command 198
Figure 165 Report from show mac-address-table igmpsnooping Command 198
Figure 166 Port Mirroring Diagram 199
Figure 167 Using the show monitor session command 200
Figure 168 Example of Specifying Source and Destination Mirror Ports 201
Figure 169 Example of Enabling Port Security 201
Figure 170 Command Example: Starting a Port Mirroring Session 201
Figure 171 Command Examples: Removing port mirroring configuration 202
Figure 172 show monitor session 1 Command Output 202
Figure 173 Example of show port all Showing Port Mirroring 203
Figure 174 Using show running-config Command Output to Show Port Mirroring 203
Figure 175 Using the show port command 203
Figure 176 Downloading Software to the Switch 205
Figure 177 Downloading Software to the Switch 206
Figure 178 Dedicating a Management Port on a Non-Default VLAN 209
Figure 179 Using the show serial Command to Determine Terminal Settings 209
Figure 180 Using the show logging traplogs Command 218

About this Guide

This chapter covers the following topics:

- Objectives on page 21
- Audience on page 21
- Introduction to the Guide on page 21
- Conventions on page 22
- Related Force10 Documents and Additional Information on page 22
- Contact Information on page 23
- Documentation Feedback on page 23
- The iSupport Website on page 23

Objectives

This document provides configuration instructions and examples for S-Series switches. It includes information on the protocols and features found in SFTOS™. Background on networking protocols is included to describe the capabilities of SFTOS.

For more complete information on protocols, refer to other documentation and IETF RFCs.

Audience

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

Introduction to the Guide

This guide provides examples of the use of the S-Series switches in a typical network. It describes the use of specific functions provided by the S2410 models of the S-Series line of switches, and includes instructions on how to configure those functions using the Command Line Interface (CLI) and the SFTOS Web User Interface.

Some S-Series switches operate purely as a Layer 2 switch, such as the S2410 models, some also as a Layer 3 router or a combination switch/router. The S2410 models also includes support for network management and Quality of Service functions such as Access Control Lists and Class of Service. Which functions you choose to activate will depend on the size and complexity of your network; this document provides detailed information on some of the most-used functions. For details on SFTOS features, see SFTOS Features on page 25.

Conventions

This document uses the following conventions to describe command syntax:

Convention	Description
keyword	Keywords are in bold and should be entered in the CLI as listed.
parameter	Parameters are in italics and require a variable—sometimes a number, sometimes a word, sometimes either—to be entered in the CLI. Shown between less-than and greater-than signs in the CLI help: <parameter>
{X}	Keywords and parameters within braces must be entered in the CLI.
[X]	Keywords and parameters within brackets are optional.
x | y	Keywords and parameters separated by bar require you to choose one.

Related Force10 Documents and Additional Information

The following documents comprise the documentation set for the S2410 models of the S-Series product line. All of the documents are available on the *S2410 Documentation* CD-ROM and on the Documents tab of iSupport (the Force10 Networks support website — http://www.force10networks.com/support:

- *SFTOS Command Reference for the S2410*
- *SFTOS Configuration Guide for the S2410*
- *S-Series and SFTOS Release Notes (2.4.1.x)*
- *S2410 Quick Reference* (also included as a printed booklet with the system)
- *Installing the S2410 System*
- MIBs files

The *S2410 Documentation* CD-ROM also contains slides from Training classes. The same kinds of documentation for all other S-Series models is on the *S-Series Documentation* CD-ROM and on iSupport. iSupport also contains S-Series Tech Tips and FAQs. Currently, access to user documentation on iSupport (see The iSupport Website on page 23) 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.

Contact Information

For technical support, see The iSupport Website on page 23. For other questions, contact Force10 using the following address:

Force10 Networks, Inc.
350 Holger Way
San Jose, CA 95134
USA

Documentation Feedback

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

- Document name
- Document part number
- Page number
- Software release version

Technical Support

The iSupport Website

Force10 iSupport provides a range of support programs to assist you with effectively using Force10 equipment and mitigating the impact of network outages. Through iSupport you can obtain technical information regarding Force10 products, access to software upgrades and patches, and open and manage your Technical Assistance Center (TAC) cases. 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 Force10 Networks 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 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	• 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	E-mail: support@force10networks.com Web: www.force10networks.com/support/ Telephone: US and Canada: 866.965.5800 International: 408.965.5800

For more on using the iSupport website and accessing services, see the *Force10 Service and Support Guide*, available on the Home tab, as displayed above.

Chapter 1 SFTOS Features

Overview of SFTOS 2.4.1 Features

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.

Note: The Layer 3 Package and the Stacking module of the Layer 2 Package are not included in SFTOS 2.4.1.

Switch Management Options

SFTOS 2.4.1 on the S2410 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 configured on the dedicated Ethernet Management port and/or the management VLAN).

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):** Force10 Networks provides Force10 Management System (FTMS), a graphical network management software product that provides a global view of your complete 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.
- **Web User Interface (Web UI):** See Chapter 4, Using the Web User Interface.

The SFTOS 2.4.1 software provides the following features through a limited version of its “Layer 2 Package” (also called the “Switching Package”).

Basic Routing and Switching Support

Note: The "Untested and Unsupported Features and Commands" section of the Release Notes contains the most current information on available features.

- BootP (RFC 951, RFC 1542)
- BootP/DHCP Relay and Server (RFC 2131)
- Host Requirements (RFC 1122)
- UDP (RFC 768)
- IP (RFC 791)
- ICMP (RFC 792)
- TCP (RFC 793)
- STP (Spanning Tree Protocol) (IEEE 802.1d)
- Rapid Spanning Tree (IEEE 802.1w)
- MSTP (IEEE 802.1s)
- 10 GigE (IEEE 802.3ae)
- 1000 Base-T (IEEE 802.3ab)
- Flow Control (IEEE 802.3x)
- IEEE 802.3ad
- 16k MAC Address Table
- Jumbo Frame Support

QoS

- ACL Entries (L2)
- Priority Queues — Four Queues per Port
- IEEE 802.1P Compliance
- Per Port Rate Limiting
- Per Queue Rate Limiting
- Strict Priority and Weighted Round Robin Scheduling
- Weighted Random Early Detect Congestion Control
- Wirespeed ACLs (L2/L3/L4)

VLAN

- IEEE 802.1q Support
- Frame Extensions (IEEE 802.3ac)
- GVRP, GARP, GMRP
- Port-based VLANs
- 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
- Log-in Access Control
- MAC-based Port Security
- Port Mirroring
- RADIUS
- SSH2 Server Support

Management

- HTML-based Management
- HTTPS/SSL
- RMON Groups
- SNMP v1/v2c
- SNTP Support
- SSHv2
- Syslog
- Telnet (RFC 854)
- TFTP (RFC 783)

Functional Details

In more detail, the functions supported by SFTOS 2.4.1 software include:

- Layer 2 Switching:
    - Bridging support (the default) for IEEE 802.1D — Spanning Tree plus IEEE 802.1w -- Rapid Reconfiguration and IEEE 802.1s — Multiple Spanning Tree (see Chapter 9, Spanning Tree, on page 135)
    - Virtual LAN (VLAN) operation conforming to IEEE 802.1Q, including Generic Attribute Registration Protocol (GARP), GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP) (see Chapter 13, VLANs, on page 175)

- Support for extensions to the Ethernet protocol:
  - VLAN tagging, required for VLAN support (formerly IEEE 802.3ac, now included in IEEE 802.3-2002)
  - Link Aggregation, which you may choose to implement to improve bandwidth and reliability for critical connections (formerly IEEE 802.3ad) (see Chapter 10, Link Aggregation, on page 155)
  - Flow Control at the MAC layer: you may configure the switch or a port to temporarily halt traffic when necessary to prevent overload (formerly IEEE 802.3x)
- Access control lists, used to control access to specified resources (see Chapter 12, Access Control Lists, on page 171.)
- Class of Service, which you can use to control traffic. See Chapter 11, Quality of Service, on page 169.
- Additional functions you can use to manage the network include IGMP Snooping (see Chapter 14, IGMP Snooping, on page 197), Port Mirroring (see Chapter 15, Port Mirroring, on page 199), and Broadcast Storm Recovery (see Enabling Broadcast Storm Control on page 133).

Chapter 2 Getting Started

This chapter summarizes the following basic tasks:

- Setting up Management Connections to the Switch on page 30
- Command Line Interface (CLI) Overview on page 33
- Checking Status on page 34
  - Displaying Statistics on page 38
  - Viewing the Software Version and Switch Numbers on page 34
  - Showing Network Settings on page 36
  - Displaying Supported Features and System Up Time on page 37
  - Verifying Details about the Switch on page 35
- User Management on page 38
  - Creating a User and Password on page 39
  - Showing and Removing Created Users on page 39
  - Setting SNMP Read/Write Access on page 39
  - Setting the Enable Password on page 40
- Enabling Interfaces on page 40
  - Enabling Ports on page 40
  - Setting the Management IP Address on page 41
  - Enabling Telnet to the Switch on page 42
  - Enabling and Using the SFTOS Web User Interface on page 42
  - Setting up SNMP Management on page 43
- Creating VLANS on page 43
- Managing Configuration and Software Files on page 47
  - Downloading and Uploading Files on page 48
  - Upgrading the Software Image on page 49
  - Managing the Configuration on page 55
  - Saving the Startup Configuration to the Network on page 56
  - Clearing the Running Configuration on page 55
  - Configuring from the Network on page 56
  - Restoring the System to the Default Configuration File on page 57
  - Using Configuration Scripts on page 58
  - Creating a Configuration Script on page 58

Setting up Management Connections to the Switch

You have a choice of methods to manage the S2410 switch. You can access the SFTOS command line interface (CLI) through either the console port on the switch or through an out-of-band method such as Telnet or SSH. To use any method other than the console port (VT100 emulation), you must first configure a management IP address on the switch. This chapter includes the procedures that connect you to the console and to set up a management IP address:

- **Console connection (VT100 interface):** See Connecting to the Console Port on page 31.
- **Management IP address:** See Setting the Management IP Address on page 41. See also Showing Network Settings on page 36.

Note: The S2410 is the only S-Series model to also have an Ethernet port dedicated to management (in addition to the console port and member ports of the management VLAN). The port is labeled "*10/100 Ethernet*" on the switch. The CLI refers to it as the "service port". This guide refers to it formally as the Ethernet Management port. The section Setting the Management IP Address on page 41 is for setting up the IP address of the management VLAN. To do the same for the Ethernet Management port, see Configuring the Ethernet Management Port on page 82.

After setting up the management IP address, you can use one of the following connection methods:

- **Simple Network Management Protocol (SNMP):** For details on setting up SNMP, see Setting SNMP Read/Write Access on page 39 and Setting up SNMP Management on page 87.

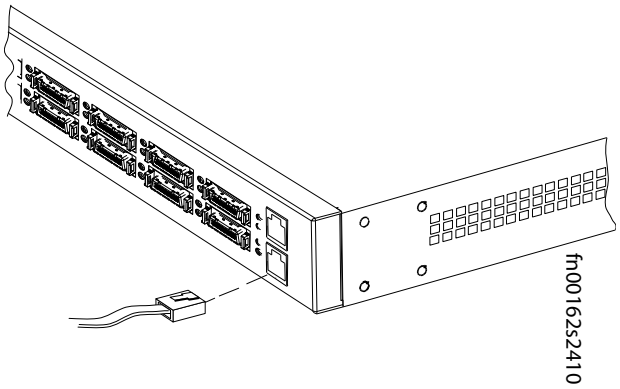
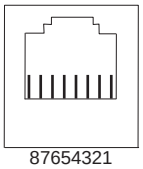
Note: The Force10 Management System (FTMS) is a graphical network management software product that provides a global view of your complete Force10 network. FTMS includes Node Manager, which not only provides GUI-based device management, it also includes the ability to execute CLI commands, either individually from Node Manager or by having Node Manager open a Telnet window to the device.

- **SFTOS Web User Interface (Web UI):** This chapter introduces you to examples of Web UI panels, such as in Creating VLANS on page 43. For details on setting up the connection to the Web UI, see Chapter 3, Using the Web User Interface. For details on adding secure access through SSL, see Enabling SSL/HTTPS on page 131.
- **Telnet:** See Enabling Telnet to the Switch on page 42. To use SSH to enable secure access over Telnet, see Enabling SSH on page 129.

Note: You can also use a configuration script to set up the switch. The maximum number of configuration file command lines is 2000. See Using Configuration Scripts on page 58.

Connecting to the Console Port

To use the console port, follow the procedure below:

Step	Task
1	**Caution:** You must use an Ethernet rollover cable (the same as used by the Force10 E-Series). This is in contrast to the straight-through cable used on other S-Series models. In more detail, The rollover cable connections are pin 1 to pin 8, pin 2 to pin 7, pin 3 to pin 6, pin 4 to pin 5, and the inverse for pins 5 through 8.   The console port pinout: Pin 1 = NC (unused) Pin 2 = DTR (output) Pin 3 = TxD (output) Pin 4 = GND Pin 5 = GND Pin 6 = RxD (input) Pin 7 = DSR (input) Pin 8 = NC
2	Connect the RJ-45/DB-9 adapter that is shipped with the switch to the RJ-45 cable.
3	Connect the adapter to a laptop.
4	Once a connection is established, ensure the following terminal settings (default settings) at both ends: 9600 baud rate, no parity, 8 data bits, 1 stop bit, no flow control (console port only). To change the settings (such as for when you want to download software at a higher speed), you must change the serial configuration on both the switch and computer. See the command options in the following step. For more, see the S2410 hardware guide or the *S2410 Quick Reference*.

Step	Task (continued)

5 Enter Line Config mode by logging in, entering Privileged Exec mode (**enable** command), then Global Config mode (**config** command), then **lineconfig**. In Line Config mode, use the **serial timeout** command to set the console inactivity timeout (0 for no timeout; up to 160 minutes):

```
User:admin
Password:
Force10 >enable
Password:

Force10 #configure
Force10 (Config)#lineconfig
Force10 (Line)#?
exit                    To exit from the mode.
serial                  Configure EIA-232 parameters and inactivity timeout.
session-limit           Configure the maximum number of outbound telnet
                        sessions allowed.
session-timeout         Configure the outbound telnet login inactivity timeout.
transport               Displays the protocol list to use for outgoing connections.
Force10 (Line)#serial ?
baudrate                Set the serial baudrate.
timeout                 Configure the serial port login inactivity timeout.

Force10 (Line)#serial timeout ?
<0-160>                 Enter time in minutes.

Force10 (Line)#serial timeout 0
Force10 (Line)#exit
Force10 (Config)#
```

Figure 1 Using the Line Config Mode and the serial timeout Command

6 To display serial (console) port configuration, enter the command **show serial**:

```
Force10 #show serial

Serial Port Login Timeout (minutes)..... 30
Baud Rate (bps)............................. 9600
Character Size (bits)....................... 8
Flow Control................................ Disable
Stop Bits................................... 1
Parity...................................... none
```

Figure 2 Using the show serial Command

Command Line Interface (CLI) Overview

The SFTOS Command Line Interface (CLI) is one of the ways to manage S-Series switches, and is the most complete. Another way is through the SFTOS Web User Interface (Web UI), which is discussed in Chapter 3, Using the Web User Interface. (Some of the Web UI panels are mentioned in this chapter.)

You can use the CLI through:

- **Console port:** As described above (Connecting to the Console Port on page 31), the port is the one located at bottom right of the front panel.)
- **Telnet (including SSH):** You can use any connected and enabled port in the management VLAN (configured with a Management IP address). See Setting the Management IP Address on page 41.

CLI Command Modes

The CLI of SFTOS follows the industry convention of mode-based access to functionality. In other words, 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 VLAN mode. For details on using the modes, see Chapter 4, Using the Command Line Interface, in the *SFTOS Command Reference*.

The main CLI command modes and the default prompts are as follows:

- User Exec: *hostname* >

Note: The default text for the *hostname* part of the prompt is “Force10 S2410”. You can modify that part of the prompt by using the **hostname** command. See Setting the Host Name Prompt on page 85.

- Privileged Exec (also called “enable mode”): *hostname* #
- Global Config (also called “config mode”): *hostname* (Config)#
- Interface Config: *hostname* (Interface *ifnumber*)#
- Interface VLAN (often shortened to “VLAN mode”): *hostname* (conf-if-vl-*vlan-id*)

Here is an example of navigating to these modes:

```
Force10 >enable
Password:
Force10  #configure
Force10  (Config)#interface 1/0/5
Force10  (Interface 1/0/5)#exit
Force10  (Config)#interface vlan 20
Force10  (conf-if-vl-20)#exit
Force10  (Config)#exit
Force10  #lineconfig
Force10  (Line)#
```

Note: Note the use of “1/0/5” in this example. SFTOS 2.4.1 does not use the initial “1/”, which would indicate the unit number in a stack. SFTOS 2.4.1 does not support stacking.

Figure 3 Example of Navigating to CLI Modes

Getting Help From the CLI

The following help commands are the same as those found in the E-Series:

- Use "**?**" at the prompt to get a list of commands in that mode: "**Force10# ?**"
- Use "**?**" with a partial command to see what initial command words in that mode begin with that string: "**Force10# i?**"
- Use "**?**" after a command or partial command to get a list of commands that start with that word: "**Force10# ip ?**"

Controlling Pagination

Starting in SFTOS Release 2.3, you can use the **terminal length** command to set how much of the output of a CLI "**show**" command to display. Use the **show terminal** command to display the current setting of the **terminal length** command. For details, see the *System Configuration Commands* chapter in the *SFTOS Command Line Reference*.

Checking Status

SFTOS follows the industry convention of using "**show**" commands to generate status reports through the command interface.

The Web UI also contains many status panels, which are clustered with their related configuration panels in the navigation tree. See Using the Web User Interface on page 65.

Viewing the Software Version and Switch Numbers

If you are concerned that you might not have the correct software version, you can select from several commands to see the installed code version. The following is an example of using **show switch** , which you can execute in either User Exec or Privileged Exec modes:

```
Force10 #show switch

        Management    Preconfig     Plugged-in         Switch          Code
Switch    Status      Model ID      Model ID           Status         Version
------ ------------ ------------- ------------- --------------------- --------
1      Mgmt Switch  SA-01-GE-48T  SA-01-GE-48T  OK                    2.3.1

Force10 #
```

Figure 4 Using the show switch Command

The Switch column shows the switch ID, which is useful if the switch is in a stack. For example, if the switch ID were 2, the switch's physical interfaces would be identified as 2/0/*port-number.*

Verifying Details about the Switch

The following example is of the **show switch** *unit* command for getting more details about the switch:

```
Force10 #show switch

        Management    Preconfig     Plugged-in         Switch          Code
Switch    Status      Model ID      Model ID           Status         Version
------ ------------ ------------ ------------ --------------------- --------
1      Mgmt Switch  SA-01-GE-48T  SA-01-GE-48T  OK                    2.3.1

Force10 #show switch 1
Switch........................... 1
Management Status................ Management Switch
Hardware Management Preference.... Unassigned
Admin Management Preference...... 1
Switch Type...................... 0x56950202
Preconfigured Model Identifier.... SA-01-GE-48T
Plugged-in Model Identifier...... SA-01-GE-48T
Switch Status.................... OK
Switch Description...............
Expected Code Type............... 0x100b000
Detected Code Version............ 2.3.1
Detected Code in Flash........... 2.3.1
Serial Number.................... DE4000106
Up Time.......................... 0 days 10 hrs 11 mins 52 secs
```

Figure 5 Verifying Details about the Switch

You can also use the **show hardware** command to display the running code version. See the sample output in the section Upgrading the Software Image on page 49.

The **show version** command displays more details about the software packages installed, and also the hardware present on the system. This command provides the details shown by the **show hardware** and **show sysinfo** commands, along with interface information, the u-boot version number, and the system image file version. The **show tech-support** command is the most lengthy, because it includes the output from each of these other commands.

Showing Network Settings

SFTOS 2.4.1 contains support for both the IP-based *management VLAN*, which is available on all S-Series switches, and for the *Ethernet Management port* (also called the *serviceport*), in the S2410, dedicated to switch management. To inspect the Ethernet Management port settings, execute the **show serviceport** command from either the User Exec or Privileged Exec modes, as shown below in Figure 6 on page 36.

```
(Force10 S2410) #show serviceport

IP Address..................................... 10.11.197.177
Subnet Mask.................................... 255.255.0.0
Default Gateway................................ 10.11.197.190
Service Port Configured Protocol Current.......... None
Burned In MAC Address.......................... 00:01:E8:99:99:9A
Link Status.................................... Up

(Force10 S2410) #
```

Figure 6 Example of Configuring the Ethernet Management Port

To inspect the settings of IP-based management VLAN for the switch, execute the **show interface managementethernet** command from either the User Exec or Privileged Exec modes. The data includes the management IP address, subnet mask, default gateway, MAC information, Web mode status, etc., as shown below:

```
Force10 #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
```

Figure 7 Using the show network Command to Display Network Settings

For details on setting up management addresses, see Setting the Management IP Address on page 41. See also Setting up Management Connections to the Switch on page 30.

Note: SFTOS v. 2.3 replaced the **show network** command with **show interface managementethernet**.

Displaying Supported Features and System Up Time

The following is an example of using **show version** to display all supported features and system up time:

```
Force10 #show version
Switch: 1
System Description.............................. Force10 S50
Vendor ID....................................... 07
Plant ID........................................ 01
Country Code.................................... 04
Date Code....................................... 062005
Serial Number................................... DE4000126
Part Number..................................... 759-00001-00
Revision........................................ 0A
Catalog Number.................................. SA-01-GE-48T
Burned In MAC Address........................... 0001.E8D5.A151
Software Version................................ 2.2.1
Additional Packages............................. Force10 QOS
                                                 Force10 Stacking
10/100 Ethernet/802.3 interface(s).............. 0
Gig Ethernet/802.3 interface(s)................. 2
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.................................. 1 days 22 hrs 55 mins 34 secs

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                    Force10 Reference MIB
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.


USM-TARGET-TAG-MIB                 SNMP Research, Inc.
F10OS-POWER-ETHERNET-MIB           F10OS Power Ethernet Extensions MIB
POWER-ETHERNET-MIB                 Power Ethernet MIB
LAG-MIB                            The Link Aggregation module for managing IEEE 802.3ad
RFC 1213 - RFC1213-MIB             Management Information Base for Network
                                   Management of TCP/IP-based internets: MIB-II
RFC 1493 - BRIDGE-MIB              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
F10OS-SWITCHING-MIB                F10OS Switching - Layer 2
F10OS-INVENTORY-MIB                F10OS Unit and Slot configuration.
F10OS-PORTSECURITY-PRIVATE-MIB     Port Security MIB.

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

Figure 8 Displaying All Supported Features and System Uptime

Displaying Statistics

Privileged Exec mode commands to display statistics include:

- Switch summary statistics:
  - **show interface switchport**
- Interface summary statistics:
  - **show interface** *slot/port*
- Switch detailed statistics:
  - **show interface ethernet switchport**
- Interface detailed statistics:
  - **show interface ethernet** *slot/port*

User Management

This section contains the following subsections:

- Creating a User and Password on page 39
- Showing and Removing Created Users on page 39
- Setting the Enable Password on page 40
- Enabling Ports on page 40
- Setting the Management IP Address on page 41
- Enabling and Using the SFTOS Web User Interface on page 42

The default CLI user, **admin**, has read/write access, with no password until you create one (see Creating a User and Password on page 39). You can also control user access through access control servers, such as TACACS+ and RADIUS. See the Security chapter for details (page 121).

A difference in SFTOS 2.2.1 and later is that the users you create (up to six, including **admin**) all have read/write access. If you enable the Web UI to the switch, these users have complete read/write access through the Web UI.

While there is no mode-level password control through the Web UI (you can create a Web access password per user, but after the user logs in, all of the configuration functions are available), there is one mode-level password that you can configure to allow the user to move from User Exec mode to Privileged Exec mode in the CLI. That password is called the “enable” password. See Setting the Enable Password on page 40.

Creating a User and Password

The **username** *passwd* command SFTOS Version 2.2.1 and above replaces the **users name** and **users passwd** commands. It creates the username and password in one statement. You can change a password either by reentering the command with the new password or by removing the user with the **no username** command and reentering the user with a new password.

```
Force10 (Config)#username w_turner passwd willspwd
User login name and password are set.

Force10 (Config)#no username w_turner

Force10 (Config)#username w_turner passwd newpwd
User login name and password are set.Password Changed!
```

Figure 9 Creating a User and a Password

Showing and Removing Created Users

An alternative to the **no username** command shown above is to use the **clear pass** command to delete all created users. The following example shows the **show users** command and the **clear pass** command:

```
Force10 #show users
                              SNMPv3          SNMPv3         SNMPv3
User Name    User Access Mode  Access Mode  Authentication  Encryption
----------  ----------------  -----------  --------------  ----------
admin        Read/Write        Read/Write   None            None
w_turner    Read/Write         Read Only    None            None

Force10 #clear pass
Are you sure you want to reset all passwords? (y/n)y
Passwords Reset!
```

Figure 10 Showing Created Users

Setting SNMP Read/Write Access

Note: You can use the User Accounts panel of the Web UI (**System** --> **Configuration** --> **User Accounts**) to accomplish both the creation of a user ID (see above) and this task. For details on the Web UI, see Using the Web User Interface on page 65.

The command **users snmpv3 accessmode** *username* {**readonly** | **readwrite**} enables you to set SNMP privileges for specific users. As used above (Showing and Removing Created Users on page 39), the **show users** command displays the read and write privileges for each defined user:

```
Force10 (Config)#users snmpv3 accessmode student2 readwrite
Force10 #show users

                                SNMPv3          SNMPv3         SNMPv3
User Name   User Access Mode  Access Mode  Authentication  Encryption
----------  ----------------  -----------  --------------  ----------
admin       Read/Write        Read/Write   None            None
student1    Read Only         Read Only    None            None
student2    Read Only         Read/Write   None            None
```

Figure 11 Creating and Displaying SNMP Access Levels

For details on SNMP, see Setting up SNMP Management on page 87.

Setting the Enable Password

To change the Privileged Exec password (also called the “Enable” password) in SFTOS Version 2.3.1 and above, you do so in Global Config mode. Enter **enable passwd**, press **Enter**, and enter a new password:

```
Force10 #enable passwd
Enter new password:*******
Confirm new password:*******
Password Changed!
```

Figure 12 Setting the Enable Password

Enabling Interfaces

This section covers the enabling of ports, VLANs, and management interfaces (Telnet, Web UI, SNMP):

- Enabling Ports on page 40
- Setting the Management IP Address on page 41
- Enabling Telnet to the Switch on page 42
- Enabling and Using the SFTOS Web User Interface on page 42
- Setting up SNMP Management on page 43

Enabling Ports

When the switch is first installed, all ports are disabled. To enable all ports, enter **no shutdown all** in Global Config mode. Alternatively, you can use the **no shutdown** command at the specific interface level.

```
Force10 >enable
Force10 #config
Force10 (Config)#no shutdown all
Force10 (Config)#
```

Figure 13 Enabling Ports Globally

```
Force10 >enable
Force10 #config
Force10 (Config)#interface 0/22
Force10 (Interface 0/22)#no shutdown
```

Figure 14 Enabling an Individual Port

For more on setting up ports, see Configuring Interfaces on page 103.

Setting the Management IP Address

On first startup, you have management access only through the console port. If you want to manage the switch through an IP-based access method (SFTOS Web User Interface, Telnet, SSH, SNMP, TFTP, etc.), you must configure a management IP interface, using the following the procedure.

Note: This section is for setting up the IP address of the management VLAN. To do the same for the Ethernet Management port (labeled "*10/100 Ethernet*" on the S2410 switch), see Creating and Changing Management IP Addresses on page 81.

Step	Command Syntax	Command Mode	Purpose
1	**show interface managementethernet**	User Exec or Privileged Exec	Display current management IP configuration.
2	**management route default** *gateway*	Global Config	Set the IP gateway of the management interface.
3	**interface managementethernet**	Global Config	Invoke the (Config-if-ma)# prompt.
4	**ip address** *ipaddr subnetmask*	(Config-if-ma)# prompt within the Global Config mode	Set the IP address and subnet mask of the management interface.

By default, the management address is reachable from all ports on the default VLAN, VLAN 1. One or more ports in that VLAN must be enabled, as described in Enabling Ports, above. To change to another VLAN, see Setting Up a Management VLAN on page 44.

After you enable and connect ports in the management VLAN and configure the management IP address, as described above, you can manage the switch through a variety of means. The following procedures describe enabling Telnet, the Web UI, and SNMP, respectively.

Enabling Telnet to the Switch

Access to the switch through a Telnet server is disabled by default. If you want to access the switch through an SSH client, you would leave Telnet disabled and set up the SSH connection, as described in Enabling Secure Management with SSH or SSL on page 128.

To enable Telnet access, execute the **ip telnet server enable** command.

Enabling and Using the SFTOS Web User Interface

The SFTOS Web User Interface (Web UI) provides much of the functionality provided by the SFTOS CLI, and, in some ways, is more powerful. Also, the CLI and Web UI can be used in combination to give you even better control and feedback.

1. To enable the Web UI, you first must enable ports, assign a management IP address, and enable the HTTP interface, which is described above in Setting the Management IP Address on page 41.

Note: For details on enabling an HTTPS secure server, see Enabling SSL/HTTPS on page 131 or the S2410 Documentation CD-ROM.

2. Enable the Web UI. In Global Config mode, execute the **ip http server** command.
3. To enable the switch icon on the Web UI (see Enabling Java Mode on page 69), execute the **ip http javamode enable** command.
4. Launch a supported Web browser. The Web browser must support:
   - HTML version 4.0, or later
   - HTTP version 1.1, or later
   - JavaScript(TM) version 1.2, or later
5. Enter the URL of the switch (http://<IP address>) in the Web browser address field. The IP address is the management IP address that you assigned in Setting the Management IP Address on page 41.
6. When the Login panel is displayed, click the **Login** button.
7. Enter the admin username and password, or any other username and password that you created, as discussed above.
8. The Navigation tree is displayed in the left frame, and the System Description panel is displayed in the right frame. Make your selection by clicking on the appropriate item in the Navigation tree.

   For example, Figure 15 on page 43, shows that the Inventory Information panel opened when the user clicked the Inventory Information node in the tree. Notice that the Inventory Information panel displays the same information as the **show version** command of the CLI, including the serial number of the switch. Notice also the large red Help button, which displays on every panel, and provides context help for the panels in the selected branch of the tree.

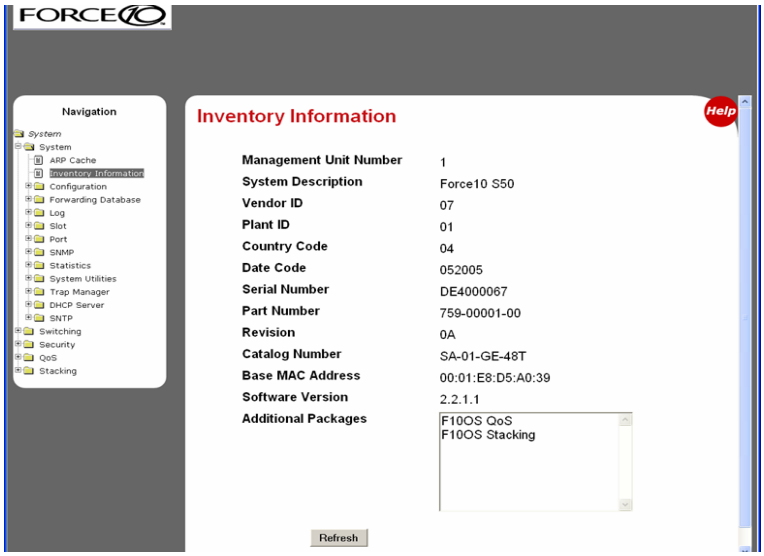


Figure 15 Inventory Information Panel of the SFTOS Web UI

For more details on using the Web UI, see Using the Web User Interface on page 65.

Setting up SNMP Management

To use an SNMP-based network management tool, you must enable a management IP address for the switch, as described above (see Setting the Management IP Address on page 41) and have the switch join an SNMP community (see Setting up SNMP Management on page 87 in the Management chapter). Most SNMP traps are enabled by default. For details, see Managing SNMP Traps on page 88 in the Management chapter.

Creating VLANS

This section contains these subsections:

- Important Points to Remember — VLANs
- Setting Up a Management VLAN
- Creating a Simple Configuration using VLANs and STP on page 44
- Enabling Spanning Tree Protocol on page 46

Important Points to Remember — VLANs

- The default management VLAN is VLAN 1 by default.
- By default, ALL ports are members of VLAN 1 untagged.
- It is possible to set the management VLAN to a VLAN that does not exist.

- If you cannot reach anything from the management address, check the management VLAN using **show interface managementethernet** or **show running-config**.

For details on setting up VLANs, see the chapter Chapter 13, VLANs.

Setting Up a Management VLAN

As described in Setting the Management IP Address on page 41, when you set up a management IP address, you can manage the switch through an IP-based access method (SFTOS Web User Interface, SNMP, Telnet, etc.); any enabled port in the management VLAN is available for the IP-based access.

By default, the management VLAN is set up on the default VLAN 1, which, on first startup, includes every port (although, by default, all ports are shut down until you enable them—see Enabling Ports on page 40.)

To set up a different VLAN to be the management VLAN, see Creating a Simple Configuration using VLANs and STP, next, and then see Changing the Management VLAN from the Default on page 83 in the Management chapter.

Creating a Simple Configuration using VLANs and STP

This section shows the use of the SFTOS Web UI. For more on using the Web UI, see Using the Web User Interface on page 65.

Using the SFTOS Web UI is the easiest way to create a VLAN. The following screenshot of the VLAN Configuration panel shows selection of a group of ports to add to a VLAN.

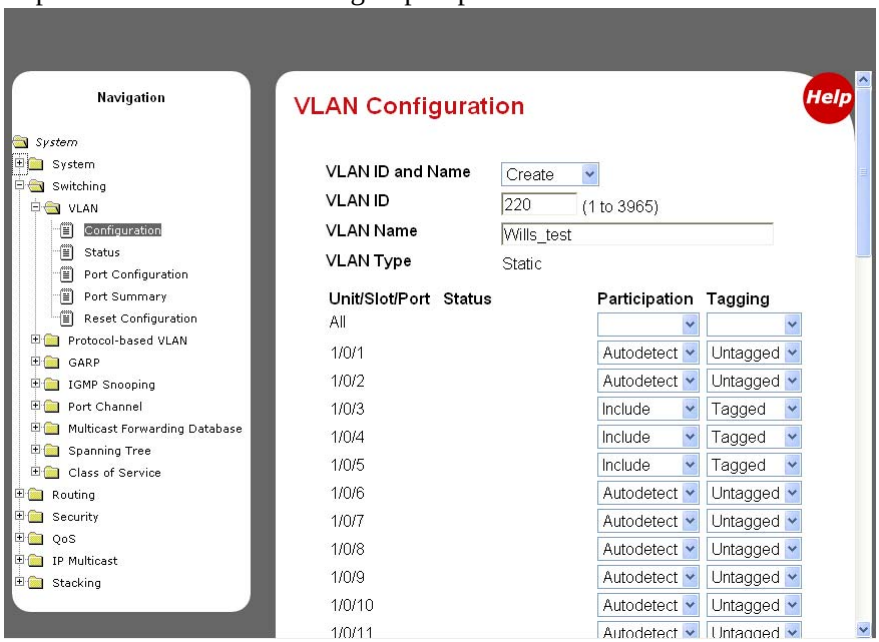


Figure 16 Using the VLAN Configuration Panel of the Web UI

1. Access the VLAN Configuration panel by traversing the Navigation tree in this sequence: **System** >> **Switching** >> **VLAN** >> **Configuration**.
2. On the VLAN Configuration panel, select **Create** from the **VLAN ID and Name** field, enter a unique number in the **VLAN ID** field to identify the VLAN.
   Optionally, enter a name for the VLAN in the **VLAN Name** field.
3. From the **Unit/Slot/Port** list, select the physical and logical interfaces that you want to include in the VLAN, and whether you want them to participate in tagged or untagged mode. Note that any configured logical interfaces will be listed at the bottom of the list.
4. When you have finished, click the **Submit** button at the bottom of the panel.

   If you have questions about VLAN configuration, click the red **Help** icon in the upper right corner of the panel.

Note: As noted in Enabling Ports on page 40, all ports are disabled by default. Enable them with **no shutdown all** (Global Config mode), or individually with the **no shutdown** command on each port.
The equivalent action on the Web UI is to select **Enable** in the Admin Mode field on the Port Configuration panel.

If you prefer to use the command line interface (CLI) for the same purpose, here is an example of using the CLI to create a VLAN (55) and add an interface to it:

```
Force10 (Config)#interface vlan 55
Force10 (Conf-if-vl-55)#tagged 0/5
Force10 (Conf-if-vl-55)#untagged 0/6
Force10 (Config)#interface 0/1
```

Figure 17 Using the CLI to Configure a VLAN

Note: The above example shows the procedure with the changes instituted in SFTOS Release 2.3, replacing **vlan database** and **vlan** *id* with **interface vlan** *id*.

The above example uses the Interface VLAN mode, which is new in SFTOS 2.3. If you need to assign many ports to the VLAN, you might use the Interface Range mode (also new in SFTOS 2.3). You can still use the Interface Config mode to accomplish the same result, but it requires more commands.

The **tagged 0/5** command not only assigns the port to VLAN 55, it also sets the Port VLAN ID (PVID) to 55 (causing untagged frames to be assigned to VLAN 55) and causes frames transmitted by this port to be tagged as part of traffic for VLAN 55.

These additional functions are handled by the VLAN Port Summary panel of the Web UI, and their Help screens can assist you in configuring them. For more on using the CLI to create VLANs, see Chapter 13, VLANs.

Enabling Spanning Tree Protocol

Spanning Tree Protocol (STP) is off by default. To use the Web UI to enable STP globally, navigate to the **Spanning Tree** branch (traverse the navigation tree: **Switching** > **Spanning Tree**), and then select the **Switch Configuration/Status** panel (This switch is running MSTP):

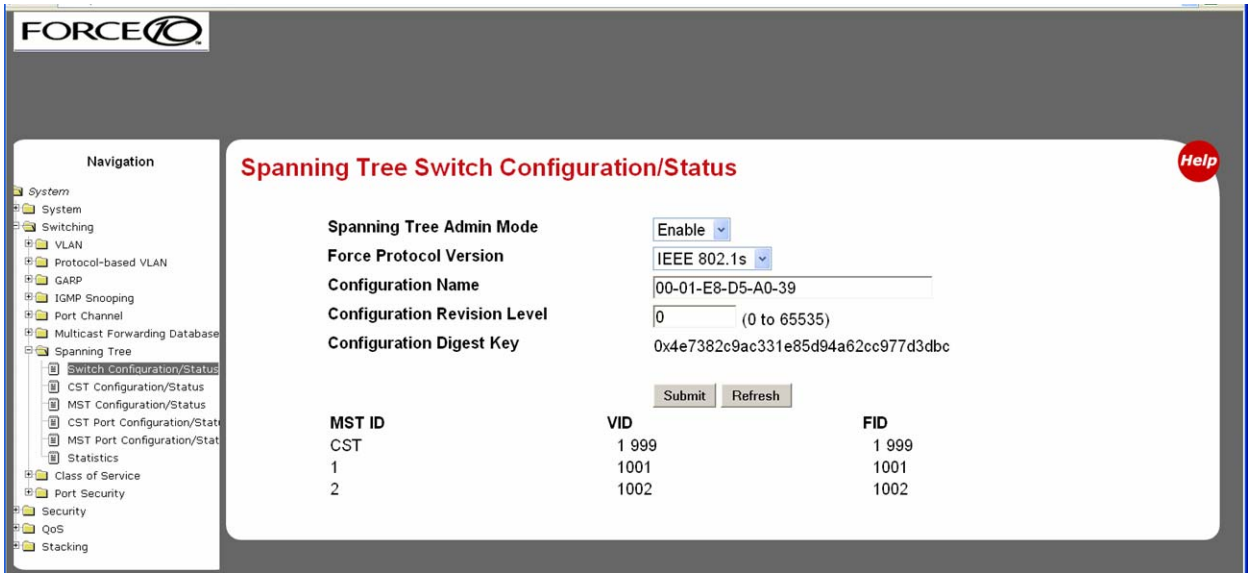


Figure 18 Spanning Tree Switch Configuration/Status Panel of the Web UI

Next, enable STP on the desired ports. To use the Web UI, select the **CST Port Configuration/Status** panel. Choose the port from the **Unit/Slot/Port** list, and then set **Port Mode** to **Enable**:

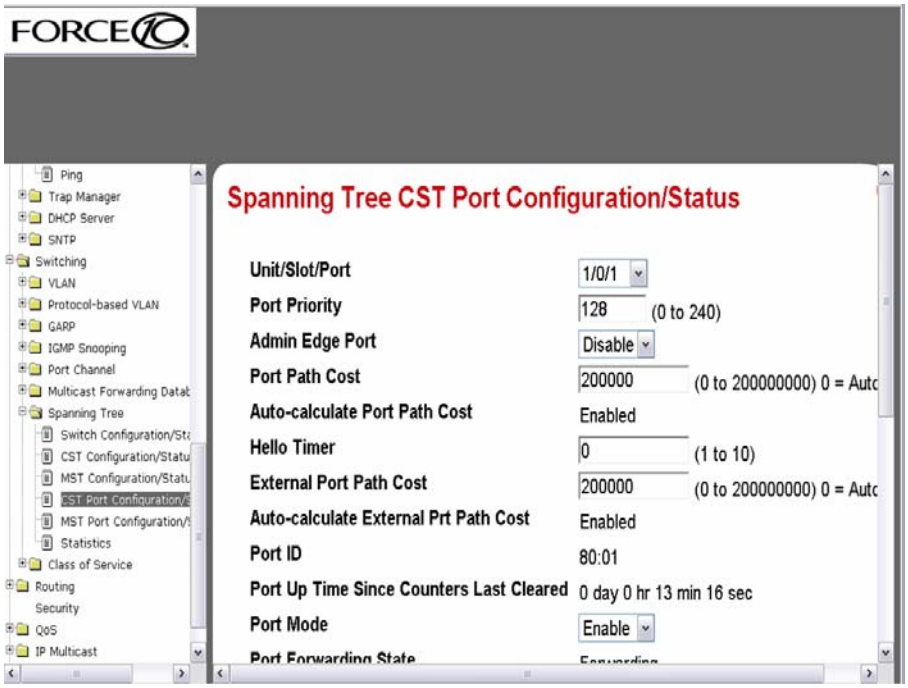


Figure 19 CST Port Configuration/Status Panel of the Web UI

Alternatively, you can use the CLI to enable STP. It is possible to enable spanning tree globally, and on all the ports with just two commands:

```
Force10 #configure
Force10 (Config)#spanning-tree
Force10 (Config)#spanning-tree port mode all
Force10 (Config)#exit
Force10 #show spanning-tree summary

Spanning Tree Adminmode.......... Enabled
Spanning Tree Version............. IEEE 802.1s
Configuration Name................ 00-01-E8-D5-A0-F7
Configuration Revision Level...... 0
Configuration Digest Key..........
0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0
No MST instances to display.

Force10 #show spanning-tree interface 0/1
Hello Time..................................... 0
Port Mode...................................... Enabled
Port Up Time Since Counters Last Cleared....... 0 day 0 hr 19 min 38 sec
STP BPDUs Transmitted.......................... 2
STP BPDUs Received............................. 593
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
```

Figure 20 Example of Entering STP Commands in CLI

For more on Spanning Tree Protocol, see the chapter Spanning Tree on page 135.

Managing Configuration and Software Files

This section contains the following major subsections, in this order:

- Important Points to Remember — Files on page 48
- Downloading and Uploading Files on page 48
- Upgrading the Software Image on page 49
- Managing the Configuration on page 55
- Using Configuration Scripts on page 58

The S-Series switch contains several discrete system management files, including a startup configuration file (“startup-config”), a running-config file, SFTOS, and a system software file (“boot code”). There are various reasons why you might want to replace one or the other. For example, for the configuration file, if you lose your password, you will need to replace the running configuration with the factory default. If you back up the startup-config file, you can copy that file to the rebooted switch to be used as the configuration on the next reload.

Note: See the Quick Start chapter in the SFTOS Command Reference, most specifically, the section “Using the Boot Menu”, for more on managing files.

Important Points to Remember — Files

- Beginning with SFTOS Version 2.3, when you save the running-config to the startup-config file, the startup-config is converted to text, if it is not already. Upgrading the software to Version 2.3 or above automatically invokes a conversion of the binary configuration file to text. The conversion also includes updating configuration statements to statements that conform to the current version.
- While you cannot cut and paste the configuration file, you can cut and paste **show run** output into a text file, and paste it in through Telnet or console.
  For a sample of the output from the **show run** output, see the **show running-config** command in the *SFTOS Command Reference Guide*, or see Displaying VLAN Configuration Information on page 194 in this guide.

Downloading and Uploading Files

Use the **copy** command (in Privileged Exec mode) to download or upload various files using TFTP or Xmodem. The following files can be uploaded from the switch:

- CLI banner (**copy nvram:clibanner**)
- error log (**nvram:errorlog**): This log is the persistent Event log. For details, see Using the Persistent Event Log on page 98.
- message log (**nvram:log**): This log is the buffered System log. For details, see Displaying System Log Files on page 97.
- script (**nvram:script** *scriptname***)**
- startup configuration (**nvram:startup-config**)
- trap log (**nvram:traplog**)

When using TFTP, the following example command shows the format for uploading from the switch.
Enter: **copy nvram:startup-config tftp://***tftp_server_ip_address/path/filename*
In place of *tftp_server_ip_address*, specify a URL for the TFTP destination. An example of *path/filename* is s50/clibanner.txt. See also Managing the Configuration on page 55.

If you use Xmodem instead, the syntax is **xmodem:***path/filename* .

Using TFTP, the following commands download files to the switch:
copy tftp://*tftp_server_ip_address/path/filename* **nvram:startup-config**
copy tftp://*tftp_server_ip_address/path/filename* **system:image**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:script**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:sslpem-root**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:sslpem-server**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:sslpem-dhweak**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:sslpem-dhstrong**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:sshkey-rsa1**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:sshkey-rsa2**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:sshkey-dsa**
copy tftp://*tftp_server_ip_address/path/filename* **nvram:clibanner**

For example: #**copy tftp://192.168.0.10/dsa.key nvram:sshkey-dsa**

For information on the SSL and SSH files listed above, see the Secure Communications folder on the S-Series Documentation and Software CD-ROM.

Points to Remember when Transferring Files

Points to remember when downloading software code or configuration files include:

- Code:
  - Overwrites existing code in flash memory
- Configuration:
  - Configuration is stored in NVRAM.
  - Active configuration is distinct from the stored configuration.
  - Changes to active configuration are not retained across resets unless explicitly saved.
  - A download replaces the stored configuration.
  - A download is stopped if a configuration error is found.
- Upload code, configuration, or logs.
- File transfer uses Xmodem or TFTP depending on platform.
- Specify the following TFTP server information.
  - IP address
  - File path (up to 31 characters)
  - File name (up to 31 characters)
- Progress of the TFTP transfer is displayed.
- Starting with SFTOS Version 2.3, you can use **dir nvram** from Privileged Exec mode to display the files stored in NVRAM.

Upgrading the Software Image

After you have set up the hardware, determine if you need a software upgrade. An S-Series switch is shipped with the base Layer 2 software installed, but you might need to install either a more recent image or the optional, extended Layer 3 image.

Note: For the migration to SFTOS Version 2.3 and above from versions below 2.3, see the Release Notes, because a software upgrade includes an automatic conversion of the binary configuration file to text.

There are two options for upgrading the software image:

- **Method 1—TFTP**: Download the image from a TFTP server, detailed below in Using TFTP to Upgrade Software on page 50.
- **Method 2—Xmodem**: A slower but simpler way to retrieve the software image is to use Xmodem. See Using Xmodem to Upgrade Software on page 53

Both the TFTP and Xmodem procedures download the image to the switch with the image filename unchanged.

If the copy process is incomplete or the copied file is corrupt, you can revert to the previous OS version, if it was intact and working. If corruption is detected in the new image before it downloads the current image into flash memory, the original image remains intact in flash. CRC fails once the image is downloaded into memory or a packet's checksum fails during download.

If the image gets corrupted in flash, the only recourse is to download a new image using Xmodem (see Using Xmodem to Upgrade Software on page 53).

Using TFTP to Upgrade Software

1. Using the CLI, gain access to the switch by logging in and issuing the **enable** command:

```
Force10
User:admin
Password:

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for
the 'normal' and 'no' command forms.  For the syntax of a particular command form,
please consult the documentation.

Force10 >enable
Password:
```

2. Set the management IP address and the gateway address as described in Setting the Management IP Address on page 41.
3. Make sure that you have a port enabled in the management VLAN. See Enabling Ports on page 40.
4. Ping the default gateway to ensure access to the server from which to download the software image.

```
Force10 #ping 10.10.1.254

Send count=3, Receive count=3 from 10.16.1.254
```

5. Ping the IP server from which you wish to download the software image:

```
Force10 #ping 10.16.1.56

Send count=3, Receive count=3 from 10.16.1.56
```

6. Load the image by using the **copy** command:

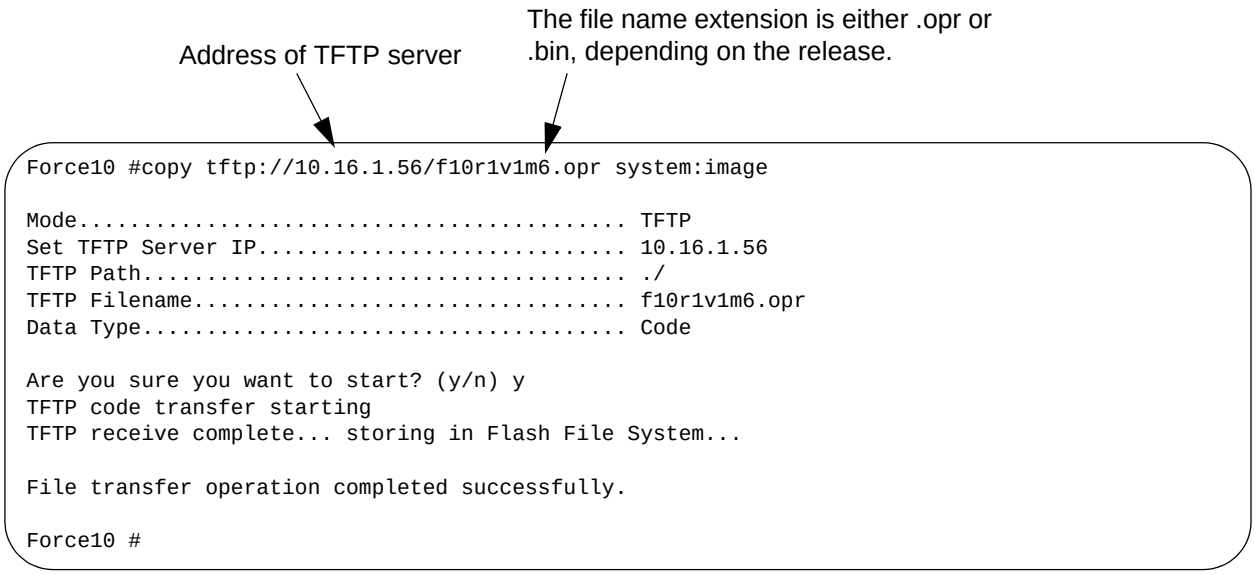


Figure 21 Downloading New Software

For details on copy command options, see Downloading and Uploading Files on page 48, above.

7. Execute one of the show commands, such as **show hardware**, **show switch**, or **show version**, that display the currently running software version:

```
Force10 #show hardware

Switch: 1

System Description..... Force10 S50
Vendor ID..... 07
Plant ID..... 01
Country Code..... 04
Date Code.....
Serial Number..... 114
Part Number.....
Revision.....
Catalog Number..... SA-01-GE-48T
Burned In MAC Address..... 00:D0:95:B7:CD:2E
Software Version..... F.2.2.1.6

Additional Packages..... Force10 QOS
                         Force10 Stacking
```

Figure 22 Displaying the Current Software Version

8. If you want to save the current configuration to NVRAM, the easy way is to enter the **write** command (no parameters; the command defaults to **write memory**.)
   An alternative is to use the **copy** command shown in the following sample:

Note: You can only save the startup config to the NVRAM (the running configuration cannot be saved to the network).

```
Force10 #copy system:running-config nvram:startup-config

This operation may take few minutes.
Management interfaces will not be available during this time.

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

Configuration Saved!
```

Figure 23 Saving the Current Configuration to NVRAM

Alternatively, if you want to restore the configuration to factory defaults (recommended by TAC when upgrading from Layer 2 Package to Layer 3 Package), see Restoring the System to the Default Configuration File on page 57.

9. Reload the switch:

```
Force10 #reload

Management switch has unsaved changes.
Would you like to save them now? (y/n) y
Configuration Saved!
Are you sure you want to reload the stack? (y/n) y

Reloading all switches.

Force10 Boot Code...Version 01.00.26 06/03/2005

Select an option. If no selection in 2 seconds then operational code will start.

1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):1

Operational Code Date: Thu Jul  7 16:37:32 2005
Uncompressing.....
                        50%                     100%
||||||||||||||||||||||||||||||||||||||||||||||||||
Attaching interface lo0...done

Adding 31485 symbols for standalone.
PCI device attached as unit 0.
PCI device attached as unit 1.
PCI device attached as unit 2.
PCI device attached as unit 3.
PCI device attached as unit 4.
PCI device attached as unit 5.
PCI device attached as unit 6.
Configuring CPUTRANS TX
Configuring CPUTRANS RX
st_state(0) = 0x0
st_state(1) = 0x2
(Unit 1)>This switch is manager of the stack.
STACK: attach 5 units on 1 cpu
```

Figure 24 Using the reload command to upgrade the OS

Using Xmodem to Upgrade Software

An alternative to using TFTP to upgrade the software image is to use the Xmodem protocol at the console port:

1. From Privileged Exec mode, enter the command **reload**.
2. You then have 2 seconds to select option **2**, as shown below in Figure 25 on page 54.
3. Then, from the boot menu, select **4** to choose the “XMODEM” option.

   Or, typically, before starting the download, users want to increase the transfer rate to the maximum. So, instead of immediately selecting 4, you would select option **2**, which accesses a menu that enables you to change the baud rate to 115200. Typically, you would then also need to modify your terminal software settings to 115200. After changing the terminal session rate to 1152000, and the connection is re-established, for example in Hyperterminal, press the ‘**?**’ key to refresh to the Boot Menu text.

```
Force10 #reload
Management switch has unsaved changes.
Would you like to save them now? (y/n) n

Configuration Not Saved!
Are you sure you want to reload the stack? (y/n) y

Reloading all switches.
Force10 Boot Code...
Version 01.00.26 06/03/2005

Select an option. If no selection in 2 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2
Boot Menu Version 01.00.26 06/03/2005
Options available
1 - Start operational code
2 - Change baud rate
3 - Retrieve event log using XMODEM (64KB).
4 - Load new operational code using XMODEM
5 - Display operational code vital product data
6 - Update Boot Code
7 - Delete operational code
8 - Reset the system
9 - Restore Configuration to factory defaults (delete config files)
[Boot Menu] 4
```

Figure 25 Example of Launching the Boot Menu to select a Code Download through Xmodem

4. After selecting option **4** for an Xmodem software transfer, use the transfer sub-menu to browse the file system for the desired software image.
5. After the transfer is complete, you can verify the current software image and save the running configuration if you want, as described above in the TFTP procedure (Using TFTP to Upgrade Software on page 50). Then issue the **reload** command, as shown in Figure 24 on page 53.

Managing the Configuration

This section contains the following major subsections, in this order:

- Clearing the Running Configuration on page 55
- Saving the Startup Configuration to the Network on page 56
- Configuring from the Network on page 56
- Restoring the System to the Default Configuration File on page 57

When the switch is booted, its configuration is managed by the startup configuration (“startup-config”) file that is stored in non-volatile memory (NVRAM). As you make configuration changes, those changes are stored in volatile system memory as the “running config” until you copy them to the startup-config. The quickest way to do that is to use the **write memory** command (executed from the Privileged Exec mode). You can also use the command **copy system:running-config nvram:startup-config**.

Beginning with SFTOS Version 2.3, making changes to the startup-config file causes that file to be stored as a text file. A major benefit of that text file, in addition to faster reboots, is that you can edit the file after you copy it to a TFTP server. You can then download the edited file to any switch to use as the startup-config file.

Caution: Beginning with Version 2.3, the following commands must be present and occur in the same relative locations in the startup-config file as if they had been automatically generated. Failure to do so will result in unpredictable behavior:

interface vlan *vlan id*
vlan configuration commands
exit
configure
stack
member commands (for example "member <unit> <switchindex>"
exit

Clearing the Running Configuration

When downloading the startup-config file to the system from a TFTP server, the file will not take effect as the startup configuration of the switch until a reboot (**reload**) is performed. However, you have the option of using the **clear config** command, followed by the **script apply startup-config** command to use the newly downloaded startup-config without rebooting the switch. For details in this chapter on using script commands, see Using Configuration Scripts on page 58.

The following example shows the **clear config** command for clearing the running-config from memory:

```
Force10 #clear config
Are you sure you want to clear the configuration? (y/n)y
Clearing configuration. Please wait for login prompt.
Force10 #
(Unit 1)>
```

Figure 26 Clearing the Running Configuration

Saving the Startup Configuration to the Network

The following is an example of how to save the startup configuration to a TFTP site on the network.

```
Force10 #copy nvram:startup-config tftp://10.16.1.56/s50_1

Mode..................................... TFTP
Set TFTP Server IP....................... 10.16.1.56
TFTP Path................................ ./
TFTP Filename............................ s50_1
Data Type................................ Config File

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

File transfer operation completed successfully.
```

Figure 27 Using the copy nvram:startup-config Command

Configuring from the Network

The following example is of installing a configuration file from the network. Beginning with SFTOS Version 2.3, you can save a startup-config file as a text file to a server, edit it, and then download it to any switch.

```
Force10 #copy tftp://10.16.1.56/s50_1 nvram:startup-config

Mode..................................... TFTP
Set TFTP Server IP....................... 10.16.1.56
TFTP Path................................ ./
TFTP Filename............................ s50_1
Data Type................................ Config

Download configuration file. Current configuration will be cleared.

Are you sure you want to start? (y/n) y
TFTP config transfer starting

TFTP download operation completed successfully.

Force10 #
(Unit 1)>                    <-------------- You are now logged off
User:
```

Figure 28 Using the copy tftp Command to Download Startup-Config

Restoring the System to the Default Configuration File

As discussed above in Clearing the Running Configuration on page 55, you can replace the running-config with the startup-config without rebooting the switch. However, if you have lost your CLI password, you might not be able to issue the necessary commands. In that case, you have the option of rebooting the the system with the factory default startup-config (recommended by TAC when upgrading from Layer 2 Package to Layer 3 Package). To do so, use the following procedure.

1. Remove and reinsert the power cord.
2. When the system reboots, select **2** to start the Boot Menu, as shown in Figure 29 on page 57.
3. Select **9** to restore the configuration to factory defaults (deletes the configuration file).

Note: Resetting the factory defaults is more powerful than the result of executing the **clear config** command, because it resets all internal values.

4. Select option **8** to reload/boot the switch.

The example in Figure 29shows the act of selecting the Boot Menu and subsequent display of it.

```
Force10 Boot Code...
Version 01.00.27 11/18/2005

Select an option. If no selection in 2 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2

Boot Menu Version 01.00.27 11/18/2005

Options available
1  - Start operational code
2  - Change baud rate
3  - Retrieve event log using XMODEM (64KB).
4  - Load new operational code using XMODEM
5  - Display operational code vital product data
6 - Update Boot Code
7 - Delete operational code
8 - Reset the system
9 - Restore Configuration to factory defaults (delete config files)
[Boot Menu] 10
```

Figure 29 Restoring the Configuration to Factory Defaults

If you have previously backed up the running-config, you can download and reapply it. See Downloading and Uploading Files on page 48 or Configuring from the Network on page 56.

Using Configuration Scripts

This section contains:

- Creating a Configuration Script on page 58
- Viewing a Configuration Script File on page 59
- Uploading a Configuration Script to a TFTP Server on page 59
- Deleting a Script on page 60
- Downloading a Configuration Script from a TFTP Server on page 60
- Applying a Configuration Script on page 61
- Listing Configuration Scripts on page 62

Configuration scripts are ‘flat’ configuration files stored in the NVRAM. Their file names are appended with the “.scr” extension.

The configuration scripts are editable text files that can be uploaded and downloaded to and from the switch and a TFTP server.

Creating a Configuration Script

One way to create a “config script” is to use a variation of the **show running-config** command:

Command Syntax	Command Mode	Purpose
show running-config <*scriptname*>**.scr**	Privileged Exec	Create a configuration script by specific name.

```
Force10 #show running-config test.scr

Config script created successfully.
```

Note: Starting with Release 2.3, you can use **show running-config startup-config** to achieve the same effect as you can with **show running-config** <*scriptname*>**.scr**. The resulting startup-config is a text file that you can save to a server and download to any switch.

Viewing a Configuration Script File

To view the config script, use the **script show** *scriptname*.**scr** command.

Command Syntax	Command Mode	Purpose
script show *scriptname*.**scr**	Privileged Exec	To view a configuration script by specific name.

```
Force10 #script show test.scr

1 : !Current Configuration:
2 : !
3 : hostname "Force10"
4 : network parms 10.10.1.33 255.255.255.0 10.10.1.254
5 : interface vlan 11
6 : !System Description "Force10 S50"
10 : !System Description F.5.6.2
...
```

Figure 30 Using the script show Command

Uploading a Configuration Script to a TFTP Server

To upload a "config script" to a TFTP server, use the **copy** command.

Command Syntax	Command Mode	Purpose
copy nvram:script *scriptname*.**scr** **tftp://***x.x.x.x*/*scriptname*.**scr**	Privileged Exec	Copies the config script from the NVRAM to a TFTP server.

```
Force10 #copy nvram:script test.scr tftp://10.16.1.56/test.scr

Mode..................................... TFTP
Set TFTP Server IP....................... 10.16.1.56
TFTP Path.....................................
TFTP Filename............................ test.scr
Data Type................................ Config Script
Source Filename.......................... test.scr

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

File transfer operation completed successfully.
```

Figure 31 Using the copy nvram:script Command

Deleting a Script

To delete a “config script”, use the **script delete** command.

Command Syntax	Command Mode	Purpose
script delete <scriptname.scr>	Privileged Exec	Deletes the named script from the switch memory.

```
Force10 #script delete test.scr

Are you sure you want to delete the configuration script(s)? (y/n)y

1 configuration script(s) deleted.
```

Downloading a Configuration Script from a TFTP Server

To download a “config script”, use the **copy** command, as in the following.

Command Syntax	Command Mode	Purpose
copy tftp://*x.x.x.x/scriptname***.scr nvram:script** *scriptname***.scr**	Privileged Exec	Downloads the named script from the TFTP server identified by the URL.

```
Force10 #copy tftp://10.16.1.56/test.scr nvram:script test.scr

Mode..................................... TFTP
Set TFTP Server IP....................... 10.16.1.56
TFTP Path.....................................
TFTP Filename............................ test.scr
Data Type................................ Config Script
Destination Filename..................... test.scr

Are you sure you want to start? (y/n) y
Validating configuration script...

hostname "Force10"

interface managementethernet
ip address 10.10.1.33 255.255.255.0
exit
management route default 10.10.1.254

interface vlan 11
<output deleted>
```

Figure 32 Using the copy tftp Command for a Script

Troubleshooting a Downloaded Script

While attempting to download a config script, the system validates the downloaded file. If the validation fails an error message like the following will appear:

```
Configuration script validation failed.
Following lines in the script may have problem:
Line 29:: permit 01:80:c2:00:00:00 any assign-queue 4
Line 30:: permit any 01:80:c2:00:00:ff assign-queue 3 redirect 0/10
Line 31:: permit 01:80:c2:00:00:ee any assign-queue 4
Line 36:: match cos 5
Line 44:: police-simple 500000 64 conform-action transmit violate-action drop
Line 45:: police-simple 500000 64 conform-action transmit violate-action drop

Total error Lines :: 6
The file being downloaded has potential problems. Do you want to save this file?
```

Figure 33 Example of a Script Validation Error Message

Applying a Configuration Script

To apply a “config script”, use the **script apply** command, as in the following.

Command Syntax	Command Mode	Purpose
script apply *scriptname*.**scr**	Privileged Exec	To do

```
Force10 #script apply test.scr

Are you sure you want to apply the configuration script? (y/n)y

The system has unsaved changes.
Would you like to save them now? (y/n) n

Configuration Not Saved!

hostname "Force10"

interface managementethernet
ip address 10.10.1.33 255.255.255.0
exit
management route default 10.10.1.254

interface vlan 11
exit
exit
Configuration script 'test.scr' applied.
```

Figure 34 Using the script apply Command

Applying a configuration script on a machine with certain previously configured features may result in an error. This is because the syntax for entering the configuration mode that allows for editing the feature may be different from the syntax that exists in the configuration (and was used to create the feature initially).

Failure to apply a config script can be resolved by one of the following solutions:

- Issue the **clear config** command before applying the script.

Note: Do not issue the **clear config** command if you telnet into the system, otherwise you will lose contact with the system. This command should be issued at the console port.

- Edit the script to use the proper syntax to edit the structure (ACL, map etc.).
- Edit the script by adding the **no** form of a command to delete a feature, then add a command to reconfigure the same feature.

Listing Configuration Scripts

The **script list** command lists the configured scripts in a system:

```
Force10 #script list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
test.scr                                2689

1 configuration script(s) found.
2045 Kbytes free.

Force10 #
```

Figure 35 Using the script list Command

Displaying Logs

The switch maintains four logs:

- Persistent — saved on switch reset
  - — Use the command **show logging**.
- Messages – system trace information, cleared on switch reset
  - — Use the command **show logging buffered**.
- Logging hosts
  - — Use the command **show logging hosts**.
- Traps – enabled trap events, cleared on switch reset
  - — Use the command **show logging traplogs**.

For details on the logs and logging, see the chapter System Logs on page 95. See also the System Log chapter in the *SFTOS Command Reference*.

Chapter 3 Using the Web User Interface

This chapter contains these major headings:

- Accessing the Web User Interface on page 65
- Command Buttons on page 67
- Enabling and Using Java Mode on page 69
- Using the Web UI for Common Functions on page 70

SFTOS provides a Web User Interface (Web UI) that is almost as powerful as the SFTOS Command Line Interface (CLI), and, in some ways, is more powerful. For example, the Web UI can display the entire forwarding database, while the CLI only displays 10 entries starting at specified addresses. On the other hand, some tasks are only available through the CLI. The CLI and Web UI can be used together to provide symbiotic control and feedback.

For new users, the Web UI is much more useful, partly because it contains a navigation panel that displays a tree structure of all the panels. If you traverse that tree systematically, you can be assured of completing the essential configuration tasks.

To use the Web UI, you must first create a management IP address for the switch (see Setting the Management IP Address on page 41) and then enable the Web UI with the CLI command **ip http server** (see Enabling and Using the SFTOS Web User Interface on page 42).

Access to the Web UI is limited to configured users. You can configure users through the CLI or the Web UI. Configuring users through the CLI is also described in the Getting Started chapter (see User Management on page 38).

The Security chapter (see Enabling SSL/HTTPS on page 131) contains details on enabling an HTTPS secure server.

Accessing the Web User Interface

1. Launch a supported Web browser. The Web browser must support:
    - HTML version 4.0, or later
    - HTTP version 1.1, or later
    - JavaScript(TM) version 1.2, or later
2. Enter the IP address of the switch in the Web browser address field.

3. When the Login panel is displayed, click the **Login** button.
4. If a username with password is required, a second login page displays. Enter the appropriate username and password, as discussed above.

   After a successful login, the Navigation tree is displayed in the left frame, and the System Description panel is displayed in the right frame, as shown below.

   Notice also the large red Help button on the right, which provides context help for the selected panel.

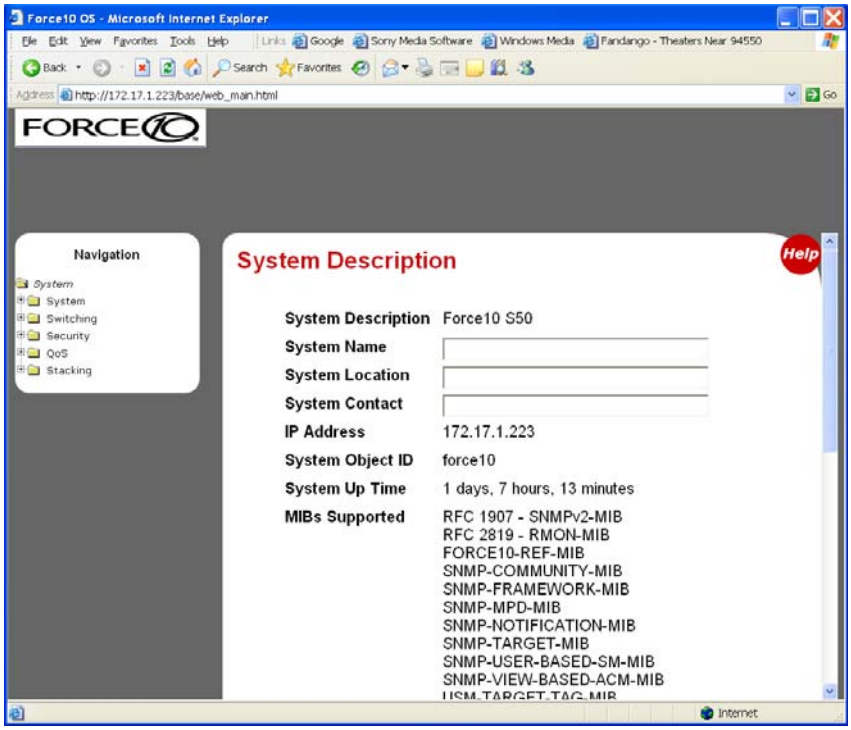


Figure 36 System Description Panel of the Web UI

5. Select a panel from the expandable Navigation tree. The corresponding panel displays in the right-hand frame. For example, the following screenshot shows that the Inventory Information panel opens when you click the Inventory Information node in the tree.

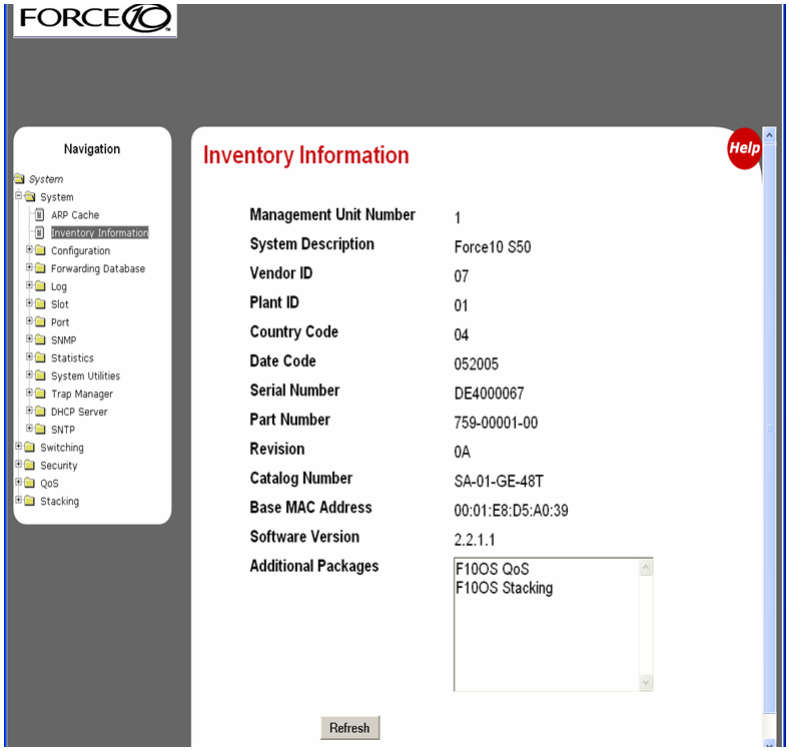


Figure 37 Inventory Information Panel of the Web UI

Command Buttons

The following command buttons are used throughout the Web UI:

Save—Implements and saves the changes you just made. Some settings may require you to reset the system in order for them to take effect.

Refresh—The Refresh button that appears on Web UI panels refreshes the data on the panel.

Conversely, if you make a change through the CLI, clicking **Refresh** on the affected panel populates the settings changed through the CLI to the panel. The exception is that, if you use the CLI to change the user name through which you are connected to the Web UI, you will need to log in again.

Submit—Sends the updated configuration data from the panel to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Other buttons include the familiar down-arrow for the list box, Clear, Clear Counters, Delete, and Reset.

Some panels display different fields after you enter data in them. For example, as shown below in the before and after images of the the SNMP Community Configuration panel (Figure 38 on page 68 and Figure 39 on page 68, respectively), when you click **Submit**, the panel adds a Delete button and the configuration data that you entered on the panel. When you click **Delete**, the configuration data that you entered is removed.

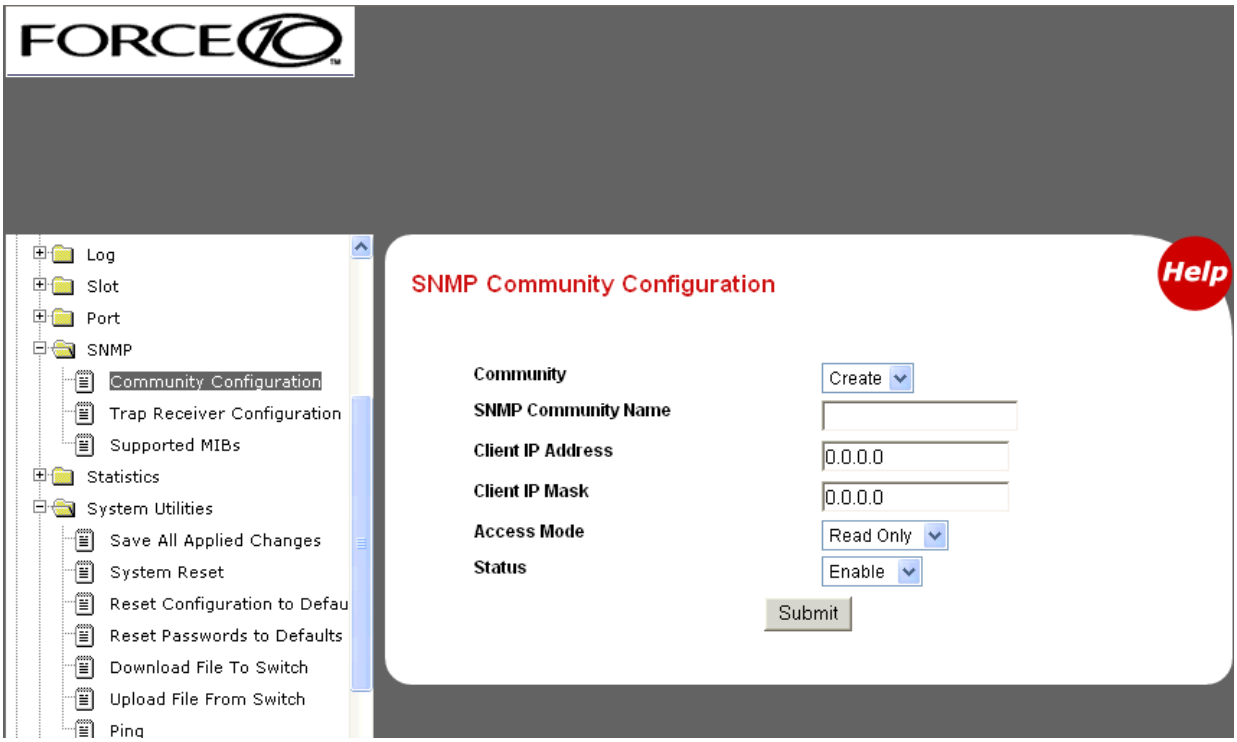


Figure 38 SNMP Community Configuration Panel before Adding a Configuration

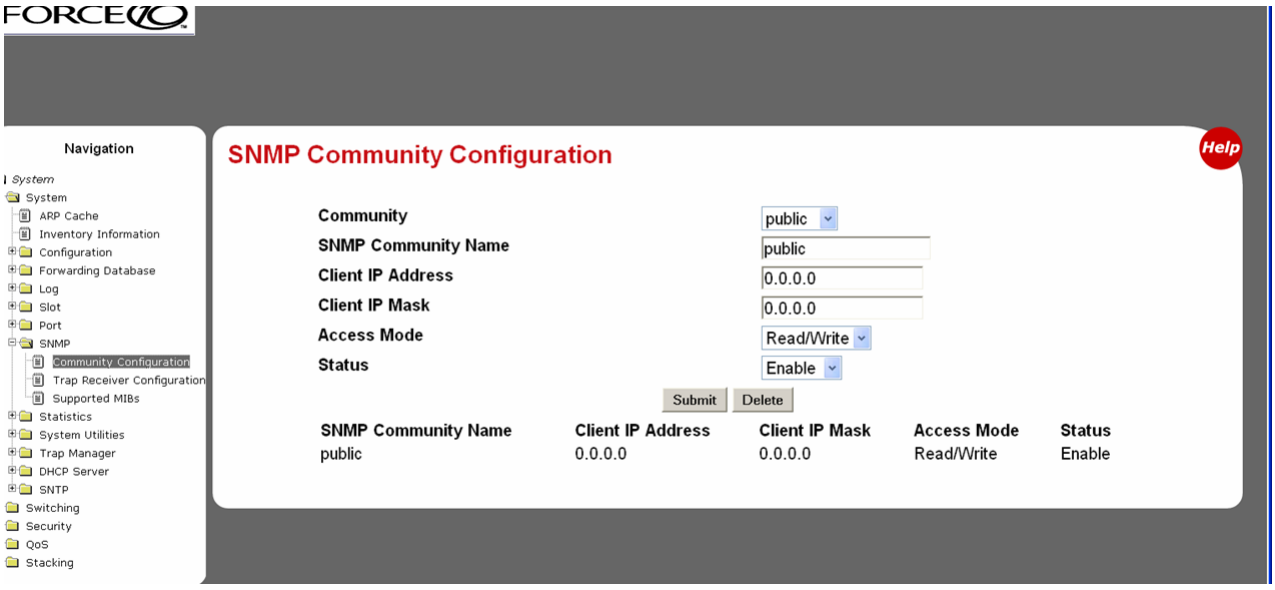


Figure 39 SNMP Community Configuration Panel after Adding a Configuration

Enabling and Using Java Mode

When you enable Java mode in SFTOS, a switch navigation icon appears at the top of the Web UI panels (Your Web browser must have the JRE plugin installed, v.2.5.1.10 or higher). You can click any port on the icon to access a menu of port-specific configuration panels. For example, if you click the Service Port (Management Port) icon, the Service Port Configuration panel displays (Figure 40).

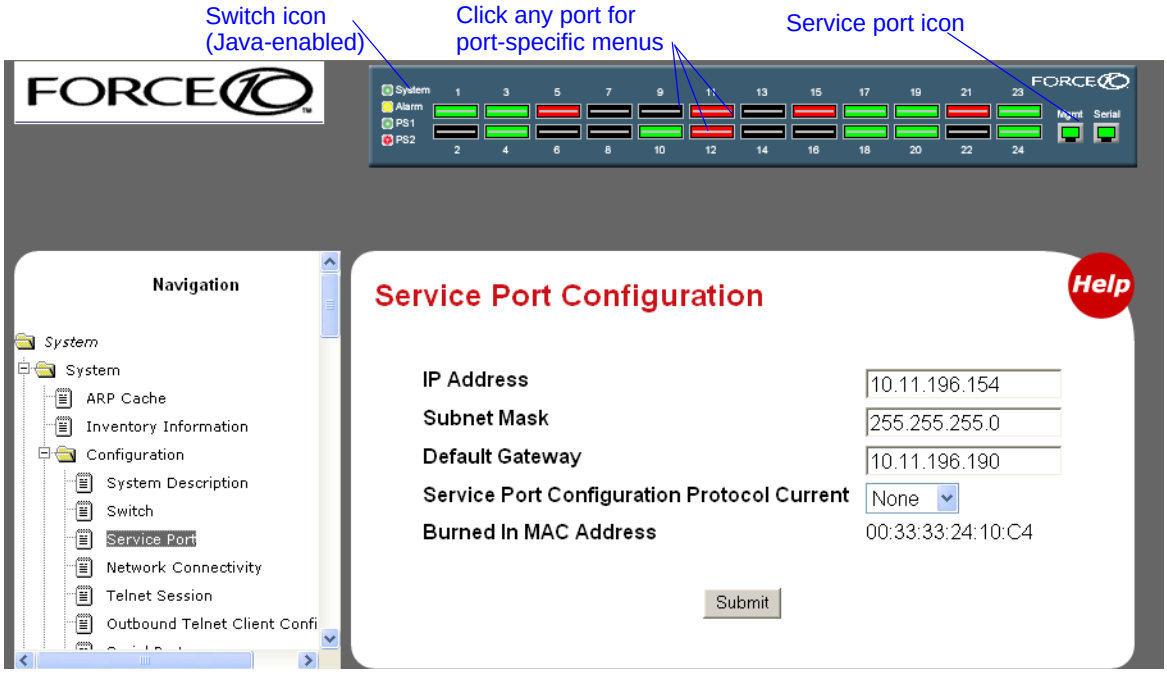


Figure 40 Switch Navigation Icon with Service Port Configuration Panel

Figure 41 shows the interactive components of the switch navigation icon.

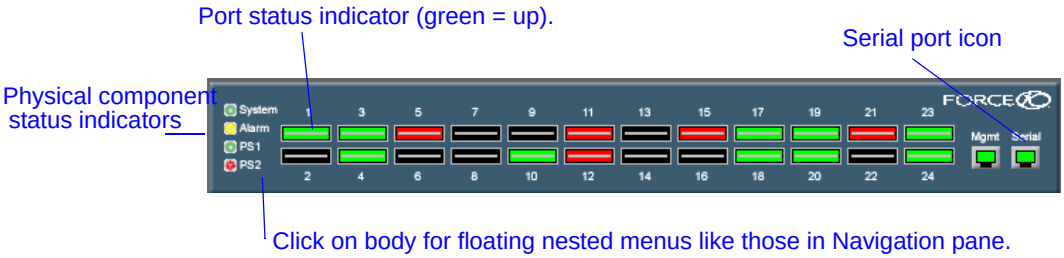


Figure 41 S2410 Switch Navigation Icon

Enabling Java Mode

To enable Java mode, use the Network Connectivity Configuration panel (**System** >> **Configuration** >> **Network Connectivity Configuration**) of the Web UI to select **Enable** in the Java Mode field (Figure 42).

Alternatively, in the CLI, execute the command **ip http javamode enable** from Global Config mode.

To disable Java mode, select Disable in the Java Mode field of the Network Connectivity Configuration panel, or execute the command **no ip http javamode enable**.

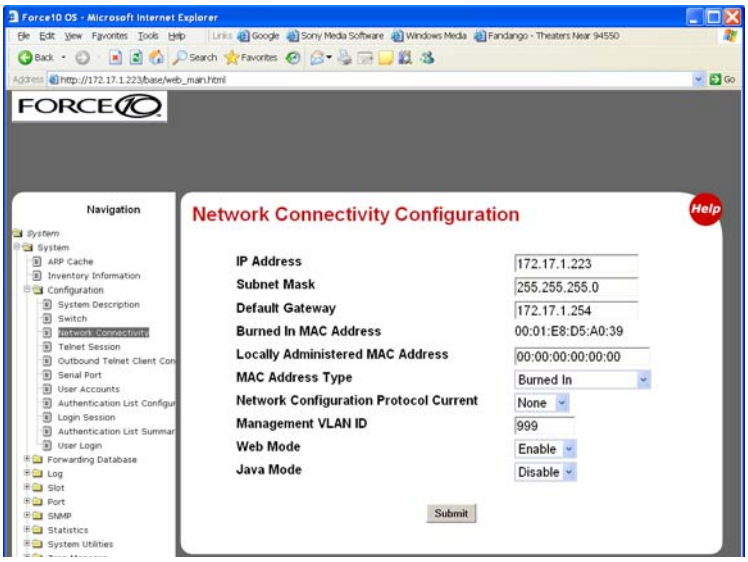


Figure 42 Network Connectivity Configuration Panel of the Web UI

Using the Web UI for Common Functions

This section contains:

- Using the Web UI to Access Information on page 70
- Using the Web UI to Configure QoS on page 72
- Using the Web UI for Switch Configuration Functions on page 72

Note: The screenshots in this section are samples to show you how easy it is to use the Web UI. The screenshots do not show recommended configuration information or sequences. Use the context-sensitive online help provided with the Web UI for detailed explanations on using the fields on the panels.

Using the Web UI to Access Information

The Web UI has many information panels. As already exemplified in Figure 36, “System Description Panel of the Web UI,” on page 66 and Figure 37, “Inventory Information Panel of the Web UI,” on page 67, they generally provide the static information that you can access through **show** commands in the CLI.

Typically, the configuration panels also contain status information, as shown in the following sections.

The Statistics group of panels contains a robust set of data. For example, as shown in Figure 43, the Port Detailed Statistics panel contains the long report that the **show interface ethernet** *u/p* command generates in the CLI.

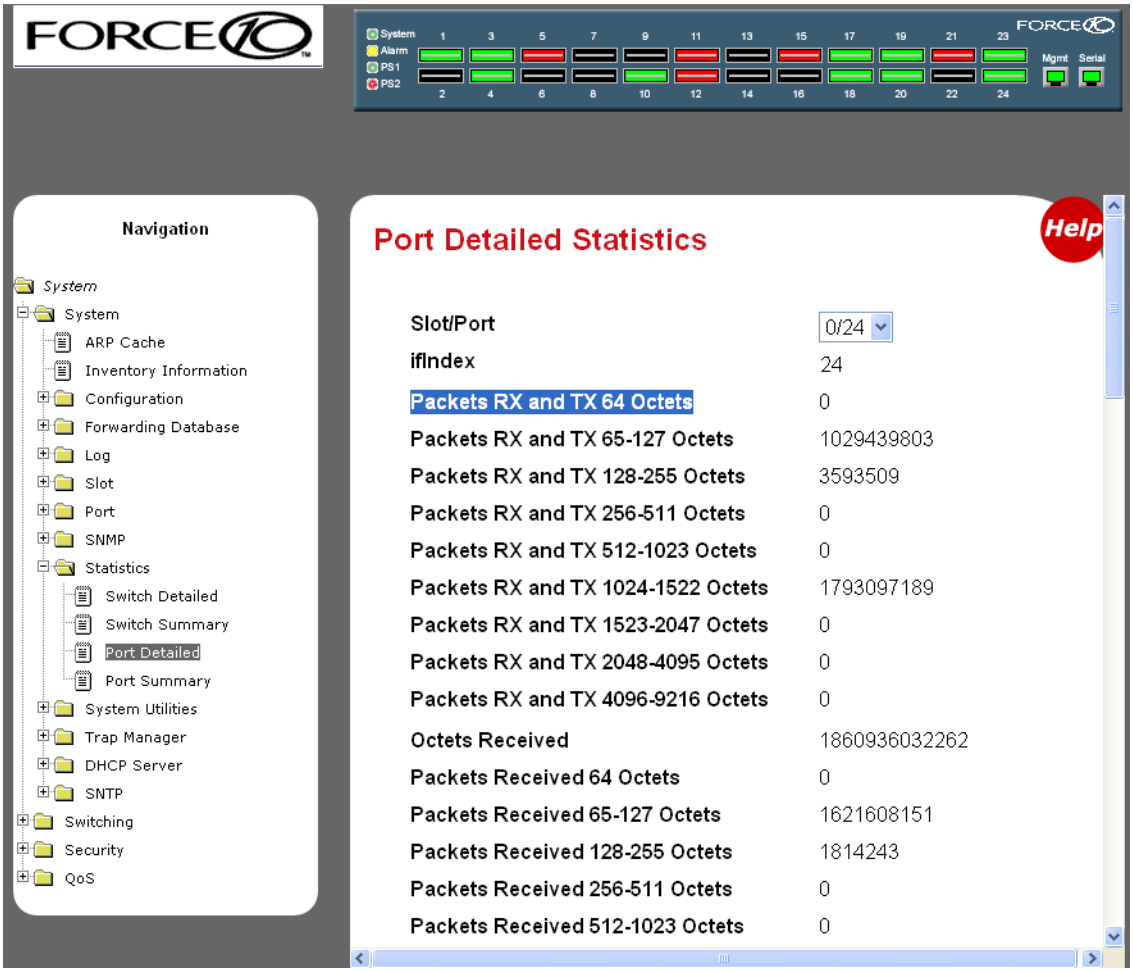


Figure 43 Port Detailed Statistics Panel of the Web UI

Figure 44 shows a sample of the Port Summary Statistics panel.

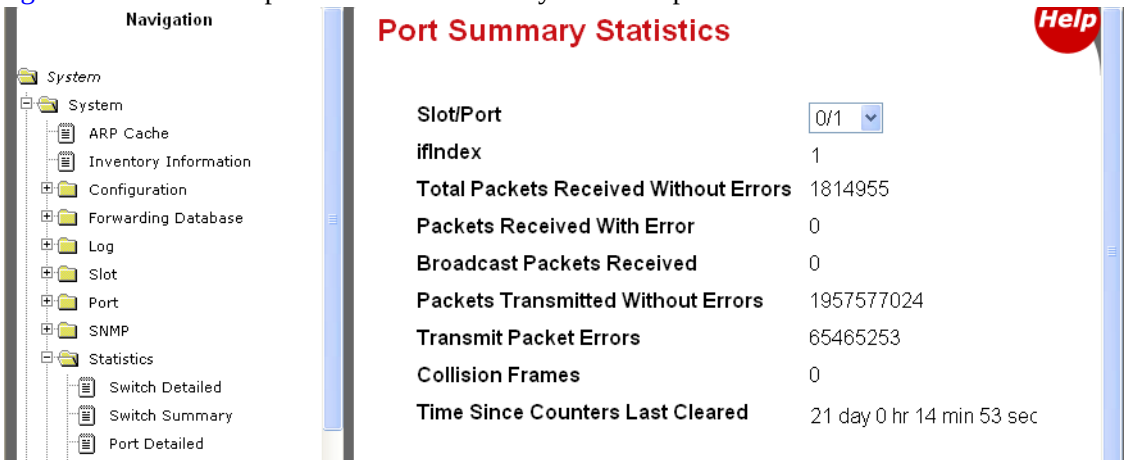


Figure 44 Port Summary Statistics Panel of the Web UI

Using the Web UI to Configure QoS

This section is the Web UI analog to the chapters in this guide on Quality of Service (QoS), including Access Control Lists (see Access Control Lists on page 171) and Class of Service (see Quality of Service on page 169). See also the Quality of Service (QoS) chapter in the *SFTOS Command Reference*.

The Web UI provides configuration and status panels for:

- Layer 2 Access Control Lists on page 72
- Differentiated Services on page 72

Layer 2 Access Control Lists

To create a Layer 2 ACL, you follow the same sequence as described above for IP ACL configuration, except that you move down the navigation tree onto the MAC Access Control Lists branch. Create an ID for the new ACL, create rules, and then use the ACL Interface Configuration panel (Figure 45) to assign one or more ACLs to the selected port.

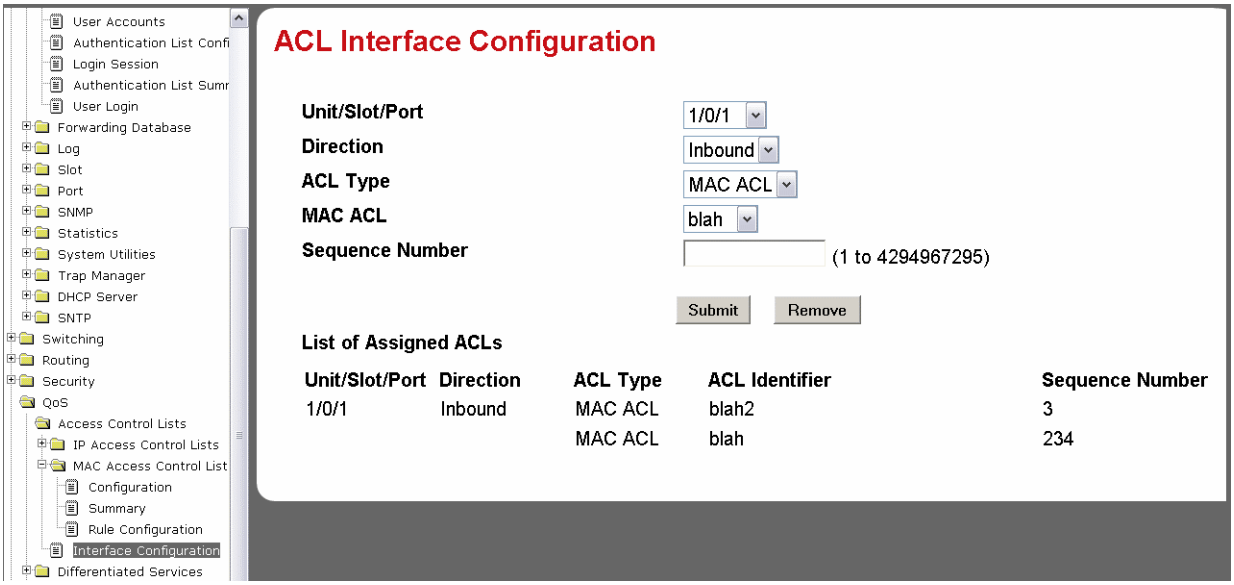


Figure 45 ACL Interface Configuration Panel of the Web UI

Differentiated Services

Note: DiffServ is not included in SFTOS 2.4.1, so that part of the Web UI is not enabled.

Using the Web UI for Switch Configuration Functions

This section contains these examples:

- Broadcast Storm Recovery on page 73
- Port Configuration on page 74

- Spanning Tree Protocol on page 74

See also, in this chapter, Using the Web UI to Configure QoS on page 72 and Using the Web UI for Security Configuration on page 76. See also the Web UI panels in Using the Web UI to Configure SNTP on page 92 in the Management chapter.

Broadcast Storm Recovery

For broadcast storm recovery, the Switch Configuration panel of the Web UI provides the equivalent of using the [**no**] **storm-control broadcast** command.

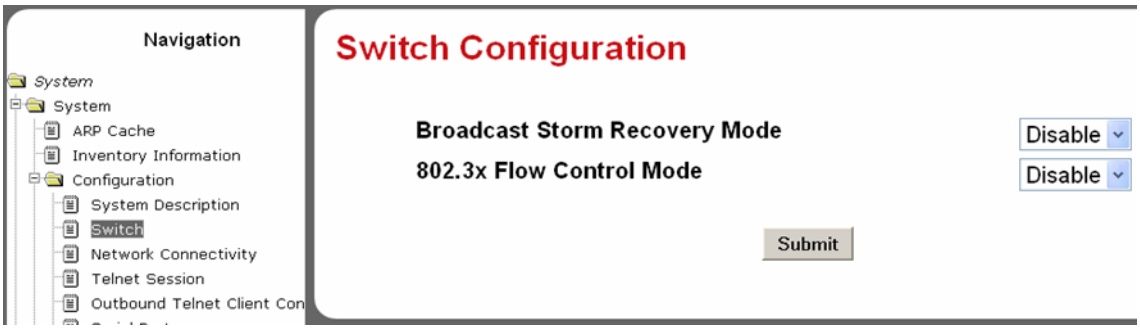


Figure 46 Switch Configuration Panel of the Web UI

Port Configuration

For port configuration, use the Port Configuration panel of the Web UI (Figure 47) to select all ports or a particular port, and then perform one or more configuration functions at one time, such as setting maximum frame size, and enabling admin mode, traps, STP, or LACP.

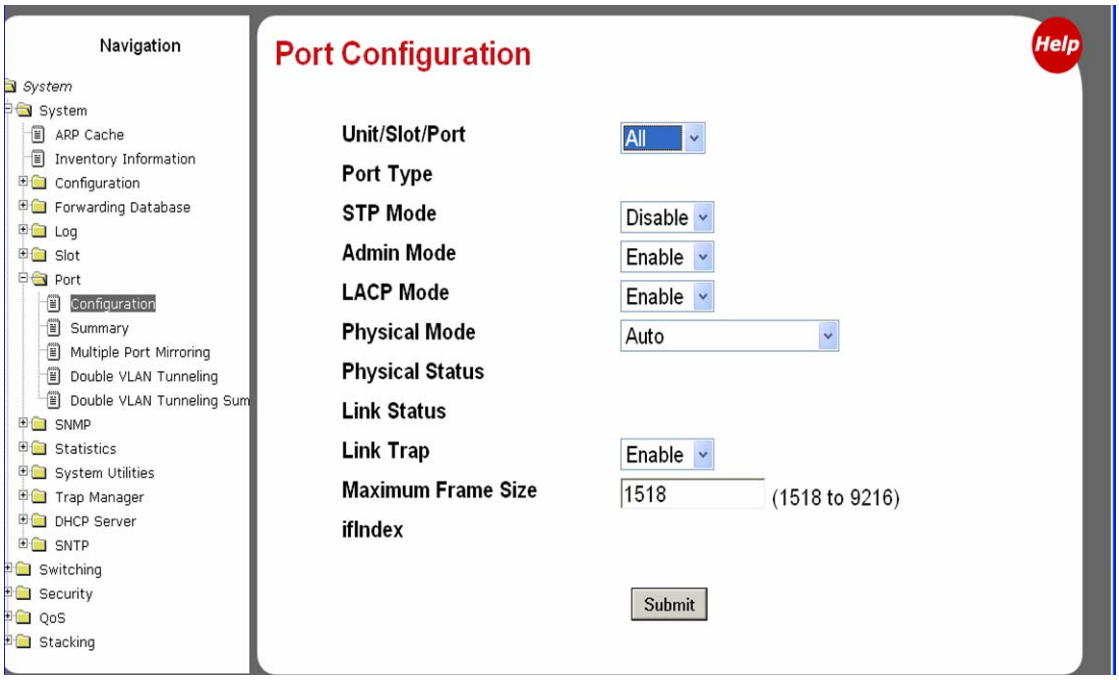


Figure 47 Port Configuration Panel of the Web UI

Spanning Tree Protocol

To use the Web UI to enable and configure Spanning Tree protocol (STP), first enable STP on the Spanning Tree Switch Configuration/Status panel (Figure 18 on page 46). The panel provides the functionality of the CLI command [**no**] **spanning-tree port mode all**.

Then, to configure STP on particular ports, use the Spanning Tree CST Port Config/Status panel (Figure 19 on page 46), as described in the Getting Started chapter in Enabling Spanning Tree Protocol on page 46.

The Spanning Tree MST Configuration/Status panel (Figure 48) and the Spanning Tree MST Port Configuration/Status panel (Figure 49) provides the equivalent functionality of these CLI commands:

[**no**] **spanning-tree port mode**
[Disable] enable administrative state for the port.

[**no**] **spanning-tree mst** *mstid* **cost** {*1-200000000* | **auto**}
[Reset] set the path cost for this port for the MST instance, or for the CST if the mstidis 0. Auto-set the cost based on the link speed.

[**no**] **spanning-tree mst** *mstid* **port-priority** *0-240*
[Reset] set the port priority for this port for the MST instance, or for the CST, in increments of 16.

[**no**] **spanning-tree edgeport**
[Reset] set a port as an edge port within the CST.

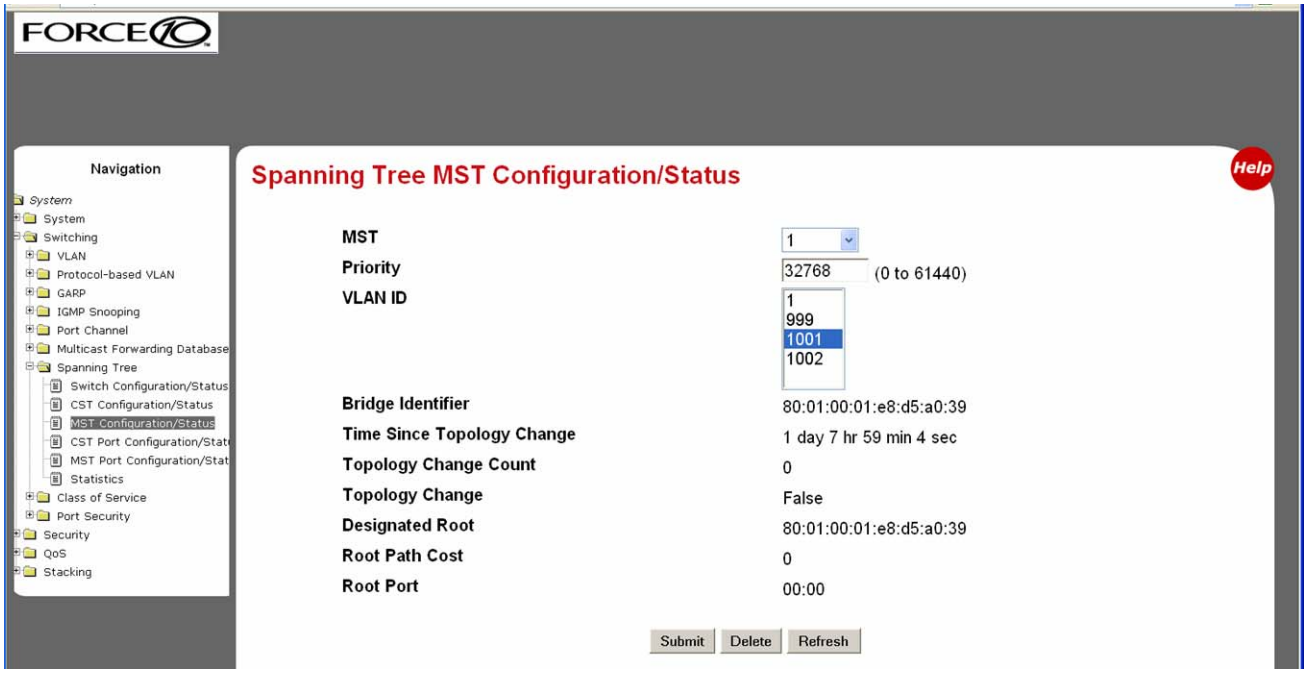


Figure 48 Spanning Tree MST Configuration/Status Panel of the Web UI

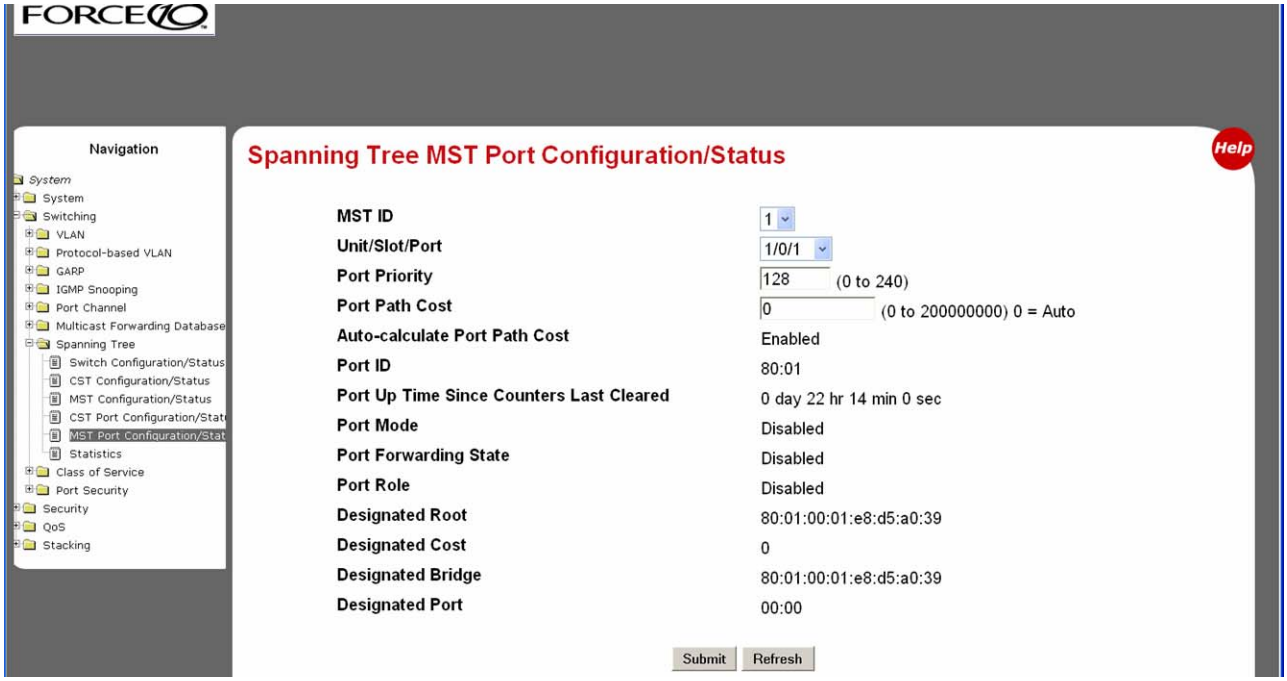


Figure 49 Spanning Tree MST Port Configuration/Status Panel of the Web UI

For more on STP, see the chapter Spanning Tree on page 135.

Using the Web UI for Security Configuration

The Switching branch of the Navigation tree on the Web UI contains the Port Security branch, which provides panels for port-level traffic security configuration. In addition, the Security branch provides configuration panels for local security (user access on a per-port basis), RADIUS, Secure Shell (SSH), and Secure Sockets Layer (SSL).

The following screenshots provide a sample of the kinds of configuration panels available for security.

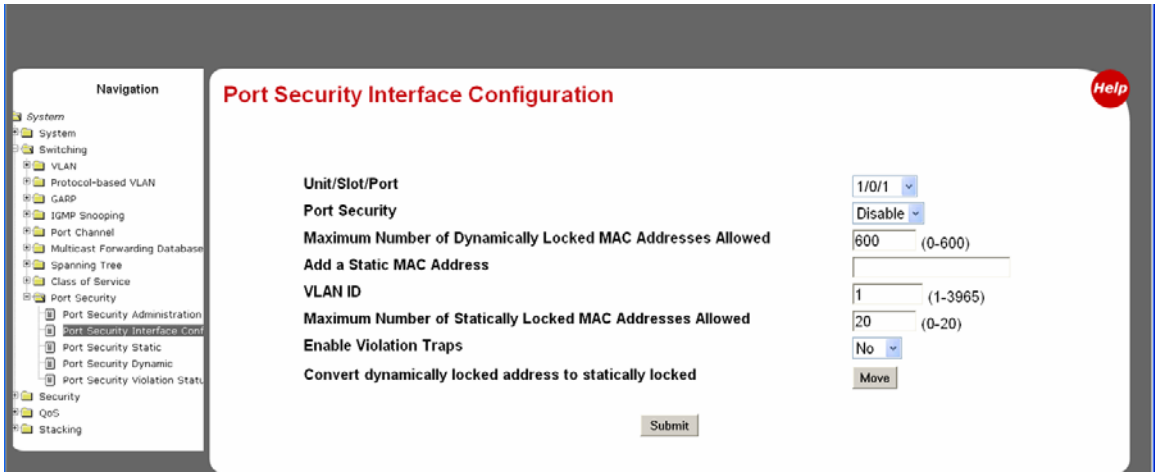


Figure 50 Port Security Interface Configuration Panel of the Web UI

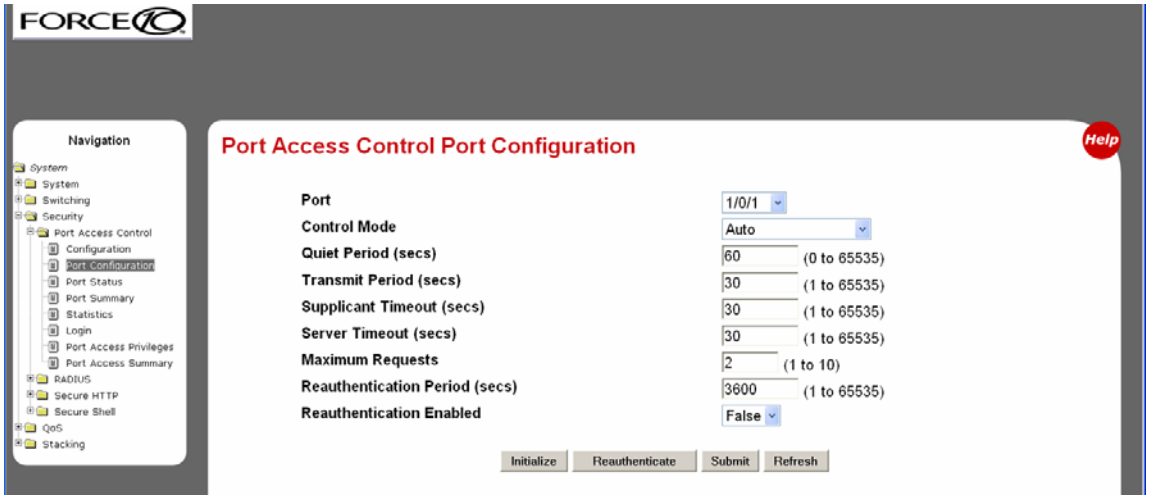


Figure 51 Port Access Control Port Configuration Panel of the Web UI

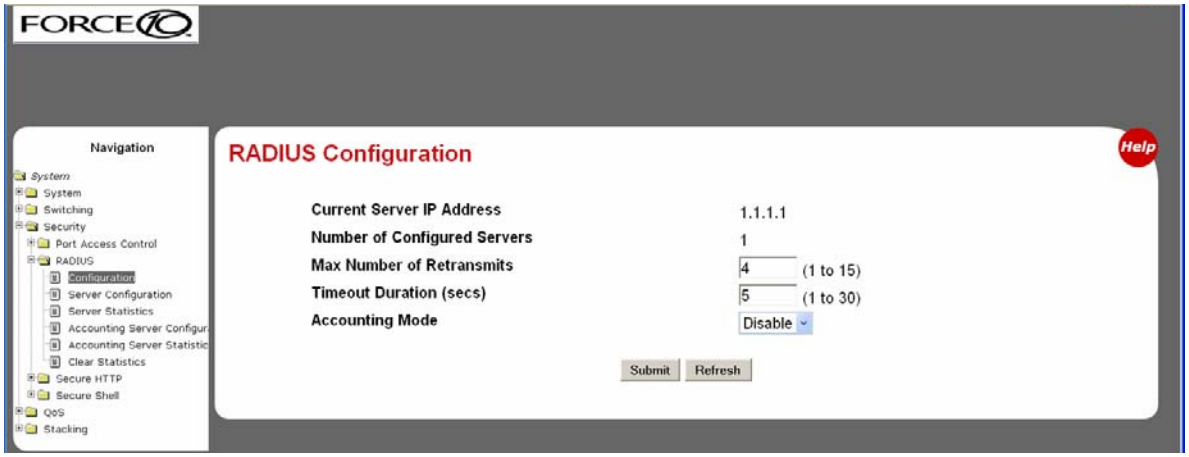


Figure 52 RADIUS Configuration Panel of the Web UI

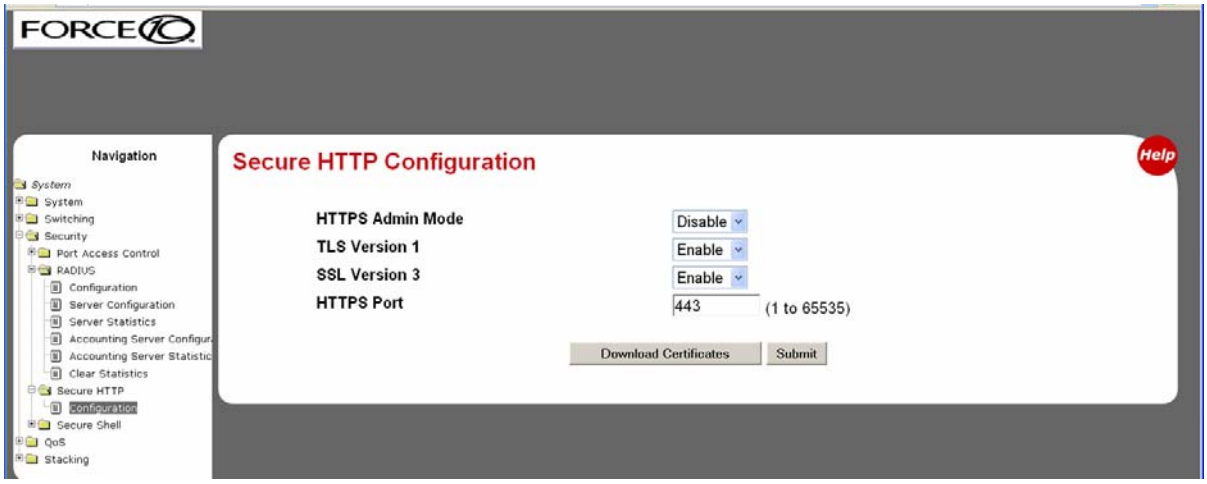


Figure 53 Secure HTTP Configuration Panel of the Web UI

Figure 53 shows the Secure HTTP Configuration panel, with HTTPS Admin Mode enabled, after the user has downloaded the SSL certificates. See Enabling SSL/HTTPS on page 131.

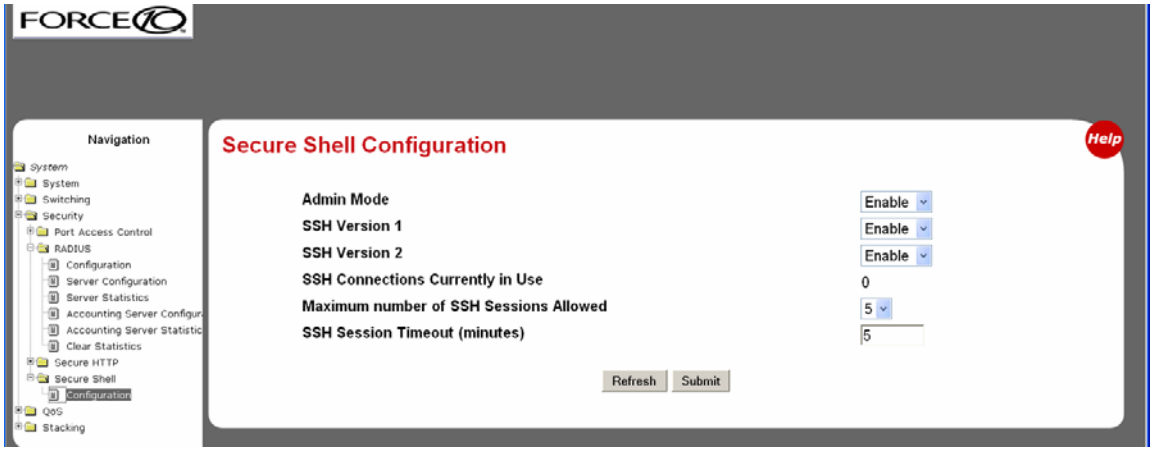


Figure 54 Secure Shell Configuration Panel of the Web UI

For more on SSL, SSH, and RADIUS configuration, see the chapter Providing User Access Security on page 121.

Chapter 4 Management

This chapter covers the following management tasks:

- Creating and Changing Management IP Addresses
- Configuring the Ethernet Management Port
- Changing the Management VLAN from the Default on page 83
- Verifying Access to the Management VLAN on page 84
- Verifying Management Port Connectivity on page 85
- Setting Stack Management Preferences on page 85
- Setting the Host Name Prompt on page 85
- Restoring the Configuration to Factory Defaults on page 85
- Setting up SNMP Management on page 87
- Setting up Simple Network Time Protocol (SNTP) on page 90

Creating and Changing Management IP Addresses

The S2410 is the only S-Series model to also have an Ethernet port dedicated to management (in addition to the console port and member ports of the management VLAN). The port is labeled “10/100 Ethernet” on the switch. The CLI refers to it as the “service port”. This guide refers to it formally as the *Ethernet Management port*. See Configuring the Ethernet Management Port on page 82.

You can configure separate IP addresses for the management VLAN (see Changing the Management VLAN from the Default on page 83) and for the Ethernet Management port, and you can access them independently at the same time to manage the switch, although doing so is obviously going to expose the switch to conflicting instructions, so it is inadviseable.

Because the Ethernet Management port is unique to the S2410, this guide and the *SFTOS Command Reference* inherit some references to the “management IP” and similar concepts without taking into consideration that the S2410 supports two “management IP” addresses.

You can use either or both the Ethernet Management port and the management VLAN to access the switch through Telnet, SNMP, or the Web UI.

Configuring the Ethernet Management Port

You have the option of using the **serviceport protocol** command to acquire an IP address for the Ethernet Management port through the Bootp protocol or the DHCP protocol. Alternatively, you can use the command of **none**, and then use the **serviceport ip** command to specify the IP address, subnet mask, and gateway.

Command Syntax	Command Mode	Purpose
serviceport protocol {**none** | **bootp** | **dhcp**}	Global Config	Specify the network configuration protocol to be used (Bootp or DHCP) for configuring access to the Ethernet Management port. Alternatively, leave the default at **none** to require the Ethernet Management port to be manually configured with IP information.
serviceport ip *ipaddr netmask* [*gateway*]	Global Config	Manually configure the IP address, IP subnet mask, and default IP gateway of the Ethernet Management port (service port).
show serviceport	Privileged Exec	Verify the Ethernet Management port configuration and status.

Example of Configuring the Ethernet Management Port

```
(Force10 S2410) (Config)#serviceport ip 10.11.197.177 255.255.0.0 10.11.197.190
(Force10 S2410) (Config)#exit
(Force10 S2410) #show serviceport

IP Address..................................... 10.11.197.177
Subnet Mask.................................... 255.255.0.0
Default Gateway................................ 10.11.197.190
Service Port Configured Protocol Current.......... None
Burned In MAC Address.......................... 00:01:E8:99:99:9A
Link Status.................................... Up
```

Figure 55 Example of Configuring the Ethernet Management Port

Changing the Management VLAN from the Default

The procedure for creating the IP address for the management VLAN is provided in Setting the Management IP Address on page 41 in the Getting Started chapter. The following example shows the use of that procedure:

```
Force10 (Config)#management route default 10.10.1.254
Force10 (Config)#interface managementethernet
Force10 (Config-if-ma)#ip address 10.10.1.251 255.255.255.0
Force10 (Config-if-ma)#exit
Force10 (Config)#exit
Force10 #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....................................... Disable
Java Mode...................................... Disable
```

Figure 56 Creating the Management Port IP Address

As stated in Setting Up a Management VLAN on page 44 in the Getting Started chapter, the default management VLAN is the default VLAN 1, so, when you configure the management IP interface (see Creating and Changing Management IP Addresses on page 81), any port that is part of the default VLAN will carry management traffic.

On first startup, the default VLAN 1 includes every port (although, by default, all ports are shut down until you enable them—see Enabling Ports on page 40.) If you want to change the management VLAN from the default VLAN to another VLAN, create the new VLAN (see Creating a Simple Configuration using VLANs and STP on page 44), and then use the following command sequence and example as your guide.

Step	Command Syntax	Command Mode	Purpose
1	**show vlan id** *vlan-id*	Privileged Exec	Inspect the VLAN that you want to assign as the management VLAN.
2	**interface managementethernet**	Global Config	Access Interface ManagementEthernet mode.
3	**vlan participation** *vlan-id*	Interface ManagementEthernet	Select a VLAN to act as the management VLAN. The VLAN number, designated in *vlan-id*, must be from 1 to 3965. **Note:** If you set the management VLAN to a VLAN that does not exist, there is no error message.

4	**show interface managementethernet**	Privileged Exec	Verify the management VLAN and other management settings.

In the following example, we create and name VLAN 5, add one port to it (you can add more), and then designate the VLAN as the management VLAN.

```
Force10 (Config)#interface vlan 5
Force10 (conf-if-vl-5)#name management_vlan
Force10 (conf-if-vl-5)#interface 0/43
Force10 (conf-if-vl-5)#exit
Force10 (Config)#interface managementethernet
Force10 (Config-if-ma)#vlan participation 5
Force10 (Config-if-ma)#exit
Force10 (Config)#
```

Figure 57 Changing the Management VLAN from the Default

Verifying Access to the Management VLAN

It is possible to set the management VLAN to a VLAN that does not exist. If you cannot reach anything from the management address, inspect the management VLAN with the commands **show interface managementethernet** or **show running-config**, to inspect the management IP settings, as shown in Figure 58.

```
Force10 #show interface managementethernet

IP Address..................................... 192.168.0.50
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 192.168.0.11
Burned In MAC Address.......................... 00:01:E8:0D:30:9A
Locally Administered MAC Address............... 00:00:00:00:00:00
MAC Address Type............................... Burned In
Network Configuration Protocol Current......... None
Management VLAN ID............................. 5
Web Mode....................................... Disable
Java Mode...................................... Disable
```

Figure 58 Verifying Management Port Network

Verifying Management Port Connectivity

```
Force10 #ping 192.168.0.100
Send count=3, Receive count=3 from 192.168.0.100 Verify management port connectivity
```

Figure 59 Verifying Management Port Connectivity

Setting Stack Management Preferences

Note: S2410 models do not support stacking.

Setting the Host Name Prompt

If you have more than one individually managed S-Series switch, you can differentiate them by creating a unique CLI host name prompt for each switch. Use the **hostname** command, in Global Config mode, to edit the prompt, as shown in Figure 60:

```
Force10 (Config)#hostname Force10_S2410
Force10_S2410 (Config)#
```

Figure 60 Setting the Host Name

The host name is case-sensitive and can be up to 64 characters in length.

Restoring the Configuration to Factory Defaults

Note: If you reset the switch to factory defaults while you access the switch by a Telnet connection, you lose connectivity to the switch.

Restoring S-Series switches to the factory default settings is useful when:

- You upgrade from the Layer 2 Package (switching) to the Layer 3 Package (routing)
- You lose the system passwords.
- You want to remove an undesirable configuration.
- The configuration has become very complex.
- You want to move a switch from one network to another.

Before you reset the switch to factory defaults, consider backing up your configuration, which you can do through one of these means:

- Back up your configuration on a TFTP server.
- Copy your configuration to a text file.
- Copy the configuration locally on the flash memory device.

To reset an S-Series switch to factory defaults, you need access to the switch console through either a physical console or a Telnet connection.

1. If you have lost your password, you must disconnect and reconnect the power cord.
   Or
   If you have your password, execute the **reload** command from the Exec Privilege mode.

   When the switch starts to reload, the following text appears at the console:

```
Reloading all switches.
Force10 Boot Code...
         Version 01.00.26 06/03/2005
Select an option. If no selection in 2 seconds then operational code will start.
1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2
```

Figure 61 Rebooting

2. When the text above appears, you have two seconds to enter **2** (as shown) and then press **Enter**. If you are not fast enough, the router will boot normally.

   If you are successul, the following menu appears:

```
Boot Menu Version 01.00.26 06/03/2005

Options available
         1 - Start operational code
         2 - Change baud rate
         3 - Retrieve event log using XMODEM (64KB).
         4 - Load new operational code using XMODEM
         5 - Display operational code vital product data
         6 - Update Boot Code
         7 - Delete operational code
         8 - Reset the system
         9 - Restore Configuration to factory defaults (delete config files)
         [Boot Menu]
```

Figure 62 Boot Menu

3. Select option **9** to delete the current configuration, including any admin and enable passwords.
4. Select option 8 to restart the system. When the switch finishes rebooting, you can configure the router from scratch.

For other methods of managing running-config and system-config files, see Managing the Configuration on page 55.

Setting up SNMP Management

Simple Network Management Protocol (SNMP) communicates management information between SNMP-based network management stations and SNMP agents in the switch. S-Series systems support SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. SFTOS sends SNMP traps, which are messages informing network management stations about the network.

SFTOS supports up to six simultaneous SNMP trap receivers. SFTOS does not support SNMP on VLANs.

SFTOS SNMP support conforms to RFC 1157 (SNMP v1), RFC 1213 (SNMP v2 (MIB-II)), and RFC 2570 (SNMP v3). For more on the MIBs and SNMP-related RFCs supported by SFTOS, refer to the SNMP appendix to this guide (see IEEE, RFCs, and SNMP on page 211). That appendix also discusses the SNMP traps that SFTOS generates.

The MIB files are on the S-Series product CD-ROM and on the iSupport website (password required): https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx

As a best practice, Force10 Networks recommends polling several SNMP object IDs (OIDs), as described here. SNMP is especially valuable in certain cases — for example when a console connection is unavailable.

All MIBs listed in the output of the **show sysinfo** command for a particular SFTOS image can be polled. Specifically, the switch supports counter MIBs, including the 32-bit and 64-bit IF-MIB and IP-MIB (accessing 64-bit counters requires SNMPv2c); hardware-related MIB variables, such as the Inventory MIB and Entity MIB; protocol-related MIBs, such as OSPF and VRRP; Layer 2 MIBs, such as the F10OS-SWITCHING-MIB; Layer 3 MIBs, such as F10OS-ROUTING-MIB, and the RMON MIB.

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 Force10 Enterprise Number.

This section provides basic configuration steps for enabling SNMP.

Command Syntax	Command Mode	Usage
show serviceport	Global Config	Learn a management IP address, either that of the Ethernet Management or of the management VLAN. For details, see Creating and Changing Management IP Addresses on page 81.
[**no**] **snmp-server community** *community-name*	Global Config	Identify an SNMP community for the switch to join. Force10 suggests that you use the same community name for all chassis that you will manage with your SNMP management system. If you have previously entered a string for another SNMP manager and agent, use the existing string.
[**no**] **snmptrap** *name ipaddr*	Global Config	Adds an SNMP trap receiver name and IP address to the SNMP community. The maximum name length is 16 case-sensitive alphanumeric characters.

Command Syntax	Command Mode	Usage
[**no**] **snmp-server enable trap violation**	Interface Config or Interface Range	Optionally, enable the sending of new violation traps for a specified interface designating when a packet with a disallowed MAC address is received on a locked port. Except for this trap, all traps are enabled by default. For details on trap options, see Managing SNMP Traps on page 88, below.

Other commands that configure the SNMP server connection include:

- **snmp-server**: Sets the name and the physical location of the switch, and the organization responsible for the network.
- **snmp-server community ipaddr**: Sets a client IP address for an SNMP community.
- **snmp-server community ipmask**: Sets a client IP mask for an SNMP community.
- [**no**] **snmp-server community mode** *name*: Activates [deactivates] the designated SNMP community. All configured communities are enabled by default.
- **snmp-server community ro**: Restricts access to switch information to read-only.
- **snmp-server community rw**: Sets access to switch information to read/write.
- **snmptrap ipaddr**: Assigns an IP address to a specified community name.
- [**no**] **snmptrap mode**: Activates [deactivates] an SNMP trap receiver name.

In Privileged Exec mode:

- To view the SNMP configuration, use the **show snmpcommunity** command.
- To display SNMP trap receiver entries, use the **show snmptrap** command.

Managing SNMP Traps

SNMP trap events are logged and sent out via SNMP. For trap management, there is one Web UI panel (Trap Flags Configuration, accessed from **System** >> **Trap Manager** — see Using the Web User Interface on page 65) and the CLI commands listed below.

Traps can be enabled for the following features:

- Authentication
- Link up/down
- Multiple users
- Spanning Tree
- OSPF
- DVMRP
- PIM (both DM and SM with one command)

Note: The DVMRP, OSPF, and PIM traps and associated commands are supported only in the Layer 3 software image of SFTOS.

Commands to [disable] enable traps are listed here.

Global Config Mode:

- [**no**] **ip dvmrp trapflags**: This command sets the DVMRP Traps flag (disabled by default).
- [**no**] **ip pim-trapflags**: This command sets the PIM Traps flag (disabled by default).
- [**no**] **snmp-server enable traps bcaststorm**: This command sets Broadcast Storm flag (sending of traps enabled by default).
- [**no**] **snmp-server enable traps linkmode**: This command sets the Link Up/Down flag (traps enabled by default).
- [**no**] **snmp-server enable traps multiusers**: This command sets the Multiple Users flag (traps enabled by default).
- [**no**] **snmp-server enable traps stpmode**: This command sets the Spanning Tree flag (traps enabled by default).
- [**no**] **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 (traps disabled by default).
- [**no**] **snmp-server traps enable**: This command sets the Authentication flag (traps disabled by default).

Interface Config Mode:

- **snmp trap link-status**: This command enables link status traps by interface.
- **snmptrap snmpversion** *name ipaddr* {**snmpv1** | **snmpv2**}: This command selects between SNMP version 1 and version 2 traps to be sent for the selected SNMP trap name.

Privileged Exec Mode:

- **show trapflags:** As shown in Figure 63, this command displays the status of each of the SNMP trap flags noted above. The final three in this example only appear when the Routing Package is loaded.

```
Force10 #show trapflags
Authentication Flag.......................... Enable
Link Up/Down Flag............................ Enable
Multiple Users Flag.......................... Enable
Spanning Tree Flag........................... Enable
Broadcast Storm Flag......................... Enable
DVMRP Traps.................................. Disable
OSPF Traps................................... Disable
PIM Traps.................................... Disable
```

Figure 63 Using the show trapflags Command

For information on the SNMP trap log, see also Displaying the SNMP Trap Log on page 99. That section also notes the relationship between the trap log and the System log.

For information on S-Series SNMP traps, MIBs, and SNMP-related RFCs, see IEEE, RFCs, and SNMP on page 211. See also the techtip "*What Should I Poll with SNMP?*" on the iSupport website: https://www.force10networks.com/csportal20/KnowledgeBase/ToolTipsSSeries.aspx

For more on SNMP commands, see the SNMP Community Commands section in the *Management* chapter of the *SFTOS Command Reference*.

Note: SFTOS supports the RMON (Remote Network Monitoring) MIB (RFC 2819), which is enabled by default and cannot be disabled. SFTOS contains no commands for configuring RMON or displaying RMON data. For more on RMON support, see the RMON techtip on iSupport, or see the RMON MIB file, which is on both the S-Series product CD and iSupport.

Setting up Simple Network Time Protocol (SNTP)

This section describes how to configure the Simple Network Time Protocol (SNTP) feature.

SNTP Overview

SNTP:

- Synchronizes network resources, particularly the timestamps in logs (see System Logs on page 95).
- Is an adaptation of NTP
- Provides a synchronized network timestamp
- Can be used in broadcast or unicast mode
- Client implemented over UDP, which listens on port 123

The SNTP command set consists of:

- **sntp broadcast client poll-interval** *poll-interval*: Set the poll interval for SNTP broadcast clients in seconds as a power of two, with a range from 6 to 16.
- **sntp client mode** [**broadcast** | **unicast**]: Enable Simple Network Time Protocol (SNTP) client mode, and, optionally, set the mode to either broadcast or unicast.
- **sntp client port** *port-ID* [*poll-interval*]: Set the SNTP client port ID to a value from 1 to 65535. Then, optionally, set the poll interval for the client in seconds, as a power of two, in the range from 6 to 10.
- **sntp unicast client poll-interval** *poll-interval*: Set the poll interval for SNTP unicast clients in seconds as a power of two, with a range from 6 to 16.
- **sntp unicast client poll-timeout** *timeout*: Set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.
- **sntp unicast client poll-retry**: Set the poll retry for SNTP unicast clients to a value from 0 to 10.
- **sntp server**: Configure an SNTP server (maximum of three).
- **show sntp**: Display SNTP settings and status.
- **show sntp client**: Display SNTP client settings.
- **show sntp server**: Display SNTP server settings and configured servers.

SNTP CLI Examples

The following examples show the major command sequences in configuring the SNTP connection.

Example #1: configuring sntp client mode

```
Force10 (Config)#sntp client mode broadcast ?
<cr> Press Enter to execute the command.
Force10 (Config)#sntp client mode unicast ?
<cr> Press Enter to execute the command.
Force10 (Config)#sntp broadcast client poll-interval ?
<6-10> Enter value in the range (6 to 10). Poll interval is 2^(value) in seconds.
```

Figure 64 Configuring SNTP Client Mode

Example #2: configuring sntp client port

```
Force10 (Config) #sntp client port 1 ?
<cr> Press Enter to execute the command.
<6-10> Enter value in the range (6 to 10). Poll interval is 2^(value) in seconds.
```

Figure 65 Configuring the SNTP Client Port

Example #3: configuring sntp server

```
Force10(Config) #sntp server 10.11.8.6 ?
<cr> Press Enter to execute the command.
<1-3> Enter SNTP server priority from 1 to 3.
```

Figure 66 Configuring the SNTP Server Connection

Example #4: show sntp client

```
Force10  #show sntp client
Client Supported Modes: unicast broadcast
SNTP Version: 4
Port: 123
Client Mode: unicast
Unicast Poll Interval: 6
Poll Timeout (seconds): 5
Poll Retry: 1
```

Figure 67 Using the show sntp client Command

Example #5: show sntp server

```
Force10  #show sntp server
Server IP Address: 10.11.8.6
Server Type: ipv4
Server Stratum: 3
Server Reference Id: NTP Srv: 128.4.1.2
Server Mode: Server
Server Maximum Entries: 3
Server Current Entries: 1
SNTP Servers
------------
IP Address: 10.11.8.6
Address Type: IPV4
Priority: 1
Version: 4
Port: 123
Last Update Time: JUNE 18 04:59:13 2005
Last Attempt Time: JUNE 18 11:59:33 2005
Last Update Status: Other
Total Unicast Requests: 1111
Failed Unicast Requests: 361
```

Figure 68 Using the show sntp server Command

Using the Web UI to Configure SNTP

The following examples use Web UI panels to configure the SNTP connection.

Use the **SNTP Global Configuration** panel (navigate to **System** >> **System** >> **SNTP** >> **Global Configuration**) to set the switch client mode (same as **sntp client mode** command), the client port (defaults to 123), poll intervals (same as **sntp unicast client poll-interval** and **sntp broadcast client poll-interval**), and timeouts (same as **sntp unicast client poll-timeout** and **sntp unicast client poll-retry**); see SNTP Overview on page 90).

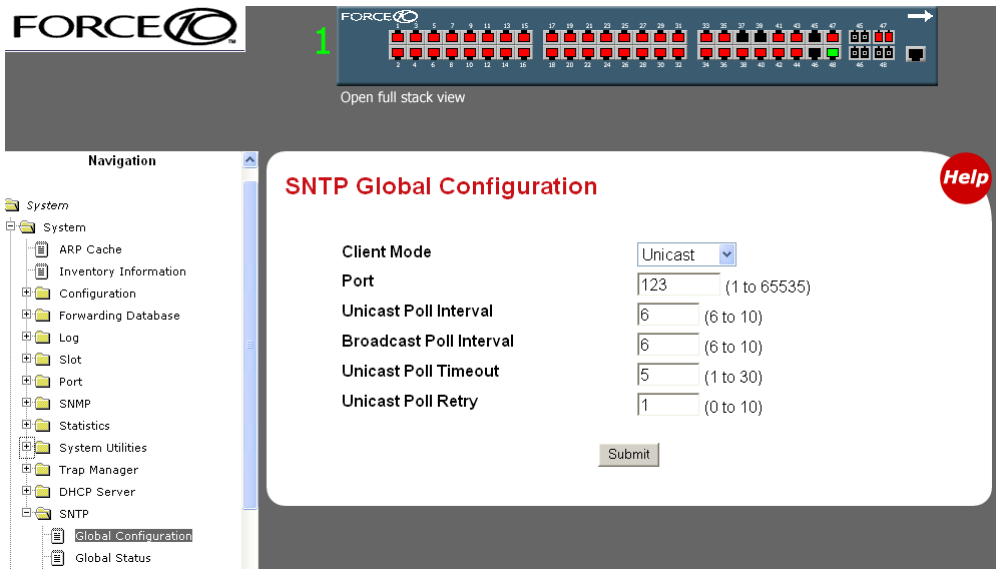


Figure 69 SNTP Global Configuration panel of the Web UI

In the navigation tree, click **Global Status** to display current status:

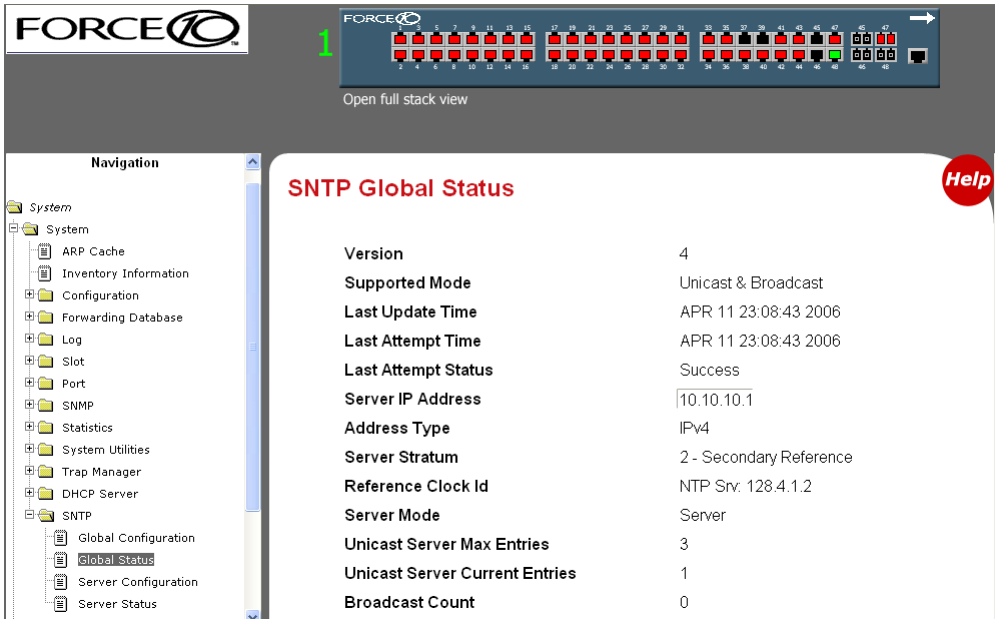


Figure 70 SNTP Global Status Panel

In the navigation tree, click **Server Configuration**:

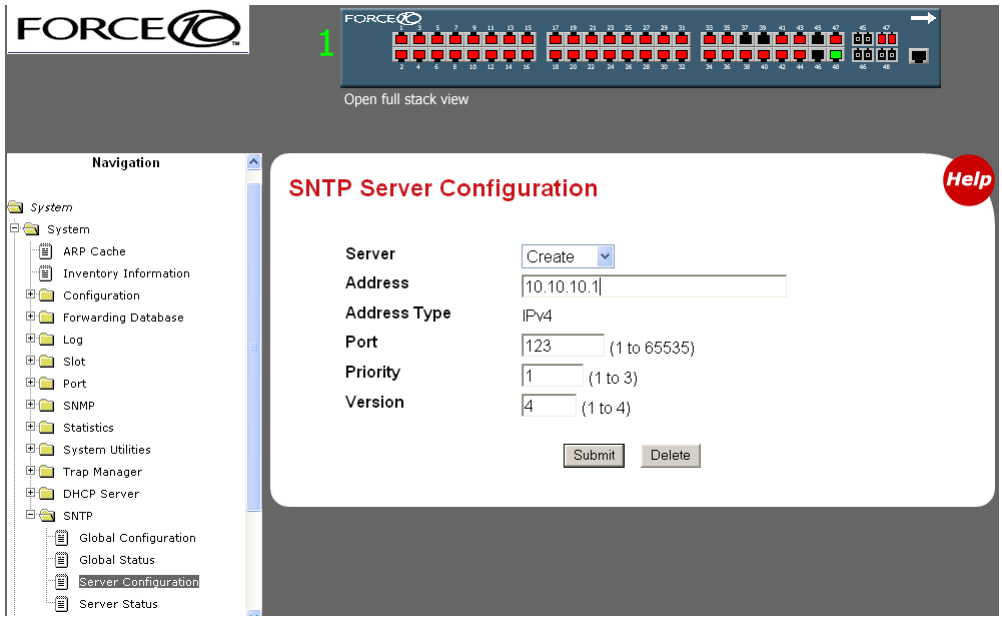


Figure 71 SNTP Server Configuration Panel

To configure a connection to a new SNTP server, select **Create** from the **Server** field. You can configure connections for up to three SNTP servers.

To edit an existing connection, select the IP address of the SNTP server from the **Server** field, as shown in Figure 72.

This SNTP Server Configuration panel is the equivalent of the CLI command **sntp server** *ipaddress* [*priority* [*version* [*portid*]]], where *ipaddress* is the IP address of the SNTP server and *priority* is a number from 1 to 3, which the switch would use to establish the sequence in which it would accept time updates from the three possible SNTP servers.

Enter the IP address of the SNTP Server:

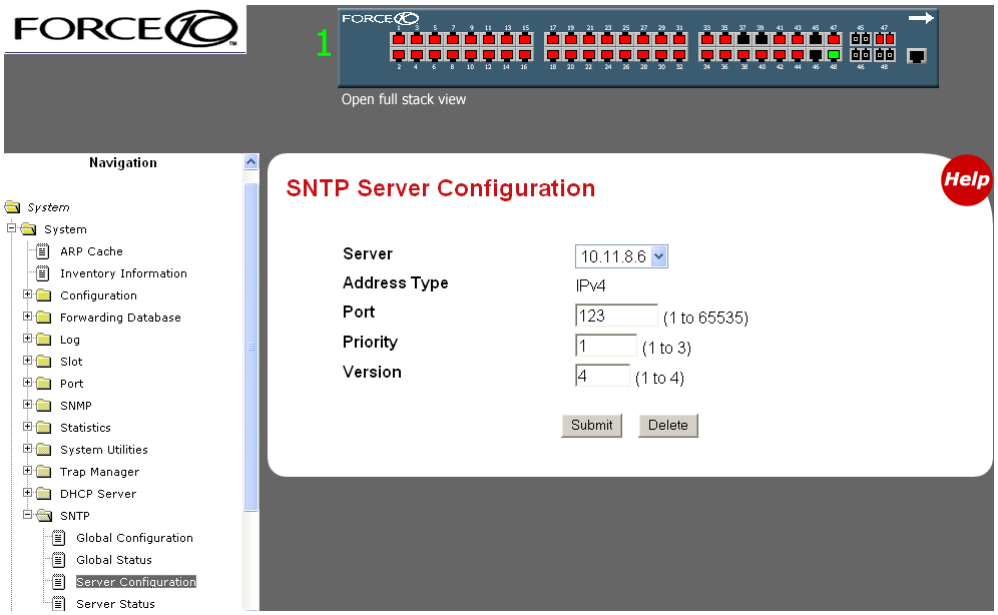


Figure 72 SNTP Server Configuration Panel

In the navigation tree, click **Server Status**:

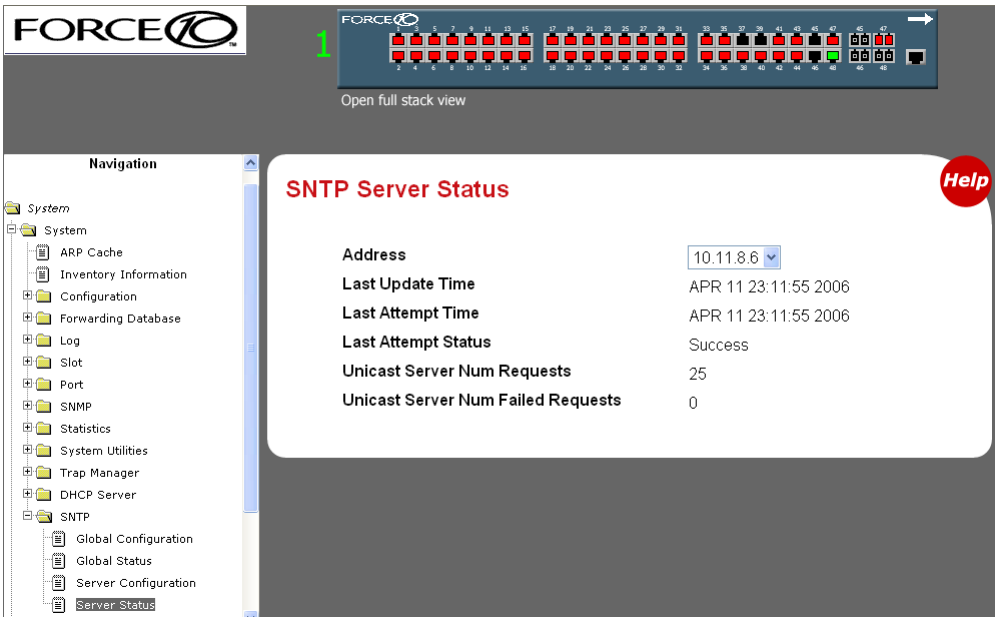


Figure 73 SNTP Server Status Panel

Chapter 5 System Logs

This chapter describes the system logging features, in these major sections:

- Logging Commands on page 95
- Configuring the System Log on page 96
- Using the Persistent Event Log on page 98
- Displaying the SNMP Trap Log on page 99
- Configuring Syslog Server Host Connections on page 100

The S-Series switch can maintain several types of log:

- **System log:** This log, also referred to as the buffered log, collects events down to the level of "critical" (by default). The log is stored in RAM until it is lost at power off or reboot. Thus, as a best practice, you should save these messages to a syslog server. For details, see Configuring Syslog Server Host Connections on page 100.
  The System log does not run by default, so you must enable it, at which time you can also set the level of detail to collect. See Configuring the System Log on page 96.
- **Event log:** This log, also referred to as the persistent log, collects exception messages and critical boot-up messages. The log is enabled by default, stored in flash memory, and is not lost upon system reboot or failover in a stack. SFTOS reserves 16 MB for the event log. See Using the Persistent Event Log on page 98.
- **Trap log:** This log collects SNMP traps. For details, see Displaying the SNMP Trap Log on page 99.

Logging Commands

The Syslog chapter in the *SFTOS Command Reference* provides a detailed explanation of the command syntax for the system log command set, which consists of the following commands:

- **logging buffered**. See Configuring the System Log on page 96.
- **logging buffered wrap**. See Configuring the System Log on page 96.
- **logging cli-command**. See Configuring the System Log on page 96.
- **logging console**. See Configuring the System Log on page 96.
- **logging host**. See Configuring Syslog Server Host Connections on page 100.
- **logging host reconfigure**. See Configuring Syslog Server Host Connections on page 100.
- **logging host remove**. See Configuring Syslog Server Host Connections on page 100.
- **logging syslog**. See Configuring Syslog Server Host Connections on page 100.
- **show logging**. See Using the Persistent Event Log on page 98.

- **show logging buffered**. See Displaying System Log Files on page 97.
- **show logging hosts**. See Configuring Syslog Server Host Connections on page 100.
- **show logging traplogs**. See Displaying the SNMP Trap Log on page 99.

Note: See also the **show trapflags** and **show snmptrap** commands in the Management chapters of this guide and the *SFTOS Command Reference*.

Configuring the System Log

By default, buffered logging (the “System log”) is disabled. To enable the system logging:

Command Syntax	Command Mode	Purpose
logging buffered	Global Config	Turn on buffered logging (off by default). Enter **no logging buffered** to disable buffered logging.
no logging buffered wrap	Global Config	(Optional) Turn off wrapping (overwriting the oldest events). The feature, enabled by default, allows continued logging when memory capacity is reached. Enter **logging buffered wrap** to reenable wrapping.
no logging cli-command	Global Config	(Optional) The logging of CLI activity is enabled by default. To turn this feature off, enter this command. Enter **logging cli-command** to reenable logging of CLI commands.
logging console [*severitylevel*]	Global Config	(Optional) Enable logging to the console (disabled by default). The default logging severity level is 2 (critical). To change the level, enter the appropriate word or equivalent integer value in place of *severitylevel*, as listed here: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7). **Note:** The severity level entered here does not affect the severity level of the system log stored in memory; that severity level is fixed at 7 (debug). Enter **no logging console** to disable console logging.
		(Optional) To display accurate times and dates in the log, configure a connection to an SNTP server. See Setting up Simple Network Time Protocol (SNTP) on page 90

Note: You can copy the System log from the switch to a TFTP server. See Downloading and Uploading Files on page 48 in the Getting Started chapter.

Displaying System Log Files

Execute the **show logging buffered** command to see the System log messages, as shown in Figure 74:

```
Force10 #show logging buffered ?

<cr>Press Enter to execute the command.

Force10 #show logging buffered

Buffered (In-Memory) Logging:       enabled
Buffered Logging Wrapping Behavior: On
Buffered Log Count:                 66


<1> JAN 01 00:00:02 0.0.0.0-0 UNKN[268434944]: usmdb_sim.c(1205) 1 %% Error 0 (0x0)
<2> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 %% Event (0xaaaaaaaa)
<6> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(531) 3 %% Starting code...
<6> JAN 01 00:00:16 0.0.0.0-3 UNKN[251627904]: cda_cnfgr.c(383) 4 %% CDA: Creating new STK file.
<6> JAN 01 00:00:39 0.0.0.0-3 UNKN[233025712]: edb.c(360) 5 %% EDB Callback: Unit Join: 3.
<6> JAN 01 00:00:40 0.0.0.0-3 UNKN[251627904]: sysapi.c(1864) 6 %% File user_mgr_cfg: same
version (6) but the sizs (2312->7988) differ
```

Figure 74 Using the show logging buffered Command

interpreting system log messages

The field descriptions in Table 1 use the first log message in Figure 74 as an example:

<2> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 %% Event (0xaaaaaaaa)

Note: A “bootos.c” entry, as in this example, occurs each time the system is reloaded. An equivalent “bootos.c” message appears in the Event log, as shown in Figure 76 on page 100.

Table 1 A System Log Message Decomposed

Field Example	Description
<2>	Severity level (emergency = 0; alert = 1; critical = 2; error = 3; warning = 4; notice = 5; informational = 6; debug = 7)
JAN 01 00:00:09	Timestamp (To activate the date stamp, enable an SNTP server connection.)
0.0.0.0-1	Stack ID (If this unit were #2 in a stack, the Stack ID would be 0.0.0.0-2.)
UNKN	Software component name (UNKN = unknown)
[268434944]:	Thread ID in software component
bootos.c	Software file name
(487)	Line number in software file identified in software file name
2	Event log message sequence number
%% Error (0xaaaaaaaa)	Event message

Using the Persistent Event Log

In addition to the optional buffered System log described above, the switch maintains a persistent Event log in NVRAM. Persistent logging is always enabled to memory and disabled to the console or to syslog servers. The log does not require configuration.

The purpose of the Event log is to save system exception information to persistent memory for analysis by Force10 Engineering. Error messages start with “ERROR”, while event messages start with “EVENT”, as shown in Figure 75.

Execute the **show logging** command (with no keyword), as shown below.

```
Force10 #show logging

Logging Client Local Port:       514
CLI Command Logging:             disabled
Console Logging:                 disabled
Console Logging Severity Filter: alert
Buffered Logging:                enabled

System Logging:                  disabled

Log Messages Received:           66
Log Messages Dropped:            0
Log Messages Relayed:            0
Log Messages Ignored:            0

Event Log
---------
                                                                  Time
       File                              Line TaskID   Code            d  h  m s
EVENT> bootos.c                           434 0FFFFE00 AAAAAAAA        0  0  0 12
ERROR> unitmgr.c                         3325 0E41CD38 00000000        3  6  8 34
EVENT> bootos.c                           434 0FFFFE00 AAAAAAAA        0  0  0 9
ERROR> unitmgr.c                         3339 0E22B298 00000000       14 22  9 4
EVENT> bootos.c                           434 0FFFFE00 AAAAAAAA        0  0  0 11
EVENT> bootos.c                           434 0FFFFE00 AAAAAAAA        0  0  0 11
ERROR> reset603.c                         177 0D6007A8 09A60110        3 13 31 59
EVENT> bootos.c                           434 0FFFFE00 AAAAAAAA        0  0  0 8
--More-- or (q)uit
```

Figure 75 Using the show logging Command

Because the **show logging** command monitors a persistent log database, it is important to correlate any ERROR entries with the timeline using the time designator. The **Time** column in the output is the system up-time, shown by number of days (“d”), hours (“h”), minutes (“m”), and seconds (“s”).

Although the structure of the System log and Event log are different, both logs contain the same software file, line, and task information. For example, a reboot is a common event, indicated in each log by “bootos.c”. All “bootos.c” entries should be between 8 to 15 seconds after the system restarts, which you can see in the **Time** column in Figure 75. The typical log entry following a “bootos.c” entry is either:

- “ERROR> unitmgr.c”: Indicates the system rebooted due to a user command.
- “ERROR> reset603.c”: Indicates the system rebooted due to a program error interrupt.
- “ERROR> broad_hpc_drv.c”: Typically indicates failed driver calls

Note: You can copy the Event log from the switch to a TFTP server. See Downloading and Uploading Files on page 48 in the Getting Started chapter.
Note: The **show logging** report is also included in the output of **show tech-support**.

Displaying the SNMP Trap Log

The **show logging traplogs** command displays a trap summary (number of traps since last reset and last view), followed by trap details, as shown in Figure 76.

```
Force10 #show logging traplogs

Number of Traps Since Last Reset.....6
Number of Traps Since Log Last Viewed.....6

Log System Up Time Trap
--- ------------- ----------------------------------------------
0 3 days 10:23:55  Last or default VLAN deleted: VLAN: 10
1 3 days 10:23:55  Last or default VLAN deleted: VLAN: 1
2 1 days 05:27:21  Link Up: Unit: 1 Slot: 0 Port: 48
3 0 days 00:00:46  Link Up: Unit: 3 Slot: 0 Port: 2
4 0 days 00:01:01  Cold Start: Unit: 0
5 0 days 00:21:33  Failed User Login: Unit: 1 User ID: admin
6 0 days 18:33:31  Failed User Login: Unit: 1 User ID: \
7 0 days 19:27:05  Multiple Users: Unit: 0 Slot: 3 Port: 1
8 0 days 19:29:57  Multiple Users: Unit: 0 Slot: 3 Port: 1
```

Figure 76 Using the show logging traplogs Command

Traps are also replicated in the System log. They are denoted by the “TRAPMGR” Component name and the “traputil.c” file name. For example, when accessing an S-Series switch through Telnet, the switch generates a multi-user trap, which appears in the **show logging traplogs** command output in this form:

0 0 days 09:24:46 Multiple Users: Unit: 0 Slot: 3 Port: 1

The System log reports, for the same event:

<5> JAN 01 09:24:46 10.16.128.4-1 TRAPMGR[241206472]: traputil.c(689) 132 % Multiple Users: Unit: 0 Slot: 3 Port: 1

For more on the System log output, see Displaying System Log Files on page 97.

Note: You can copy the trap log from the switch to a TFTP server. See Downloading and Uploading Files on page 48 in the Getting Started chapter.

The **clear traplog** command (Privileged Exec mode) empties the trap log.

For more on SNMP management, see Setting up SNMP Management on page 87.

Configuring Syslog Server Host Connections

A syslog server can:

- Store system messages and/or errors
- Store to local files on the switch or a remote server running a syslog daemon
- Collect message logs from many systems

The S-Series switch sends System log messages to all enabled syslog servers. You have the following choices for managing the logging settings:

- Configure and enable the connections to up to eight syslog servers for a particular switch.
- Limit the amount of data in the log, both by type (such as CLI activity) and severity.

The following commands enable you to manage syslog server settings:

Command Syntax	Command Mode	Purpose
logging host *ipaddress* [*port* [*severitylevel*]]	Global Config	Configure logging to a syslog server. Up to eight server hosts can be configured. Enter the IP address of the server, followed, optionally, by the port (514, by default), and then, optionally, by the severity; the levels are the same as for **logging console**—emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7). **Note:** The severity level set here does not change the severity level of the buffered system log. You also can use this command to change existing syslog host settings. See also the **logging host reconfigure** and **logging host remove** commands in the *SFTOS Command Reference* for details on changing existing syslog host settings.
logging syslog [**port** *portid*]	Global Config	Enable logging to any configured syslog server.
show logging hosts	Privileged Exec	Display configured syslog servers.

Note: You can also copy logs from NVRAM to a TFTP server. See Downloading and Uploading Files on page 48 in the Getting Started chapter.

An example of using the **logging host** command is shown in Figure 77.

An example of using the **show logging host** command is shown in Figure 78.

```
Force10 #config
Force10 (Config)#logging ?
buffered       Buffered (In-Memory) Logging Configuration.
cli-command    CLI Command Logging Configuration.
console        Console Logging Configuration.
host           Enter IP Address for Logging Host.
syslog         Syslog Configuration.

Force10 (Config)#logging host ?
<hostaddress>            Enter Logging Host IP Address
reconfigure              Logging Host Reconfiguration
remove                   Logging Host Removal

Force10 (Config)#logging host 10.11.130.7 ?
<cr>                     Press Enter to execute the command.
<port>                   Enter Port Id

Force10 (Config)#logging host 10.11.130.7 514 ?
<cr>                     Press Enter to execute the command.
<severitylevel>          Enter Logging Severity Level (emergency|0, alert|1,
                         critical|2, error|3, warning|4, notice|5, info|6,
                         debug|7).

Force10 (Config)#logging host 10.11.130.7 514 1 ?
<cr>                     Press Enter to execute the command.

Force10 (Config)#logging host 10.11.130.7 514 1
Force10 (Config)#
```

Figure 77 Using the logging host Command

The **show logging hosts** command displays the host settings that you configured with **logging syslog** and **logging host**.

```
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
```

Figure 78 Using the show logging hosts Command

Chapter 6 Configuring Interfaces

This chapter contains overview information on interfaces supported by SFTOS, along with information on configuring physical interfaces, in the following sections:

- Interface Support in SFTOS
- Viewing Interface Information on page 104
- Viewing Layer 3 Interface Information on page 108
- Configuring Physical Interfaces on page 108
- Bulk Configuration on page 113

Interface Support in SFTOS

SFTOS 2.4.1 supports the following interface types:

- 10 Gigabit Ethernet ports (10G)
- Layer 2 VLANs: See Chapter 13, VLANs.
- Layer 2 link aggregation groups (LAGs; also called port channels): See Link Aggregation on page 155.
- Console port (TTY emulation): See Connecting to the Console Port on page 31.
- IP-based Management Ethernet: See Creating and Changing Management IP Addresses on page 81. Note that the S2410 provides both the management VLAN and the Ethernet Management port. See Configuring the Ethernet Management Port on page 82.

Note: SFTOS 2.4.1 does not support loopback and null interfaces.

In the S-Series, you can place physical interfaces, port channel interfaces, and VLANs in Layer 2 mode (Table 2).

Table 2 Interfaces in the S-Series

Type of Interface	Modes Possible	Require Creation	Default State
10G Ethernet	Layer 2	No	Shut down (disabled)
Ethernet Management port	n/a	No	Enabled

Table 2 Interfaces in the S-Series

Type of Interface	Modes Possible	Require Creation	Default State
LAG (Port Channel)	Layer 2	Yes	Shut down (disabled)
		Yes	
VLAN	Layer 2	Yes*	Enabled
Management VLAN		No	Shut down (disabled)

*The Default VLAN (VLAN 1) does not require creation, but it can be modified.

Physical and logical interfaces are automatically in Layer 2 mode.

Viewing Interface Information

S-Series (SFTOS) ports are configured for Layer 2 by default, so you do not need to explicitly configure them as Layer 2, as you do on the E-Series (FTOS). Initially, the running configuration file simply displays the series of ports without any configuration annotations. As you configure a port, those changes appear in the running configuration following the affected port.

For example, Figure 79 shows part of a running configuration; it displays the configuration for the series of ports numbered 0/5 through 0/8. Each port listing is followed by *no shutdown* to indicate that each of these ports has been enabled.

```
Force10 #show running-config
!--Output deleted--!

interface 0/5
no shutdown
exit

interface 0/6
no shutdown
exit

interface 0/7
no shutdown
exit

interface 0/8
no shutdown
exit

!--Output deleted--!
```

Figure 79 show running-config Command Example Showing Layer 2 Interface Information

In addition to inspecting the running config, as described above (see Figure 79), the CLI provides multiple commands to inspect the status and configuration of interfaces:

- **show interface managementethernet**: Use this command, in either Privileged Exec mode or User Exec mode (the only command in this set that is available in User Exec mode), to display the current Management Ethernet interface settings. See Verifying Access to the Management VLAN on page 84.
- **show interface switchport**: Displays a packet transmission summary for the switch. See Figure 80.
- **show interface** *slot/port*: 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. This command provides a summary of packets received and transmitted on the designated interface. See Figure 81.
- **show interface ethernet switchport**: Displays more packet transmission details for the switch than the **show interface switchport** command. See Figure 82.
- **show interface ethernet** *slot/port*: Displays details on port activity on the designated interface. See Figure 83.
- **show interfaces cos-queue** [*slot/port*]: The *slot/port* parameter (as described above) is optional. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed. See Figure 84 on page 108.
- **show interfaces description** {*slot/port* | *1-3965*}: Enter an interface ID, in slot/port format, to report on a particular interface, or enter a VLAN ID to display information for that VLAN.

Note: The port LEDs on the face of the switch also provide status information. For details, see the hardware guide for your switch.

```
Force10 #show interface switchport

Broadcast Packets Received..................... 0
Packets Received With Error.................... 0
Packets Transmitted Without Errors............. 0
Broadcast Packets Transmitted.................. 0
Transmit Packet Errors......................... 0
Address Entries Currently in Use............... 1
VLAN Entries Currently in Use.................. 1
Time Since Counters Last Cleared............... 0 day 0 hr 25 min 47 sec

Force10 #
```

Figure 80 Using the show interface switchport Command for Switch Summary Packet Information

```
Force10 #show interface 0/1
Ports 1 through 48
Packets Received Without Error..... 0
Packets Received With Error..... 0
Broadcast Packets Received..... 0
Packets Transmitted Without Errors..... 0
Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 0 day 0 hr 25 min 38 sec

Force10 #
```

Figure 81 Using the show interface Command for Summary Packet Information for One Port

```
Force10 #show interface ethernet switchport

Total Packets Received (Octets)..... 0
Unicast Packets Received..... 0
Multicast Packets Received..... 0
Broadcast Packets Received..... 0
Receive Packets Discarded..... 0

Octets Transmitted..... 0
Packets Transmitted Without Errors..... 0
Unicast Packets Transmitted..... 0
Multicast Packets Transmitted..... 0
Broadcast Packets Transmitted..... 0
Transmit Packets Discarded..... 0
Most Address Entries Ever Used..... 1
Address Entries Currently in Use..... 1

Maximum VLAN Entries..... 1024
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 25 min 45 sec

Force10 #
```

Figure 82 Using the show interface ethernet Command for Switch Detailed Packet Information

Use the **show interface ethernet** *slot/port* command for detailed packet information for the designated port, as shown in Figure 83 on page 107.

```
Force10 #show interface ethernet 0/4

Total Packets Received (Octets)..............  16217658
Packets Received > 1522 Octets...............  0
Packets RX and TX 64 Octets..................  3260
Packets RX and TX 65-127 Octets..............  11968
Packets RX and TX 128-255 Octets.............  6329
Packets RX and TX 256-511 Octets.............  4812
Packets RX and TX 512-1023 Octets............  338
Packets RX and TX 1024-1518 Octets...........  7710
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........  34091
Unicast Packets Received.....................  30641
Multicast Packets Received...................  2010
Broadcast Packets Received...................  1440
Total Packets Received with MAC Errors.......  0
Jabbers Received.............................  0
Fragments/Undersize Received.................  0
Alignment Errors.............................  0
--More-- or (q)uit
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)...........  52084
Max Frame Size...............................  1518

Total Packets Transmitted Successfully.......  326
Unicast Packets Transmitted..................  105
Multicast Packets Transmitted................  0
Broadcast Packets Transmitted................  221
Total Transmit Errors........................  0
FCS Errors...................................  0
--More-- or (q)uit
Tx Oversized.................................  0
Underrun Errors..............................  0

Total Transmit Packets Discarded.............  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
MSTP BPDUs Transmitted.......................  0
MSTP BPDUs Received..........................  0
--More-- or (q)uit

EAPOL Frames Transmitted.....................  0
EAPOL Start Frames Received..................  0

Time Since Counters Last Cleared.............  0 day 5 hr 7 min 16 sec
```

Figure 83 Checking Detailed Interface Counters Per Port

The **show interfaces cos-queue** [*slot/port*], with and without the *slot/port* parameter, produces almost the same report — one version for the interface and the other for the switch. The version of the report generated with the *slot/port* parameter is shown in Figure 84.

```
Force10 #show interfaces cos-queue 0/1

Interface..................................... 0/1
Interface Shaping Rate........................ 0

Queue Id   Min. Bandwidth   Scheduler Type   Queue Management Type
--------   --------------   --------------   ---------------------
0          0                Weighted         Tail Drop
1          0                Weighted         Tail Drop
2          0                Weighted         Tail Drop
3          0                Weighted         Tail Drop
4          0                Weighted         Tail Drop
5          0                Weighted         Tail Drop
6          0                Weighted         Tail Drop

Force10 #
```

Figure 84 Using the show interfaces cos-queue Command on a Port

Viewing Layer 3 Interface Information

Note: Layer 3 interfaces can only be created with the Layer 3 Package of SFTOS, which is not included in SFTOS 2.4.1. The **show ip interface** command is not available.

Use the **show version** command to determine what package is installed. See Figure 8 on page 37.

Configuring Physical Interfaces

As described in Interface Support in SFTOS on page 103, except for the 10/100/1000 Ethernet Management port dedicated to switch management, the S2410 switch has only 10G Layer 2 ports. By default, all 10G interfaces are disabled to traffic. When enabled, the port speed is fixed at 10G.

The physical interfaces can become part of virtual interfaces such as VLANs or port channels:

- For more information on VLANs, see Chapter 13, VLANs.
- For more information on port channels, see Link Aggregation on page 155.

The following basic configuration tasks for physical interfaces are discussed in this chapter:

- enable an interface on page 110 (mandatory)
- configure speed and duplex mode on page 111 (optional)
- clear interface counters on page 111 (optional)

The System Configuration chapter of the *SFTOS Command Line Reference* details the commands used in this chapter.

You can duplicate the execution of a particular configuration command against an interface without repercussion. For example, you can execute the **no shutdown** command twice on a port. The first use of the command enables the port. The second use of the command has no effect.

Nevertheless, as a best practice, you should determine the status of physical interfaces before executing commands on them. For that purpose, you can select from the commands described in Viewing Interface Information on page 104.

Another option is the **show port all** command, the use of which is shown below in Figure 85. (The sample in Figure 85 is truncated at port 19.)

```
Force10 #show port all

                  Admin Physical   Physical    Link   Link    LACP    Flow
Interface   Type    Mode    Mode       Status   Status  Trap    Mode    Mode
---------- ------ ------- ---------- ---------- ------ ------- ------- -------
0/1                Enable  10G Full              Down   Enable  Enable  Disable
0/2                Enable  10G Full              Down   Enable  Enable  Disable
0/3                Enable  10G Full              Down   Enable  Enable  Disable
0/4                Enable  10G Full              Down   Enable  Enable  Disable
0/5                Enable  10G Full              Down   Enable  Enable  Disable
0/6                Enable  10G Full              Down   Enable  Enable  Disable
0/7                Enable  10G Full              Down   Enable  Enable  Disable
0/8                Enable  10G Full              Down   Enable  Enable  Disable
0/9                Enable  10G Full   10G Full   Up     Enable  Enable  Disable
0/10               Enable  10G Full              Down   Enable  Enable  Disable
0/11               Enable  10G Full   10G Full   Up     Enable  Enable  Disable
0/12               Enable  10G Full   10G Full   Up     Enable  Enable  Disable
0/13               Enable  10G Full              Down   Enable  Enable  Disable
0/14               Enable  10G Full              Down   Enable  Enable  Disable
0/15               Enable  10G Full              Down   Enable  Enable  Disable
0/16               Enable  10G Full              Down   Enable  Enable  Disable
0/17               Enable  10G Full              Down   Enable  Enable  Disable
0/18               Enable  10G Full              Down   Enable  Enable  Disable
0/19               Enable  10G Full              Down   Enable  Enable  Disable
--More-- or (q)uit
```

Figure 85 Interfaces Listed in the show port all Command (Partial)

The **show port all** command generates a report with the following fields:

- Interface—Valid slot and port number separated by forward slash.
- 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—The field shows if the port is enabled or shut down. To enable the port, see enable an interface on page 110.

- Physical Mode—For an S2410, the field should only show 10G Full.
- Physical Status—Indicates the port speed and duplex mode. Ports in an S2410 with Link Status of Up should only show 10G Full.
- Link Status— For an S2410, the field only displays *Up* or *Down*.
- Link Trap—This field indicates whether or not to send a trap when link status changes. The default is enabled.
- LACP Mode—Displays whether Link Aggregation Control Protocol (LACP) is enabled or disabled on the port.
- Flow Mode—Whether the port is enabled for Flow Control (802.3x), disabled by default

In an S2410, the **show slot** report shows that no optional modules (slots) are available. All 10G ports are in the chassis.

```
Force10 #show slot

              Admin   Power          Configured Card          Hot       Power
Slot  Status  State   State             Model ID              Pluggable Down
----- ------ ------- ------- ------------------------------- --------- -----
0     Empty  Enable  Disable S2410-01-10GE-24CP                 No      No
```

Figure 86 Example of the show slot Command

After you determine the status of physical interfaces, you can access the Interface Config mode to configure the designated interface.

enable an interface

Ports are shut down by default. To enable them, you can do so in bulk mode or per port. For more on bulk configuration, see Bulk Configuration on page 113.

To enable an individual port, use the following sequence of commands:

Step	Command Syntax	Command Mode	Purpose
1	**interface** *slot/port*	Config	To access the Interface Config mode for the selected port, enter the keyword **interface** followed by the port number in *slot/port* format. For example, to configure port 4, enter **interface 0/4**.
2	**no shutdown**	Interface Config	Enable the selected interface.

configure speed and duplex mode

As stated above, the 10G ports in the S2410 are fixed at 10 gigabits per second, so the **show port** command (**show port all** or **show port** *slot/port)* should always indicate “10G Full” in the Physical Mode field (indicating 10-gigabits per second, full-duplex). If the Admin Mode field indicates that the port is administratively enabled, then the Physical Status field should also indicate “10G Full”.

```
Force10 S2410 #show port 0/10

                    Admin    Physical    Physical    Link    Link     LACP     Flow
Interface    Type    Mode     Mode        Status     Status  Trap     Mode     Mode
---------- ------ ------- ---------- ---------- ------ ------- ------- -------
0/10        PC Mbr  Enable  10G Full              Down   Enable  Enable  Disable

Force10 S2410 #
```

Figure 87 Using the show port Command to Verify Port Settings

The Link Status field indicates whether the port is passing traffic. Of course, at some point in the process you must connect ports for that field to indicate *Up*.

configure Layer 3 mode

Note: Layer 3 (routing) is not available in SFTOS 2.4.1.

clear interface counters

The counters in the report generated by the **show interfaces** command can be reset by the following command. This command does not clear the counters captured by any SNMP program.

Command Syntax	Command Mode	Purpose
clear counters [*slot/port* | **all**]	Privileged Exec	Without an interface specified, the command clears counters for all ports. With an interface specified, the command clears counters for that interface only. When you use the keyword **all**, the command clears counters for the entire switch.

When you enter the **clear counters** command, the CLI prompts you to confirm that you want SFTOS to clear the type of counters that you specified. The three options and responses are shown in Figure 88.

```
Force10 #clear counters 0/1
Are you sure you want to clear the port stats? (y/n)y
Port Stats Cleared.
Force10 #clear counters  all
Are you sure you want to clear ALL port stats? (y/n)y
ALL Port Stats Cleared.
Force10 #clear counters
Are you sure you want to clear the switch stats? (y/n)y
Switch Stats Cleared.
```

Figure 88 Clearing Counters

Bulk Configuration

Bulk configuration means to configure groups of interfaces (physical or logical) with the same command(s).

You have three bulk configuration options:

- **Global:** Make system-level changes in the Global Config mode. For example, to enable all ports, enter **no shutdown all** in Global Config mode. You can then disable certain ports in the Interface Config mode.
- **Interface Range mode:** Select one or more sequences of interfaces — ports or logical (VLAN or LAG) — with the **interface range** command, to configure with the same settings. For example, see Figure 89 and Figure 90 on page 114.
- **Web UI:** You can use the Web UI to perform bulk configuration tasks. For more on the Web UI, see Using the Web User Interface on page 65.

Using Interface Range Mode

An interface range is a user-selected set of interfaces — ports, VLANs, or port channels — to which you can apply the same configuration change.

There must be at least one valid interface within the range. Bulk configuration excludes from configuration any non-existing interfaces from an interface range. A default VLAN may be configured only if the interface range being configured consists of only VLAN ports.

In combination with the parameter values you include, the **interface range** command creates the interface range and accesses the Interface Range mode, where you can execute the commands that are applied to that range of interfaces.

The interface range prompt offers the interface (with slot and port information) for valid interfaces. The maximum size of an interface range prompt is 32. If the prompt size exceeds this maximum, it displays (...) at the end of the output.

Note: When creating an interface range, interfaces appear in the order they were entered and are not sorted.

The System Configuration chapter in the *SFTOS Command Reference* provides syntax details on the commands used in the Interface Range mode.

See the following section, Bulk Configuration Examples on page 114, for more on bulk configuration.

In this guide, see also Using the Interface Range Mode on page 163 in the LAG chapter.

Bulk Configuration Examples

The following examples are of using the **interface range** command for bulk configuration.

configuring a single range

In this example, the **interface range ethernet** *range* command was used to select ports 1 through 23 on stack member 5. Then, the **no shutdown** command enabled all of those ports.

```
Force10 (config)#interface range ethernet 0/1-0/23
Force10 (config-if-range-et-0/1-0/23)#no shutdown
Force10 (config-if-range-et-0/1-0/23)#
```

Figure 89 Using Bulk Configuration on a Single Range

Note that spaces are not allowed around hyphens when specifying the range.

The resulting prompt includes interface types with slot/port information for valid interfaces, in this case *(conf-if-range-et-0/1-0/23)#*. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).

configuring multiple ranges

In this example, the **interface range ethernet** *range* command was used to select multiple ranges in order to enable ports.

```
Force10 (Conf)#interface range ethernet 0/1-0/3,0/10-0/13,0/15-0/17
Force10 (conf-if-range-et-0/1-0/3,0/10-0/13...)#
```

Figure 90 Using Multiple Ranges

Note that spaces are also not allowed around commas when specifying the range.

As shown above, if the **interface range** command specifies multiple port ranges, the resulting prompt displays the first two ranges, and then an ellipsis (...) for any subsequent ranges. If overlapping port ranges are specified, the overlapping ranges are represented by one range showing the lowest port number and the highest port number of the overlapping ranges.

Chapter 7 DHCP

This chapter describes how to configure the S-Series to serve as a DHCP/BootP relay agent or a DHCP server.

Note: The S-Series switch can only act as a DHCP/BootP relay agent when the Layer 3 Package of SFTOS is installed.

This chapter contains the following sections:

- Protocol Overview
- Configuring the Switch as a DHCP Server on page 116
- Using the Switch as a BootP/DHCP Relay Agent on page 118
- Configuration Example — DHCP Server and Relay Agent on page 120

DHCP Commands

The *SFTOS Command Reference* contains the following DHCP commands:

- DHCP server function — Chapter 11, DHCP Server Commands
- DHCP/BootP relay agent function — Chapter 20, Routing Commands

Protocol Overview

SFTOS support for DHCP is based on the following RFCs. For DHCP details beyond this document, consult those RFCs:

- RFC 2131: DHCP
- RFC 2132: DHCP Options and BootP Vendor Extensions
- RFC 1534: Interoperation between DHCP and BootP
- RFC 1542: Clarifications and Extensions for the BootP
- RFC 2241: DHCP Options for Novell Directory Services
- RFC 2242: Netware/IP Domain Name and Information

Table 3 describes the messages that are exchanged between a DHCP client and server.

Table 3 Messages Exchanged between a DHCP Client and Server

Reference	Message	Use
0x01	DHCPDISCOVER	The client is looking for available DHCP servers.
0x02	DHCPOFFER	The server response to the client's DHCPDISCOVER message.
0x03	DHCPREQUEST	The client broadcasts to the server, requesting offered parameters from one server specifically, as defined in the packet.
0x04	DHCPDECLINE	The client-to-server communication, indicating that the network address is already in use.
0x05	DHCPACK	The server-to-client communication with configuration parameters, including committed network address.
0x06	DHCPNAK	The server-to-client communication, refusing the request for configuration parameter.
0x07	DHCPRELEASE	The client-to-server communication, relinquishing network address and canceling remaining leases.
0x08	DHCPINFORM	The client-to-server communication, asking for only local configuration parameters that the client already has externally configured as an address.

Configuring the Switch as a DHCP Server

Important Points to Remember

- The S-Series supports a maximum of 16 pools. If you attempt to configure more than 16 pools, the switch prints the following error message:
  `Could not create DHCP pool.`
- Up to 256 leases can be offered.
- To create a partial scope, use the **ip dhcp excluded-address** *ip address* command.
- When configuring VLANs, SFTOS automatically matches the requests coming from a particular subnet to the pool with that subnet and assigns an IP address accordingly. For example, it will recognize that a request has been received from a host on VLAN 10, which is using addresses on the 10.10.10.0 network, and automatically assign it an address from the 10.10.10.0 pool.

Configuration Task List

- Configuring a DHCP address pool (required) on page 117
- Excluding IP addresses (optional) on page 117
- Enabling the SFTOS DHCP Server feature (required) on page 117

Configuring a DHCP address pool (required)

You can configure a DHCP address pool with a name that is a symbolic string (such as "Engineering") or an integer (such as 0). Configuring a DHCP address pool also places you in DHCP pool configuration mode, as identified by the "`(config-dhcp)#`" prompt, from which you can configure pool parameters (for example, the IP subnet number and default router list). To configure a DHCP address pool, complete the following required steps. For details on these commands, see the DHCP Server Commands chapter in the *SFTOS Command Reference*.

Step	Command	Mode	Purpose
1	**ip dhcp pool** *poolname*	Global Config	Creates a name for the DHCP server address pool and places you in DHCP pool configuration mode (identified by the "`config-dhcp#`" prompt).
2	**network** *ip_address mask*	DHCP Pool Config	Configures an IP address and subnet mask for this DHCP address pool, which contains the range of available IP addresses that the DHCP server may assign to clients.
3	**default-router** *address1* [*address2...address8*]	DHCP Pool Config	Specifies the default router list for a DHCP client. After a DHCP client boots, the client begins sending packets to its default router. The IP address of the default router must be on the same subnet as the client.
4	**dns-server** *address1* [*address2...address8*]	DHCP Pool Config	Specifies the IP address of a DNS server that is available to a DHCP client. A single IP address can be configured. Note: If more than one address is configured, SFTOS overwrites the configuration with the most recent address.

Excluding IP addresses (optional)

The DHCP server assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP address that the DHCP server should not assign to clients.

Use the **ip dhcp excluded-address** *lowaddress* [*highaddress*] command in Global Config mode to create partial scopes.

Enabling the SFTOS DHCP Server feature (required)

By default, the SFTOS DHCP Server feature is disabled on the S-Series. Use the **service dhcp** command in Global Config mode to enable the SFTOS DHCP Server feature:

Verifying the DHCP Server Configuration

Use the **show ip dhcp server statistics** command to verify the DHCP server configuration:

```
Force10 #show ip dhcp server statistics

Automatic Bindings.............................. 0
Expired Bindings................................ 0
Malformed Bindings.............................. 0

Messages                                     Received
----------                                  ----------
DHCP DISCOVER................................... 5
DHCP REQUEST.................................... 0
DHCP DECLINE.................................... 0
DHCP RELEASE.................................... 0
DHCP INFORM..................................... 0

Messages                                       Sent
----------                                     ------
DHCP OFFER...................................... 0
DHCP ACK........................................ 0
DHCP NACK....................................... 0
```

Figure 91 Using the show ip dhcp server statistics Command

Using the Switch as a BootP/DHCP Relay Agent

The S-Series also can serve as a BootP/DHCP relay agent, forwarding DHCP packets between clients and a DHCP server (you can only use the switch as a relay agent to one DHCP server). This section describes the concepts and tasks needed to configure the DHCP relay agent.

DHCP Relay Agent Overview

When the switch is configured to act as a DHCP relay agent, it forwards DHCP client broadcasted requests to a DHCP server on another broadcast domain (Layer 3 network). These broadcasted requests from a DHCP client use a destination IP address of 255.255.255.255 (all networks broadcast address).
The DHCP relay agent process is as follows:

1. The DHCP relay agent makes these two changes to the in-bound DHCP packet:
   - **a** The relay agent appends its own IP address to the source IP address of the DHCP frames going to the DHCP server.
   - **b** The relay agent populates the Gateway IP address field with the IP address of the interface on which the DHCP message is received from the client.
2. The relay agent forwards the rewritten DHCP request on behalf of a DHCP client to the DHCP server.
3. The DHCP server unicasts a reply to the DHCP relay agent, using the Gateway IP address field to determine the subnet from which the DHCPDISCOVER, DHCPREQUEST, or DHCPINFORM message originated.
4. The relay agent forwards the packet to the DHCP client.

Configuring the Switch as a DHCP Relay Agent

Implement the DHCP relay agent feature with **bootpdhcprelay** commands, all in Global Config mode. For details on these commands, see the Bootp/DHCP Relay Commands section of the Routing Commands chapter in the *SFTOS Command Reference*.

Step	Command	Mode	Purpose
1	**bootpdhcprelay serverip** *ip-address*	Global Config	Enter the IP address of the DHCP server.
2	**bootpdhcprelay enable**	Global Config	Enable forwarding of BootP/DHCP requests. By default, the DHCP relay agent feature is disabled.
3	**bootpdhcprelay maxhopcount** *1-16*	Global Config	(Optional) Configure the maximum allowable relay agent hops. The parameter has a range of 1 to 16. By default, the packet will be forwarded a limit of four hops.
4	**bootpdhcprelay minwaittime** *0-100*	Global Config	(Optional) Configure the minimum wait time in seconds for BootP/DHCP relay requests. 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 default value is 0 seconds.

Verifying the DHCP Relay Agent Configuration

Use the **show bootpdhcprelay** command to verify the DHCP Relay Agent configuration, as shown in Figure 92.

```
Force10 #show bootpdhcprelay

Maximum Hop Count.............................. 4
Minimum Wait Time(Seconds)..................... 0
Admin Mode..................................... Enable
Server IP Address.............................. 10.16.1.2
Circuit Id Option Mode......................... Disable
Requests Received.............................. 0
Requests Relayed............................... 0
Packets Discarded.............................. 0
```

Figure 92 Using the show bootpdhcprelay Command

Configuration Example — DHCP Server and Relay Agent

In the following example, a DHCP address pool is created for PCs on the 10.1.3.0 network. In this pool, all addresses except the excluded address, which is the router's IP address, are available to the DHCP server for assigning to clients.

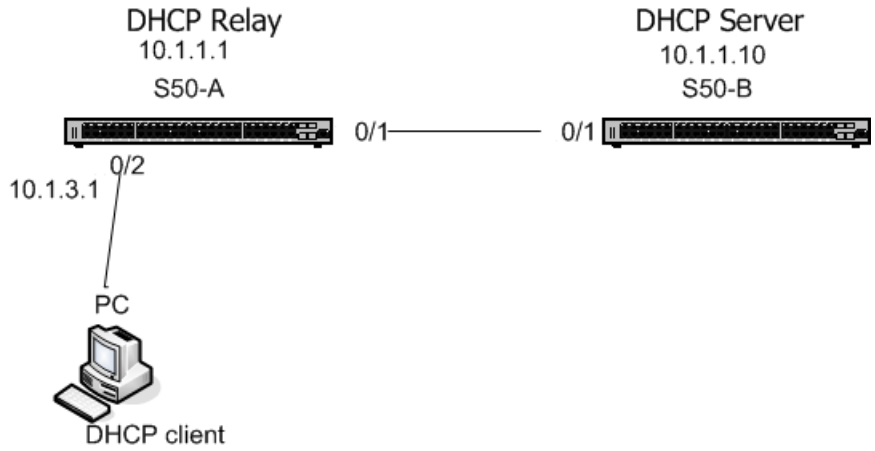


Figure 93 Diagram of Two Switches Acting as DHCP Server and Relay Agent

Configure switch "S50-B", from the diagram above, as a DHCP server, as shown in Figure 94.

```
S50-B #config
S50-B (Config)#service dhcp
S50-B (Config)#ip dhcp pool Pool1
S50-B (config-dhcp)#network 10.1.3.0 255.255.255.0
S50-B (config-dhcp)#default-router 10.1.3.1
S50-B (config-dhcp)#dns-server 192.168.1.90
S50-B (config-dhcp)#exit
S50-B (Config)#ip dhcp excluded-address 10.1.3.1 10.1.3.11
S50-B (Config)#ip routing
S50-B (Config)#interface 0/1
S50-B (Config)#routing
S50-B (Interface 0/1)#ip address 10.1.1.10 255.255.255.0
S50-B (Interface 0/1)#exit
S50-B (Config)#ip route 10.1.3.0 255.255.255.0 10.1.1.1
!--Using a static route to ensure the DHCP server can ping 10.1.3.1.--!
S50-B (Config)#exit
```

Figure 94 Example of Configuring a Switch as a DHCP server

Configure switch S50-A and S50-B (Figure 93), as the DHCP relay agent and DHCP server, respectively.

```
S50-A #config
S50-A (Config)#ip routing
S50-A (Config)#bootpdhcprelay serverip 10.1.1.10
S50-A (Config)#bootpdhcprelay enable
S50-A (Config)#interface 0/2
S50-A (Interface 0/2)#ip address 10.1.3.1
S50-A (Interface 0/2)#exit
S50-A (Config)#interface 0/1
S50-A (Interface 0/1)#ip address 10.1.1.1
```

Figure 95 Example of Configuring a Switch as a DHCP relay agent

Chapter 8 Providing User Access Security

This chapter contains the following major sections:

- Choosing a TACACS+ Server and Authentication Method
- Configuring TACACS+ Server Connection Options on page 124
- Configuring a RADIUS Connection on page 124
- Enabling Secure Management with SSH or SSL on page 128
- Enabling Broadcast Storm Control on page 133

SFTOS supports several user-access security methods, including local (see Creating a User and Password on page 39), port security (IEEE 802.1X) through RADIUS and Terminal Access Controller Access Control System (TACACS+), and encrypted transport session (between the management station and switch) using Secure Shell (SSH), Secure Sockets Layer (SSL), or HTTPS. This chapter describes how to configure each of those methods.

For more on port security configuration (including MD5), see the Security deck of the S-Series Training slides, which are on the S-Series Documentation CD-ROM. For the syntax of port-based security commands, which is also known as port MAC locking, see the Security chapter of the *SFTOS Command Reference*.

Choosing a TACACS+ Server and Authentication Method

To use TACACS+ to authenticate users, you specify at least one TACACS+ server with which the S-Series will communicate, then identify TACACS+ as one of your authentication methods. To select TACACS as the login authentication method, use the following command sequence:

Step	Command Syntax	Command Mode	Purpose
1	**tacacs-server host** *ip-address*	Global Config	Configure a TACACS+ server host. Enter the IP address or host name of the TACACS+ server. You can use this command multiple times to configure multiple TACACS+ server hosts.

Step	Command Syntax	Command Mode	Purpose
2	**exit**	TACACS Config	Return to Global Config mode. Alternatively, while you are still in TACACS Config mode, you can set values for server-specific parameters, such as priority, key, and timeout. See Configuring TACACS+ Server Connection Options on page 124.
3	**authentication login** *listname* {*method1* [*method2* [*method3*]]}	Global Config	Create a method-list name and specify that **TACACS** is one method for login authentication.
4	**users defaultlogin** *listname*	Global Config	Assign a method list to use to authenticate non-configured users when they attempt to log in to the system.
5	**show tacacs**	Privileged Exec	Verify the configuration and status of TACACS servers (See Figure 97).
6	**show authentication**	Privileged Exec	Display the ordered authentication methods for all authentication login lists.

TACACS would generally not be the last method specified, in order to avoid a situation where the final authentication option depends on a server that might be offline. Generally, you would specify **local** as the final method. For example, in the command string "**authentication login listone tacacs local**", "listone" is the name given to the method list, followed by the selected sequence of authentication methods—"tacacs" and then "local". For details on setting local passwords, see Creating a User and Password on page 39.

TACACS+ includes a group of configurable settings that you can also leave in their default settings. You can configure some global settings (for all TACACS+ servers), or you can configure settings at the individual server level. See the Security chapter in the *SFTOS Command Line Reference* for details on global settings. See the following section, Configuring TACACS+ Server Connection Options on page 124, for more on configuring one host.

Specify the IP address of the TACACS host with the **tacacs-server host** command in the Config mode, as shown in Figure 96. In this example, the user then changes the local timeout to 5 seconds:

```
Force10_S2410 (Config)#tacacs-server host 1.1.1.1
Force10_S2410 (Tacacs)#timeout 5
Force10_S2410 (Tacacs)#exit
Force10_S2410 (Config)#
```

Figure 96 Setting the IP Address of a TACACS+ Server

```
Force10_S2410 #show tacacs

IP address         Status        Port    Single       Timeout   Priority    Connection
---------------   ------------   -----   ----------   -------   --------
1.1.1.1           Disconnected   49      No           Global       0
10.16.1.58        Disconnected   49      No           Global       0

Global values
--------------
Timeout: 10
```

Figure 97 Settings for Multiple TACACS+ Servers

Figure 98 shows the creation of three authentication method lists, each with a different priority sequence:

- The first list, named “one”, sets **local** as the first authentication method, the TACACS+ server as the second
- List “two” defaults to local authentication
- List “three” sets the TACACS+ server as the first method and **reject** (The reject keyword indicates the user is never authenticated) as the second “method”.:

```
Force10_S2410 (Config)#authentication login one local tacacs
Force10_S2410 (Config)#authentication login two
Force10_S2410 (Config)#authentication login three tacacs reject
```

Figure 98 Setting the Authentication Method

```
Force10_S2410)#show authentication
Authentication Login List Method 1 Method 2  Method 3
------------------------- -------- --------  --------
defaultList               local    undefined undefined
one                       local    tacacs    undefined
two                       undefined undefined undefined
three                     tacacs   reject    undefined
```

Figure 99 Verifying the Authentication Method Lists with the show authentication Command

Figure 100 shows the assignment of list “three” to authenticate non-configured (default) users.

```
Force10_S2410) (Config)#users defaultlogin three
Force10_S2410) (Config)#exit
Force10_S2410)#show users authentication
Authentication Login Lists

User       System Login     802.1x
---------- ---------------- -------------
admin      defaultList      defaultList
default    three            defaultList
```

Figure 100 Assigning and Verifying the Authentication Method List Assigned to Non-configured Users

Configuring TACACS+ Server Connection Options

To configure a TACACS+ host connection, you must first enter its IP address with the **tacacs-server host** command, as described above. After you identify the host, the CLI puts you in the TACACS Configuration mode for that particular host. In that mode, you can override global and default settings of the communication parameters. The following commands are available for a specified TACACS host:

Command Syntax	Command Mode	Purpose
key *key-string*	TACACS Configuration	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. Range: 1 to 128 characters
port *port-number*	TACACS Configuration	Specify a server port number for that TACACS host. Range: zero (0) to 65535. Default = 49
priority *priority*	TACACS Configuration	Determine the order in which the server will be used with multiple authentication servers, with 0 being the highest priority. Range: zero (0) to 65535. Default = 0
single-connection	TACACS Configuration	Configure the client to maintain a single open connection with the TACACS server. Default = multiple connections
timeout	TACACS Configuration	Range: 1 to 30 seconds. Default = global setting

To delete a TACACS+ server host, use the **no tacacs-server host** *ip-address* command.

Note: Web UI panels were not available for TACACS+ configuration before SFTOS Release 2.3.

Configuring a RADIUS Connection

Remote Authentication Dial-In User Service (RADIUS) is another means of port-based network access control. The switch acts as an intermediary to a RADIUS server, which provides both an authentication and an accounting function to maintain data on service usages.

Under RFC 2866, an extension was added to the RADIUS protocol giving the client the ability to deliver accounting information about a user to an accounting server. Exchanges to the accounting server follow similar guidelines to that of an authentication server, but the flows are much simpler.

At the start of service for a user, the RADIUS client configured to use accounting sends an accounting start packet specifying the type of service that it will deliver. Once the server responds with an acknowledgement, the client periodically transmits accounting data. At the end of service delivery, the

client sends an accounting stop packet allowing the server to update specified statistics. The server again responds with an acknowledgement.

Setting up a connection to a server running Remote Authentication Dial-In User Service (RADIUS) is basically the same as the TACACS+ procedure described above (see Choosing a TACACS+ Server and Authentication Method on page 121 and Configuring TACACS+ Server Connection Options on page 124), where you identify the address of the authentication server and you specify an ordered set of authentication methods. The following RADIUS commands are documented in the Security chapter of the *SFTOS Command Reference*:

- **radius accounting mode:** Enable the RADIUS accounting function.
- **radius server host:** Configure the RADIUS authentication and accounting server.
- **radius server key:** Configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server.
- **radius server msgauth:** Enable the message authenticator attribute for a specified server.
- **radius server primary:** Configure the primary RADIUS authentication server for this RADIUS client.
- **radius server retransmit:** Set the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server.
- **radius server timeout:** Set the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received.
- **show radius:** to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers.
- **show radius accounting statistics:** Display the configured RADIUS accounting mode, accounting server, and the statistics for the configured accounting server.
- **show radius statistics** (authentication)**:** Display the statistics for RADIUS or configured server.

Using the CLI to Configure Access through RADIUS

The following example configuration sequence configures:

- A single RADIUS server at IP address 10.10.10.10, to be used for both authentication and accounting
- The RADIUS server shared secret for both authentication and accounting to be the word “secret”
- An authentication list called “radiusList”, specifying RADIUS as the only authentication method
- radiusList method associated with the 802.1x default login (for non-configured users for 802.1x port security). 802.1x port-based access control is enabled for the system.
- Interface 0/1 in force-authorized mode, because this is where the RADIUS server and protected network resources are located

If a user, or supplicant, attempts to communicate through the switch on any interface except port 0/1, the system challenges the supplicant for login credentials. The system encrypts the provided information and

transmits it to the RADIUS server. If the RADIUS server grants access, the system sets the 802.1x port state of the interface to authorized and the supplicant is able to access network resources.

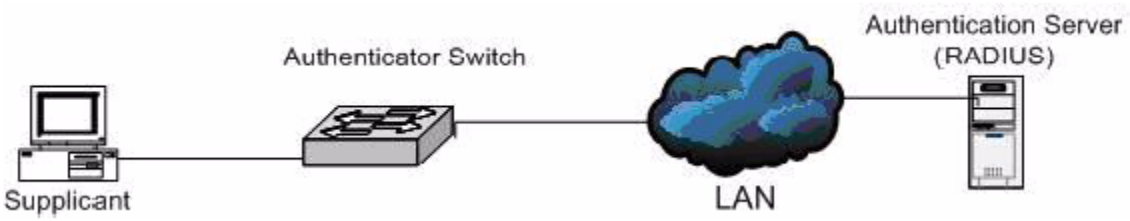


Figure 101 RADIUS Topology

```
Force10 #config
Force10 (Config)#
Force10 (Config)#radius server host auth 10.10.10.10          <-- authentication
Force10 (Config)#radius server key auth 10.10.10.10
Enter secret (16 characters max):******
Re-enter secret:******
Force10 (Config)#radius server host acct 10.10.10.10          <-- accounting
Force10 (Config)#radius server key acct 10.10.10.10
Enter secret (16 characters max):******
Re-enter secret:******
Force10 (Config)#radius accounting mode
Force10 (Config)#authentication login radiusList radius
Force10 (Config)#dot1x defaultlogin radiusList
Force10 (Config)#dot1x system-auth-control
Force10 (Config)#interface 0/1
Force10 (Interface 0/1)#dot1x port-control force-authorized
Force10 (Interface 0/1)#exit
Force10 (Config)#exit
```

Figure 102 Configuration Example for RADIUS

Figure 103 and Figure 104 show a setup with two RADIUS servers as authentication servers. The command **radius server key auth 10.10.10.10** invokes a request for “secret1” to be the shared secret word for the RADIUS server at IP address 10.10.10.10 , while **radius server key auth 11.11.11.11** invokes a request for “secret2” as the shared secret for the second RADIUS server. The **radius server primary** command sets the first RADIUS server as the primary authenticator, and the rest of the configuration is as was done above.

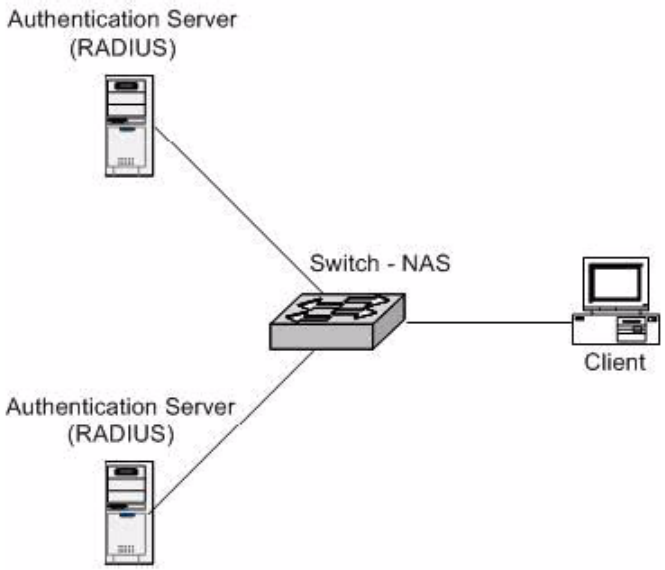


Figure 103 Topology with Two RADIUS Servers

```
Force10 #config
Force10 (Config)#radius server host auth 10.10.10.10
Force10 (Config)#radius server key auth 10.10.10.10
Enter secret (16 characters max):******
Re-enter secret:******
Force10 (Config)#radius server host auth 11.11.11.11
Force10 (Config)#radius server key auth 11.11.11.11
Enter secret (16 characters max):******
Re-enter secret:******
Force10 (Config)#radius server primary 10.10.10.10
Force10 (Config)#authentication login radiusList radius local
Force10 (Config)#users defaultlogin radiusList
Force10 (Config)#exit
```

Figure 104 Configuration Example for Two RADIUS Servers

Using the Web UI to Configure Access through RADIUS

You can also use the SFTOS Web User Interface (Web UI) to configure the RADIUS connection. To configure the IP address and UDP port used by the server, navigate to the RADIUS Server Configuration panel (**Security** >> **RADIUS Server Configuration**).

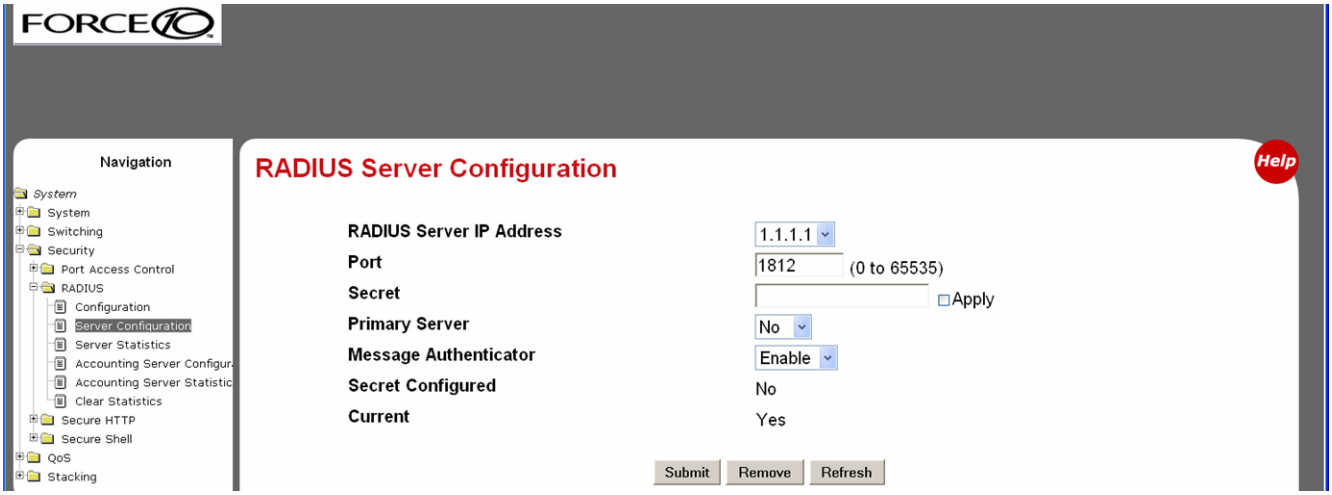


Figure 105 RADIUS Server Configuration Panel of the Web UI

If there is a shared secret to be used with the specfied accounting server, enter the secret in the Secret field.

If you are also want the RADIUS accounting server feature, use the RADIUS Accounting Server Configuration panel.

Enabling Secure Management with SSH or SSL

SFTOS supports three ways to provide more secure management access to the switch:

- Interactive login using the Telnet protocol with Secure SHell (SSH) aded for security
- Web browser (see Using the Web UI for Security Configuration on page 76 in Chapter 3, Using the Web User Interface) with Secure Sockets Layer (SSL) provided for security
- SNMP: SNMP includes its own security features.

Secure SHell (SSH) and Secure Sockets Layer (SSL/HTTPS) both provide secure management through an encrypted transport session between the management station and switch.

Enabling secure management through SSH and SSL is a four-step process:

1. Generate the SSH keys or SSL certificates offline.
2. Copy the SSH keys or SSL certificates to the switch using TFTP.
3. Enable the secure management server (SSH or HTTPS) on the switch.
4. Disable the insecure version of the management server (Telnet or HTTP).

The SSH keys and SSL certificates are in a .zip file that are on the S2410 Documentation CD-ROM. You can also get them from your Force10 account team. The .zip file contains two directories—ssh and ssl:

- The ssh directory has example RSA1, RSA2, and DSA keys and a shell script called "generate-keys.sh" that can be used to generate your own SSH keys.
- The ssl directory has example certificates and a shell script called "generate-pem.sh" that can be used to generate your own SSL certificates.

The scripts provided use OpenSSH (http://www.openssh.org/) and OpenSSL (http://www.openssl.org/) for key and certificate generation. Other free and commercial tools exist that can provide the same functionality, and you can use them if you like.

For an introduction to the options and commands related to the Telnet, SSH, and HTTP/HTTPS features, see Setting up Management Connections to the Switch on page 30.

Enabling SSH

1. Generate the SSH keys using the script in the ssh directory, or copy the example keys (which end in .key) to your TFTP server.
2. Copy the keys to NVRAM with TFTP, as follows from this example, using the IP address of your TFTP server. For SSHv1, copy the RSA1 key; for SSHv2, copy the RSA2 and DSA keys.

```
Force10 #copy tftp://192.168.0.10/rsa1.key nvram:sshkey-rsa1
Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ rsa1.key
Data Type................................ SSH RSA1 key
Are you sure you want to start? (y/n) y
TFTP SSH key receive complete... updating key file...
Key file transfer operation completed successfully
```

Figure 106 Copying RSA1 Key to NVRAM for SSHv1

```
Force10 #copy tftp://192.168.0.10/rsa2.key nvram:sshkey-rsa2
Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ rsa2.key
Data Type................................ SSH RSA2 key
Are you sure you want to start? (y/n) y
TFTP SSH key receive complete... updating key file...
Key file transfer operation completed successfully

Force10 #copy tftp://192.168.0.10/dsa.key nvram:sshkey-dsa
Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ dsa.key
Data Type................................ SSH DSA key
Are you sure you want to start? (y/n) y
TFTP SSH key receive complete... updating key file...
Key file transfer operation completed successfully
```

Figure 107 Copying RSA2 and DSA Keys to NVRAM for SSHv2

3. Enable the SSH server with the **ip ssh server enable** command.
4. To verify that the server has started, use the **show ip ssh** command to show the SSH server status.

```
Force10 #show ip ssh
SSH Configuration
Administrative Mode: ..................... Enabled
Protocol Levels: ......................... Versions 1 and 2
SSH Sessions Currently Active: ........... 0
Max SSH Sessions Allowed: ................ 5
SSH Timeout: ............................. 5
```

Figure 108 Using the show ip ssh Command to Show SSH Server Status

5. Check the log file for the following messages:

```
Force10 #show logging buffered
JAN 01 00:31:54 192.168.0.34-1 UNKN[222273672]: sshd_control.c(444) 15 %% SSHD:
sshdListenTask started
JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(596) 16 %% SSHD: successfully
opened file ssh_host_dsa_key
JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(609) 17 %% SSHD: successfully
loaded DSA key
JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(631) 18 %% SSHD: successfully
opened file ssh_host_rsa_key
JAN 01 00:31:54 192.168.0.34-1 UNKN[209305936]: sshd_main.c(643) 19 %% SSHD: successfully
loaded RSA2 key
JAN 01 00:31:56 192.168.0.34-1 UNKN[209305936]: sshd_main.c(353) 20 %% SSHD: Done
generating
```

Figure 109 Using the show logging buffered Command to Show SSH Server Status

6. Using an SSH client, connect to the switch and log in to verify that the SSH server is working.

7. Once you have verified that you can connect to the switch with an SSH client, the Telnet server can be disabled (if it was enabled) with the **no ip telnet server enable** command for additional security. The Telnet server is disabled by default.

Enabling SSL/HTTPS

1. Generate the SSL certificates using the script in the ssl directory, or copy the example certificates (which end in .pem) to your TFTP server.
2. Copy the certificates to NVRAM with TFTP, as shown in the following example, using the IP address of your TFTP server.

```
Force10 #copy tftp://192.168.0.10/dh512.pem nvram:sslpem-dhweak
Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ dh512.pem
Data Type................................ SSL DH weak
Are you sure you want to start? (y/n) y
TFTP SSL certificate receive complete... updating certificate file...
Certificate file transfer operation completed succesfully

Force10 #copy tftp://192.168.0.10/dh1024.pem nvram:sslpem-dhstrong
Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ dh1024.pem
Data Type................................ SSL DH strong
Are you sure you want to start? (y/n) y
TFTP SSL certificate receive complete... updating certificate file...
Certificate file transfer operation completed succesfully

Force10 #copy tftp://192.168.0.10/server.pem nvram:sslpem-server
Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ server.pem
Data Type................................ SSL Server cert
Are you sure you want to start? (y/n) y
TFTP SSL certificate receive complete... updating certificate file...
Certificate file transfer operation completed succesfully
Force10 #copy tftp://192.168.0.10/rootcert.pem nvram:sslpem-root
Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.0.10
TFTP Path.....................................
TFTP Filename............................ rootcert.pem
Data Type................................ SSL Root cert
Are you sure you want to start? (y/n) y
TFTP SSL certificate receive complete... updating certificate file...
Certificate file transfer operation completed successfully
```

Figure 110 Copying SSL Certificates to NVRAM

3. Enable the HTTPS server with the **ip http secure-server** command.
4. To verify that the server has started, use the **show ip http** command to show the HTTPS server status, and check the log file for the following messages.

```
Force10 #show ip http
HTTP Mode (Unsecure): Disabled
HTTP Mode (Secure): Enabled
Secure Port: 443
Secure Protocol Level(s): TLS1 SSL3

Force10 #show logging buffered
JAN 01 01:16:19 192.168.0.34-1 UNKN[209189968]: sslt_util.c(321) 39 %% SSLT: Successfully
loaded all required SSL PEM files
```

Figure 111 Using the show ip http Command to Show HTTPS Server Status

5. Using a Web browser, connect to the switch using an https:// URL, and log in to verify that the SSL server is working. The padlock icon on your browser should indicate an encrypted connection.

   If you used the example certificates, your browser will display a warning that it cannot verify the authenticity of the certificate. This is because the example certificates have not been certified by a Certification Authority. When certificates are acquired from a Certification Authority and loaded on the switch, this warning will not occur.

6. Once you have verified that you can connect to the switch with a Web browser, the HTTP server can be disabled with the **no ip http server** command for additional security (if it was enabled previously). The HTTP server is disabled by default.

Enabling Broadcast Storm Control

A broadcast storm occurs when incoming packets flood the LAN, degrading network performance. SFTOS provides broadcast storm control at a global (switch) level, not for individual interfaces.

To enable storm control, execute the command **storm-control broadcast** in Global Config mode. Disable storm control with the command **no storm-control broadcast**.

See also, in the *SFTOS Command Reference for the S2410*:

- **storm-control flowcontrol** in the Security Commands chapter
- **snmp-server enable traps bcaststorm** in the System Management Commands chapter

Broadcast storm control is implemented in SFTOS with automated high and low thresholds that are based on a percentage of link speed. If broadcast traffic on any port exceeds the high threshold percentage (as represented in the following table) of the link speed, the switch discards the broadcast traffic until the traffic returns to the low threshold percentage or less.

Table 4 Broadcast Storm Control Thresholds

Link Speed	High	Low
10M	20	10
100M	5	2
1000M	5	2

Use the **show storm-control** command to verify the setting.

Note: The **show interface-ethernet** *slot/port* command is designed to display the number of packets not forwarded in a broadcast storm condition when broadcast storm control has been implemented. However, because of S2410 hardware limitations, broadcast storm recovery counters are not incremented.

Chapter 9 Spanning Tree

This chapter contains the following major sections:

- SFTOS STP Features
- Spanning Tree Protocol (IEEE 802.1d) on page 136
- Spanning Tree Configuration Tasks on page 137
- Setting the STP Version Parameter on page 137
- Multiple Spanning-Tree Protocol (MSTP, IEEE 802.1s) on page 141
- Rapid Spanning Tree Protocol (RSTP) on page 146
- Display Spanning Tree Configuration on page 148

SFTOS STP Features

- Forwarding, Aging and Learning
- Spanning Tree, IVL and STP per VLAN
- IEEE 802.1d Spanning Tree
- IEEE 802.1s Multiple Spanning Tree
- IEEE 802.1w Rapid Spanning Tree

Forwarding, Aging, and Learning

- Forwarding
  - — At Layer 2, frames are forwarded according to their MAC address.
- Aging
  - — SFTOS supports a user-configurable address aging timeout parameter as defined in IEEE 802.1d.
- Learning
  - — SFTOS learns and manages MAC addresses as specified in IEEE 802.1d and IEEE 802.1q.
  - — SFTOS supports Shared VLAN Learning (SVL), although Independent VLAN Learning (IVL) is the default.

Spanning Tree Protocol (IEEE 802.1d)

Spanning Tree Protocol (STP) uses a spanning tree algorithm to provide path redundancy while preventing undesirable loops in a network:

- SFTOS switching can be configured to run with STP enabled or disabled.
- Without STP, a path failure causes a loss of connectivity.
- STP allows only one active path at a time between any two network devices, but allows for backup paths.
- When a topology change occurs, accelerated aging is used on the forwarding database(s).

SFTOS Spanning-Tree Protocol (STP) conforms to IEEE 802.1D and RFC 1493 Bridge MIB. STP allows port costs to be configured as zero, which causes the port to use IEEE 802.1D-recommended values. In addition, per-port Administrative Mode affects sequence when the link comes up:

- IEEE 802.1D mode—SFTOS follows the standard.
- Fast mode—listening and learning timers set to two seconds (this is recommended to avoid time-outs during reconfiguration).
- Off/manual mode—port is always in forwarding mode (this is recommended, but only when no loops are possible).

STP CLI Management

Privileged and User Exec Mode CLI commands:

- Display STP settings and parameters for the switch
  - **show spanning-tree summary**
- Display STP settings and parameters for the bridge instance
  - **show spanning-tree [brief]**

Global Config Mode CLI commands:

- [Disable] enable spanning tree for the switch:
  - **[no] spanning-tree**
- Set maximum time for discarding STP configuration messages, default 20 seconds
  - **[no] spanning-tree max-age 6-40**
- Set time between STP config messages, default 2 seconds
  - **[no] spanning-tree hellotime 1-10**
- Set time spent in listening and learning, default 15 seconds
  - **[no] spanning-tree forward-times 4-30**
- Set the protocol Version parameter to a new value:
  - **spanning-tree forceversion** {**802.1d | 802.1w | 802.1s**}

CLI Port Management

Privileged and User Exec Mode CLI command:

- Display STP settings and parameters for an interface:
  - **show spanning-tree interface** *slot/port*

Global Config Mode CLI command:

- [Disable] enable STP administrative mode for all interfaces:
  - **[no] spanning-tree port mode enable all**

Interface Config Mode CLI command:

- [Disable] enable STP administrative mode for an interface:
  - **[no] spanning-tree port mode enable**

Spanning Tree Configuration Tasks

1. Determine if Spanning Tree Protocol (STP) is enabled globally and on ports. See Figure 120 on page 148 and Figure 121 on page 149.
2. Select an STP operational mode. See Setting the STP Version Parameter on page 137.
3. Start STP: Enable STP globally each on participating switch and enable STP on ports. See Enabling STP on page 138.
4. Verify the global configuration, the interface configuration, and the STP convergence. See Display Spanning Tree Configuration on page 148.
5. (OPTIONAL) Change global STP operational parameters. See Changing Spanning Tree Global Parameters on page 140.
6. (OPTIONAL) Enable an edge port. See Enabling an Edge Port on page 141.
7. (OPTIONAL) Set MSTP behavior. See MST CLI Management on page 143.

Setting the STP Version Parameter

Note: The default spanning tree mode in SFTOS is IEEE 802.1s (MST), 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 Global Config mode command **spanning-tree forceversion** {**802.1d | 802.1w | 802.1s**} sets the protocol Version parameter to a new value. 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)

The **no spanning-tree forceversion** command sets the Force Protocol Version parameter to the default value, 802.1s.

Enabling STP

Use the following commands to run Spanning Tree convergence on participating switches.

spanning tree	Global Config	Enable the Spanning Tree Protocol on participating switches.
spanning-tree port mode enable all	Global Config	Activate STP on all ports on each participating switch.
spanning-tree port mode enable	Interface Config	Alternatively to enabling STP on all ports, enable STP on selected ports.

Example of Configuring STP

Figure 112 shows three S-Series switches, S50-1, S50-2, and S50-3. A physical connection exists between each pair of switches. Enabling the Spanning Tree Protocol (STP) on this topology will enable one least-cost route between each of the switches, so that redundant packets are not sent in both directions around the loop.

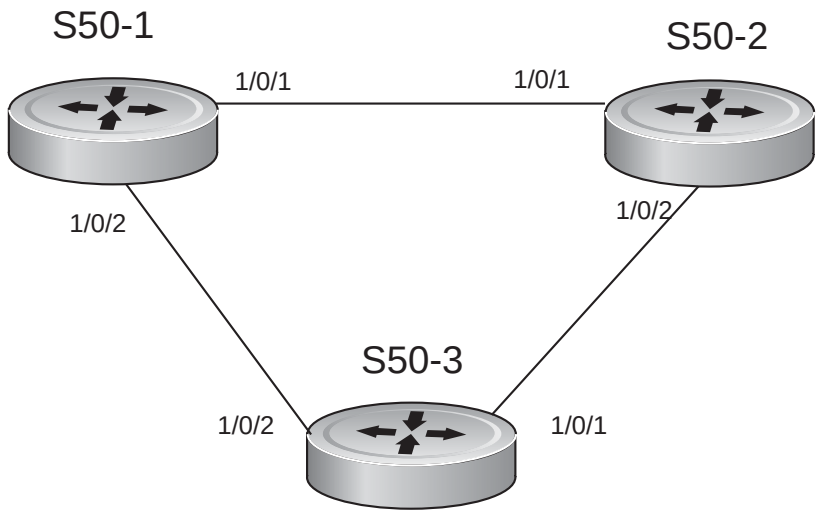


Figure 112 Spanning Tree Topology Example

Note: This example uses the CLI to set up a spanning tree (STP). For details on using the SFTOS Web UI for STP, see Spanning Tree Protocol on page 92.

1. Use the **show spanning-tree interface** command and **show spanning-tree summary** command to determine if STP is initially disabled on the interface and globally (See Figure 120 on page 148 and Example Output from show spanning-tree mst port summary Command for Individual Ports on page 150). Use **show spanning-tree brief** (see Figure 121 on page 149) to determine the current bridge characteristics.
2. On each participating switch, use the **spanning-tree** command (Global Config mode) to enable Spanning Tree Protocol (STP).

```
S50-1 #config
S50-1 (Config)#spanning-tree

S50-2 #config
S50-2 (Config)#spanning-tree

S50-3 #config
S50-3 (Config)#spanning-tree
```

Figure 113 Using the spanning-tree Command

3. Use either the **spanning-tree port mode enable all** command (Global Config mode) to enable Spanning Tree on all ports (as shown in Figure 114), or use the **spanning-tree port mode enable** command (Interface Config mode) (Figure 115) to enable selected ports.

```
S50-1 (Config)#spanning-tree port mode enable all

S50-2 (Config)#spanning-tree port mode enable all
```

Figure 114 Using the spanning-tree port mode enable all Command

To enable STP on individual ports:

```
S50-3 (Config)#interface 0/1
S50-3 (Interface 0/1)#spanning-tree port mode enable
S50-3 (Interface 0/1)#exit
S50-3 (Config)#interface 0/2
S50-3 (Interface 0/2)#spanning-tree port mode enable
```

Figure 115 Using the spanning-tree port mode enable Command

4. Use the **show spanning-tree** command to verify the STP convergence (see Figure 122 on page 149) and **show spanning-tree mst port summary** command (see Figure 123 on page 150) for behaviour of ports participating in the spanning tree.

Note: Another configuration example is in MSTP configuration example on page 144.

Changing Spanning Tree Global Parameters

The Spanning Tree protocol (STP) in SFTOS has the following operational parameters that you can change from their defaults.

Command Syntax	Command Mode	Purpose
[**no**] **spanning-tree forward-time** *4-30*	Global Config	Set the Bridge Forward Delay forward-time value for the common and internal spanning tree, with the value being greater than or equal to "(Bridge Max Age / 2) + 1". Range: 4 to 30 seconds Default: 15 seconds
spanning-tree hello-time *1-10*	Global Config	Set the Admin Hello Time for the common and internal spanning tree, with the value being less than or equal to "(Bridge Max Age / 2) - 1". Range: 1 to 10 seconds Default: 2 seconds
spanning-tree max-age *6-40*	Global Config	Set the Bridge Max Age for the common and internal spanning tree, with the value being less than or equal to "2 times (Bridge Forward Delay - 1)". Range: 6 to 40 seconds Default: 20 seconds
spanning-tree max-hops *1-127*	Global Config	Set the MSTP Max Hops value for the common and internal spanning tree. Range: 1 to 127 Default: 20

Enabling an Edge Port

Note: Only interfaces connected to end stations should be set up as edge ports. Edge ports in 802.1D mode are not supported.

The edge port feature (Portfast) enables interfaces to begin forwarding packets immediately after they are connected. When enabled as an edge port, an interface skips the blocking and learning states so that it can start forwarding traffic sooner (typically saving 30 seconds that the switch would use to check for loops). To enable an edge port, use the following command.

Command Syntax	Command Mode	Purpose
[**no**] **spanning-tree edgeport**	Interface Config or Interface Range	Enable an edge port on an interface.

Multiple Spanning-Tree Protocol (MSTP, IEEE 802.1s)

Multiple Spanning Tree Protocol (MSTP) allows LAN traffic to be channeled over different interfaces. MSTP also allows load balancing without increasing CPU usage.

Rapid reconfiguration minimizes the time to recover from network outages, and increases network availability.

SFTOS supports IEEE 802.1D, IEEE 802.1s, and IEEE 802.1w (see Setting the STP Version Parameter on page 137). The default spanning tree mode in SFTOS is IEEE 802.1s, supporting MSTP:

- The overall Root bridge for 802.1s is calculated in the same way as for 802.1D or 802.1w.
- IEEE 802.1s bridges can interoperate with IEEE 802.1D and IEEE 802.1w bridges

Important Points to Remember

- MSTP instances can only exist within a region.
- One Common Instance (CIST) and four additional Multiple Instances (MSTIs) are supported.
- Each port supports multiple STP states, with one state per instance. Thus, a port can be in the forwarding state in one instance and blocking in another instance.
- MSTP BPDUs appear as normal BPDUs for the CIST while including information for the MSTIs (one record for each MSTP Instance). The CIST is mapped to Instance 0.
- VLANs are associated with one and only one instance of STP.
- Multiple VLANs can be associated with an STP instance.

MSTP Implementation

MSTP is part of the SFTOS switching package. Either IEEE 802.1D or IEEE 802.1s operates at any given time. The following is the SFTOS implementation of MSTP:

- One Common Instance (CIST) and 4 additional Multiple Instances (MSTIs)
- VLANs are associated with one and only one instance of Spanning Tree
- Multiple VLANs can be associated with an Instance of Spanning Tree
- Each port supports multiple STP states, one state per instance. (For example, a port can be Forwarding in one instance while Blocking in another instance.)

MST Regions

A Multiple Spanning Tree region is a collection of MST bridges that share the same VLAN-to-STP instance mappings. They are administratively configured on each MST Bridge in the network.

MST regions are identified by:

- 32-byte alphanumeric configuration name
- Two-byte configuration revision number
- The mapping of VLAN IDs to STP instance numbers

MST Interactions

Bridge Protocol Data Units (BPDU) considerations:

- MSTP instances can only exist within a region.
- MSTP instances never interact outside a region.
- MSTP BPDUs appear as normal BPDUs for the CIST while including information for the MSTIs (one record for each MSTP Instance).
- The CIST is mapped to Instance 0.
- Both ends of a link may send BPDUs at the same time, as they may be the designated ports for different instances.

MSTP Standards

- SFTOS conforms to IEEE 802.1s.
- SFTOS is compatible with IEEE 802.1w and IEEE 802.1D.
- SNMP management is via a private MIB, as no standard MIB exists.

MST CLI Management

Privileged Exec and User Exec mode display (show) commands

- Display STP settings and parameters for the switch:
  - **show spanning-tree summary**
- Display settings and parameters for all MST instances:
  - **show spanning-tree mst summary**
- Display settings and parameters for one MST instance:
  - **show spanning-tree mst detailed** *mstid*
- Display settings and parameters for the CIST:
  - **show spanning-tree** [**brief**]
- Display the association between an MST instance and a VLAN:
  - **show spanning-tree vlan** *vlanid*
- Display settings and parameters for a port within an MST instance:
  - **show spanning-tree mst port summary** *mstid* {*slot/port* | **all**}
  - **show spanning-tree mst port detailed** *mstid slot/port*
- Display settings and parameters for a port within the CIST:
  - **show spanning-tree interface** *slot/port*

Global Config mode CLI commands

- [Disable] enable STP operational state for the switch:
  - **[no] spanning-tree**
- [Disable] enable STP administrative state for all ports:
  - **[no] spanning-tree port mode enable all**
- [Reset] set the STP protocol version for the switch:
  - **spanning-tree forceversion {802.1d | 802.1w | 802.1s}**
- [Reset] set a configuration name to identify the switch:
  - **[no] spanning-tree configuration name** *name*
- [Reset] set the configuration revision level for the switch:
  - **[no] spanning-tree configuration revision** *0-65535*
- [Reset] set max-age for the CIST:
  - **[no] spanning-tree max-age** *6-40*
- [Reset] set forward-time for the CIST:
  - **[no] spanning-tree forward-time** *4-30*
- [Reset] set hellp-time for the CIST:
  - **[no] spanning-tree hello-time** *1-10*
- [Remove] add an MST instance:
  - **[no] spanning-tree mst** *mstid*
- [Reset] set the bridge priority for an MST instance:
  - **[no] spanning-tree mst priority** *mstid 0-61440*

- [Remove] add a VLAN to an MST instance:
  - **[no] spanning-tree mst vlan** *mstid vlanid*

Interface Config mode CLI commands

[Disable] enable administrative state for the port:

- **[no] spanning-tree port mode enable**

- [Reset] set the path cost for this port for the MST instance, or for the CST if the mstid is 0. (Auto sets the cost based on the link speed.):
  - **[no] spanning-tree mst** *mstid* **{cost** *1-200000000* **| auto}**
- [Reset] set the port priority for this port for the MST instance, or for the CST, in increments of 16:
  - **[no] spanning-tree mst** *mstid* **port-priority** *0-240*
- [Reset] set a port as an edge port within the CST:
  - **[no] spanning-tree edgeport**

The edge port feature enables interfaces to begin forwarding packets immediately after they are connected. With an edge port enabled, an interface does not go through the Blocking and Learning states and forwards traffic sooner. Only interfaces connected to end stations should be set up as edge ports. To enable an edge port on an interface, use the **spanning-tree edgeport** command in either Interface Config mode or Interface Range mode.

MSTP configuration example

The following example creates two MST instances to accommodate two bridged VLANs. The fact that this example shows the same port numbers participating in the same two VLANs on each participating switch — R4, R5, and R7 — is simply an expedient way to clone the configuration steps.

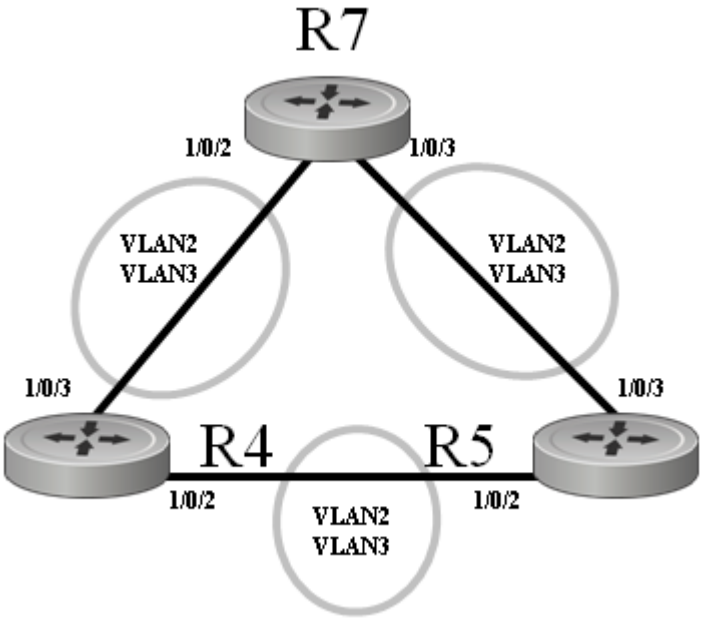


Figure 116 MSTP Topology Example

1. Configure switch R7. Enable STP globally and on associated ports; create MST instances and associated VLANs:

```
R7 (Config)#spanning-tree
R7 (Config)#spanning-tree configuration name spt1
R7 (Config)#spanning-tree configuration revision 1
R7 (Config)#spanning-tree mst instance 2
R7 (Config)#spanning-tree mst vlan 2 2
R7 (Config)#spanning-tree mst instance 3
R7 (Config)#spanning-tree mst vlan 3 3
R7 (Config)#interface 0/2
R7 (Interface 0/2)#no shutdown
R7 (Interface 0/2)#spanning-tree port mode enable
R7 (Interface 0/2)#exit
R7 (Config)#interface 0/3
R7 (Interface 0/3)#no shutdown
R7 (Interface 0/3)#spanning-tree port mode enable
R7 (Interface 0/3)#exit
R7 (Config)#interface vlan 2
R7 (Conf-if-vl-2)#tagged 0/2
R7 (Conf-if-vl-2)#tagged 0/3
R7 (Conf-if-vl-2)#exit
R7 (Config)#interface vlan 3
R7 (Conf-if-vl-3)tagged 0/2
R7 (Conf-if-vl-3)tagged 0/3
```

Figure 117 MST Configuration on Switch R7

2. Configure switch R4, as above:

```
R4 (Config)#spanning-tree
R4 (Config)#spanning-tree configuration name spt1
R4 (Config)#spanning-tree configuration revision 1
R4 (Config)#spanning-tree mst instance 2
R4 (Config)#spanning-tree mst vlan 2 2
R4 (Config)#spanning-tree mst instance 3
R4 (Config)#spanning-tree mst vlan 3 3
R4 (Config)#interface 0/2
R4 (Interface 0/2)#no shutdown
R4 (Interface 0/2)#spanning-tree port mode enable
R4 (Interface 0/2)#exit
R4 (Config)#interface 0/3
R4 (Interface 0/3)#no shutdown
R4 (Interface 0/3)#spanning-tree port mode enable
R4 (Interface 0/3)#exit
R4 (Config)#interface vlan  2
R4 (Conf-if-vl-2)#tagged 0/2
R4 (Conf-if-vl-2)#tagged 0/3
R4 (Conf-if-vl-2)#exit
R4 (Config)#interface vlan 3
R4 (Conf-if-vl-3)tagged 0/2
R4 (Conf-if-vl-3)tagged 0/3
```

Figure 118 MST Configuration on R4

3. Configure switch R5, as above:

```
R5 (Config)#spanning-tree
R5 (Config)#spanning-tree configuration name spt1
R5 (Config)#spanning-tree configuration revision 1
R5 (Config)#spanning-tree mst instance 2
R5 (Config)#spanning-tree mst vlan 2 2
R5 (Config)#spanning-tree mst instance 3
R5 (Config)#spanning-tree mst vlan 3 3
R5 (Config)#interface 0/2
R5 (Interface 0/2)#no shutdown
R5 (Interface 0/2)#spanning-tree port mode enable
R5 (Interface 0/2)#exit
R5 (Config)#interface 0/3
R5 (Interface 0/3)#no shutdown
R5 (Interface 0/3)#spanning-tree port mode enable
R5 (Interface 0/3)#exit
R5 (Config)#interface vlan 2
R5 (Conf-if-vl-2)#tagged 0/2
R5 (Conf-if-vl-2)#tagged 0/3
R5 (Conf-if-vl-2)#exit
R5 (Config)#interface vlan 3
R5 (Conf-if-vl-3)tagged 0/2
R5 (Conf-if-vl-3)tagged 0/3
```

Figure 119 MST Configuration on R5

4. Use the **show spanning-tree** command to verify the STP convergence (see Figure 122 on page 149) and **show spanning-tree mst port summary** command (see Figure 123 on page 150) for behaviour of ports participating in the spanning tree.

Note: Another configuration example is in Example of Configuring STP on page 138.

Rapid Spanning Tree Protocol (RSTP)

SFTOS supports Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) as a non-default mode. See Setting the STP Version Parameter on page 137.

RSTP provides faster convergence than Spanning Tree Protocol (STP) and interoperability with other switches configured with STP and MSTP.

RSTP Implementation

Port Roles

RSTP adds new port roles to STP.

Port roles that forward include:

- Root Port: This is the port that is the closest to the root bridge based on path cost. A bridge sends traffic on this port to the root.
- Designated Port: This is the port that is the closest to the root bridge based on path cost. A bridge receives traffic on this port from others on the segment.

Port roles that do not forward include:

- Alternate Port: This is a port that is an alternate path to the root on a different bridge than the designated bridge.
- Backup Port: This is a port that is an alternate path to the root on the designated bridge.
- Disabled Port: This is a port that has no role in RSTP.

Port States

RSTP merges states from STP, leaving just three possible operational states. The 802.1D blocking and disabled states are merged into the 802.1w discarding state. The 802.1D learning and listening states are merged into the 802.1w learning state.

Port Costs

RSTP introduces new default port costs.

BPDU Format

RSTP has a unique BPDU format that uses all bits of the Flags field to communicate additional states. The RSTP BPDUs act as a keep-alive between bridges, allowing for significantly faster link failure detection.

Convergence with RSTP

The faster convergence with RSTP results from the use of BPDUs as keep-alives between adjacent switches, which establish the state before passing information to the downstream device. In contrast, the pre-RSTP version of STP uses timers to allow BPDUs to flow from root to all leaves. Non-edge ports stay a set time in listening and learning modes to gather all available BPDU information to decide the port state.

Configuration Task List for RSTP

RSTP uses the same commands as used in STP (see Spanning Tree Configuration Tasks on page 137) to enable RSTP on the switch and on interfaces, to set global parameters, and to display configuration (see below). The following command is the only one in SFTOS to contain any RSTP specifiicity:

Command Syntax	Command Mode	Purpose
spanning-tree bpdumigrationcheck {*slot/port* | **all**}	Global Config	Force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *slot/port* parameter to transmit a BPDU from a specified interface, or use the **all** keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a **no** version. Use the **show interface ethernet** *slot/port* command to display BPDU counters. See Figure 129 on page 153.

Display Spanning Tree Configuration

Use the **show spanning-tree interface** command and **show spanning-tree summary** command (Figure 120) to verify that STP is initially disabled, both on interfaces and globally:

```
Force10 #show spanning-tree interface 0/1
Hello Time..................................... 0
Port Mode...................................... Enabled
Port Up Time Since Counters Last Cleared....... 0 day 4 hr 50 min 17 sec
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0

Force10 #show spanning-tree summary
Spanning Tree Adminmode........... Enabled
Spanning Tree Version............. IEEE 802.1s
Configuration Name................ 00-01-E8-D5-A7-82
Configuration Revision Level...... 0
Configuration Digest Key.......... 0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0
No MST instances to display.
```

Figure 120 Example Output from show spanning-tree interface Command

Use the **show spanning-tree brief** command (Figure 121) to determine current bridge characteristics:

```
Force10 #show spanning-tree brief

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:00:01:E8:D5:A7:82
Bridge Max Age............................... 20
Bridge Max Hops.............................. 20
Bridge Hello Time............................ 2
Bridge Forward Delay......................... 15
Bridge Hold Time............................. 3
```

Figure 121 Example Output from spanning-tree brief Command

Use the **show spanning-tree** command to verify that STP has converged. In Figure 122, executing the command on three participating switches shows that they have merged into one spanning tree, selecting S50-1 as the root bridge:

```
S50-1 #show spanning-tree

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:00:01:E8:D5:A7:82   <-- Bridge ID selected as root bridge by each switch
Time Since Topology Change................... 0 day 0 hr 0 min 19 sec
Topology Change Count........................ 3
Topology Change in progress.................. TRUE
Designated Root.............................. 80:00:00:01:E8:D5:A7:82   <-- Designated Root = Bridge ID
Root Path Cost............................... 0

S50-2 #show spanning-tree

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:00:01:E8:D5:A7:BE
Time Since Topology Change................... 0 day 0 hr 3 min 21 sec
Topology Change Count........................ 2
Topology Change in progress.................. FALSE
Designated Root.............................. 80:00:00:01:E8:D5:A7:82   <-- Designated Root = Bridge ID
Root Path Cost............................... 20000

S50-3 #show spanning-tree

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:00:01:E8:D5:A8:D6
Time Since Topology Change................... 0 day 0 hr 1 min 23 sec
Topology Change Count........................ 2
Topology Change in progress.................. FALSE
Designated Root.............................. 80:00:00:01:E8:D5:A7:82   <-- Designated Root = Bridge ID
Root Path Cost............................... 20000
```

Figure 122 Example Output from show spanning-tree Command

In Figure 122, all three switches point to S50-1 as the Designated Root (DR), by identifying the bridge ID (MAC address — 00:01:E8:D5:A7:82) of S50-1as the DR. Note also that the Root Path Cost on the DR is 0 (zero), while, on the two other S50s, the Root Path Cost is 20000.

Inspect the output of the **show spanning-tree mst port summary** command for ports participating in the spanning tree:

```
S50-1 #show spanning-tree mst port summary 0 0/1

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type         State            Role
--------- -------- ------- ---------------- ----------
0/1     Enabled          Forwarding        Designated

S50-1 #show spanning-tree mst port summary 0 0/2

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type         State            Role
--------- -------- ------- ---------------- ----------
0/2     Enabled          Forwarding        Designated
```

Figure 123 Example Output from show spanning-tree mst port summary Command for Individual Ports

In Figure 123, S50-1 is the Designated Root (DR), so all of its ports are listed as Forwarding under STP State and the Port Role is Designated for both listed ports. In contrast, note in Figure 124 that 0/1 of S50-2 is listed as Root and 0/2 as Designated.

```
S50-2 #show spanning-tree mst port summary 0 0/1

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type         State            Role
--------- -------- ------- ---------------- ----------
0/1     Enabled          Forwarding        Root

S50-2 #show spanning-tree mst port summary 0 0/2

MST Instance ID.............................. CST

            STP                  STP            Port
Interface   Mode   Type         State            Role
--------- -------- ------- ---------------- ----------
0/2     Enabled          Forwarding        Designated
```

Figure 124 Example Output from show spanning-tree mst port summary Command for Individual Ports

The selection of 0/1 as the root port was based, in this case, on the value of the assigned cost. As shown by the use of the **show spanning-tree mst port detailed** command in Figure 125, the cost through 0/1 is 0 (zero), because it is directly connected to a designated port on the root bridge, and it is receiving a 0 cost value to the root bridge. 0/2 is receiving a cost of 20000 to the root from its connection to 0/2 of S50-3. So the shorter route to the root is through 0/1.

```
S50-2 #show spanning-tree mst port detailed  0 0/1
Designated Port Cost..... 0

S50-2 #show spanning-tree mst port detailed  0 0/2
Designated Port Cost..... 20000
```

Figure 125 Example Output from show spanning-tree mst port detailed Command for Individual Ports

Figure 126 shows the output of the **show spanning-tree mst port summary** command from S50-3 for participating ports:

```
S50-3 #show spanning-tree mst port summary 0 0/1

MST Instance ID..... CST

            STP                  STP            Port
Interface   Mode   Type         State            Role
--------- -------- ------- ---------------- ----------
0/1     Enabled          Forwarding        Root

S50-3 #show spanning-tree mst port summary 0 0/2

MST Instance ID..... CST

            STP                  STP            Port
Interface   Mode   Type         State            Role
--------- -------- ------- ---------------- ----------
0/2     Enabled          Discarding        Alternate
```

Figure 126 Example Output from show spanning-tree mst port summary Command

In this case (Figure 126), S50-3 has a higher bridge ID than S50-2 and S50-3, so interface 0/2 is in the Discarding state, and the physical loop through that port to S50-1 (Figure 123) is broken.

Figure 126 shows the output of the **show spanning-tree mst port summary** command before lowering the priority of an MST instance:

```
Force10 #show spanning-tree mst port summary 50 all

            STP                  STP            Port
Interface   Mode   Type         State             Role
--------- -------- ------- ----------------- ----------
0/1       Enabled          Disabled          Disabled
0/2       Enabled          Disabled          Disabled
0/3       Enabled          Disabled          Disabled
0/4       Enabled          Disabled          Disabled
0/5       Enabled          Disabled          Disabled
0/6       Enabled          Disabled          Disabled
0/7       Enabled          Disabled          Disabled
0/8       Enabled          Disabled          Disabled
0/9       Enabled          Disabled          Disabled
0/10      Enabled          Forwarding        Designated
0/11      Enabled          Discarding        Backup
0/12      Enabled          Disabled          Disabled
0/13      Enabled          Disabled          Disabled
0/14      Enabled          Disabled          Disabled
0/15      Enabled          Disabled          Disabled
--More-- or (q)uit
```

Figure 127 Example Output from show spanning-tree mst port summary Command

Figure 128 shows the output of the **show spanning-tree mst port summary** command after lowering the priority of the MST instance (contrast to Figure 126):

```
Force10 #show spanning-tree mst port summary 50 all

            STP                  STP            Port
Interface   Mode   Type         State             Role
--------- -------- ------- ----------------- ----------
0/1       Enabled          Disabled          Disabled
0/2       Enabled          Disabled          Disabled
0/3       Enabled          Disabled          Disabled
0/4       Enabled          Disabled          Disabled
0/5       Enabled          Disabled          Disabled
0/6       Enabled          Disabled          Disabled
0/7       Enabled          Disabled          Disabled
0/8       Enabled          Disabled          Disabled
0/9       Enabled          Disabled          Disabled
0/10      Enabled          Discarding        Backup
0/11      Enabled          Forwarding        Designated
0/12      Enabled          Disabled          Disabled
0/13      Enabled          Disabled          Disabled
0/14      Enabled          Disabled          Disabled
0/15      Enabled          Disabled          Disabled
--More-- or (q)uit
```

Figure 128 Example Output from show spanning-tree mst port summary Command

Displaying STP, MSTP, and RSTP Operation

Use the **show interface ethernet** *slot/port* command to display STP, MSTP, and RSTP BPDUs transmitted and received.

```
Force10 #show interface ethernet 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

!---------------<snip>-----------------!

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
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 10 sec
```

Figure 129 Example Output from show interface ethernet Command

Chapter 10 Link Aggregation

This chapter contains the following major sections:

- Link Aggregation—IEEE 802.3
- Link Aggregation Group (LAG) Commands on page 157
- Configuring a LAG on page 158
- Link Aggregation Control Protocol (LACP) on page 164
- Displaying LAGs (Port Channels) on page 166

Link Aggregation—IEEE 802.3

SFTOS supports the IEEE802.3ad Link Aggregation Group (LAG), also called a *port channel*, *Etherchannel group*, or *trunking*, which allows IEEE 802.3 MAC interfaces to be grouped logically to appear as one physical link. LAGs enable you to treat multiple physical links between two end-points as a single logical link, providing automatic redundancy between two devices.

Each link of a LAG must run at the same speed and must be in full-duplex mode. Set the speed and mode of a port to that of the LAG before adding the port to the LAG..

LAGs:

- Behave like any other Ethernet link to a VLAN
- Can be a member of a VLAN
- Are treated as physical ports with the same configuration parameters, spanning tree port priority, path cost, etc.
- Can have a router port member, but routing will be disabled while it is a member.

A LAG is often used to directly connect two switches when the traffic between them requires high bandwidth and reliability, or to provide a higher bandwidth connection to a public network. A LAG can offer the following benefits:

- Increased reliability and availability — if one of the physical links in the LAG goes down, traffic will be dynamically and transparently reassigned to one of the other physical links.
- Better use of physical resources — traffic can be load-balanced across the physical links.
- Increased bandwidth — the aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth — A LAG may be used when a physical upgrade would produce a 10-times increase in bandwidth, but only a two- or five-times increase is required.

LAG Load Distribution

Traffic is distributed (load-balanced) over links in a LAG using a hashing algoritm. Since the packet-forwarding ASICs differ among the S-Series platforms, the load-balancing algorithm is also different. Currently, the CLI does not include a command to change the algorithm.

- **S50**:

  IPv4 packets: The hash is based on the eXclusive OR (XOR) of the 3 least significant bits (LSB) of the source and destination *IP addresses*.

  Non-IP packets: The hash is based on the XOR of the 3 LSBs of the source and destination *MAC addresses*.

- **S50V, S50N, S25P**:

  IPv4 and IPv6 packets: The hash is based on the XOR of the source IP (v4 or v6) address and Layer 4 port with the destination IP (v4 or v6) address and Layer 4 port.

  Non-IP packets: The hash is based on the source and destination MAC addresses, VLAN, type, ingress ASIC, and ingress port.

- **S2410**:

  All packets: The hash is based on the source and destination MAC addresses, type, VLAN, VLAN priority, and ingress port..

On all platforms, MAC addresses must be learned for hashing to work. Broadcast, unknown unicast, and multicast packets are sent to a single port (the lowest numbered port) in the LAG.

LAG Implementation Restrictions

Interface restrictions:

- LAG speed may not be changed.
- Routing is not supported on links in a LAG.
- An interface can belong to only one LAG.
- SFTOS 2.4.1 supports 12 LAGs, with a maximum of 12 members each.
- A LAG cannot have an IP address.
- LAG ports that are shut down before a reboot are removed from the LAG.

SFTOS supports IEEE 802.3 Clause 43 with minor exceptions:

- No optional features supported, e.g. Marker Generator/Receiver
- MUX machine implemented as coupled, not independent control
- Some MIB variables are not supported.

Link Aggregation—MIB Support

The IEEE 802.3 Annex 30c MIB objects that are not supported are:

- dot3adAggPortDebugTable
- dot3adAggPortStatsMarkerResponsePDUsRx
- dot3adAggPortStatsMarkerPDUsTx
- dot3adAggPortActorAdminSystemPriority
- dot3adAggPortActorOperSystemPriority
- dot3adAggPortPartnerAdminSystemPriority
- dot3adAggPortPartnerOperSystemPriority
- dot3adTablesLastChanged

Static LAG Requirements

Manual aggregation is disabled by default, and when enabled, applies to all LAG interfaces. Manual aggregation uses the following default values:

- If an LACP PDU (Link Aggregation Control Protocol Protocol Data Unit) is received with different values, the link drops out.
- When all member links have dropped out, the group will re-aggregate with the new information.
- If the partner does not respond with LACP PDUs, the system waits three seconds and aggregates manually.
- The static LAG configuration should only be enabled if both parties are 802.3ad-compliant and have the protocol enabled.
- LAGs should be configured and STP-enabled on both devices before connecting cables.

Link Aggregation Group (LAG) Commands

Note: The [**no**] **port lacpmode enable** command (Interface Config mode) and [**no**] **port lacpmode enable all** command (Global Config mode) are deprecated.

The CLI commands in Global Config mode used to create a LAG are:

- To [enable] disable LACP (enabled by default) for all LAGs:
  - [**no**] **port-channel staticcapability**
- To configure the LAG:
  - [**no**] **port-channel** {*name* | **enable all**}

    Use **show port-channel all** to display the logical *slot/port* (see below).
  - **port-channel name** {*slot/port* | **all**} *name*

    In the case of logical interfaces, such as this is, the *slot/port* is automatically expressed as 1/[sequential #].
  - [**no**] **port-channel linktrap** {*slot/port* | **all**}

— (at the LAG prompt) **spanning-tree** {**edgeport** | **hello-time** | **port** | **mst**} (Specify **edgeport** for fast, **no spanning-tree edgeport** for 802.1d.)

- To [disable] enable the administrative mode for all LAGs:
  — [**no**] **port-channel enable all**
- To delete all ports from a LAG:
  — **deleteport** *slot/port* **all**
- To delete a LAG or all LAGs:
  — **no port-channel** {*slot/port* | **all**}

The CLI commands in Interface Config mode used to configure and manage a LAG are:

- To [enable] disable the selected LAG:
  — [**no**] **shutdown**
  (Access the LAG from Global Config mode with interface **1/***port_number*. Learn the *port_number* from **show port-channel brief** (see below).)
- Add the selected port to a designated LAG:
  — **addport** *slot/port* (where *slot/port* is the logical interface defined by the system for the LAG)
- Delete the selected port from a designated LAG:
  — **deleteport** *slot/port*

In Privileged Exec mode, display LAG members and link speed:

- **show port-channel** {*slot/port* | **all** | **brief**} (where *slot/port* is the logical interface defined by the system for the LAG). **show port-channel brief** is also in User Exec mode. It displays whether static capability is enabled.

Static LAG CLI Management

Global Config mode commands to disable/enable static capability for the switch:

- **port-channel staticcapability**
  — All LAGs with configured members but no active members will now aggregate statically on link UP interfaces
- **no port-channel staticcapability**
  — Active members of static LAGs will drop. A LAG with no active members will go down.

Configuring a LAG

Use the following procedure to create and configure a LAG (port channel).

Step	Command Syntax	Command Mode	Purpose
1	**show port-channel all**	Privileged Exec	Display current settings.

Step	Command Syntax	Command Mode	Purpose
2	**port-channel** *name*	Global Config	Create the LAG. For the *name* variable, enter a character string that uniquely identifies the LAG from other configured LAGs. The character string allows the dash "-" character as well as alphanumeric characters.
3	**show port-channel brief** or **show port-channel all**	Privileged Exec	Discover the logical interface ID assigned to the LAG name. (The switch autonumbers the logical slot/port in the form 1/[sequential integer]; for example, the second LAG created is 1/2. You need to use this command to verify the logical interface IDs, which you use to identify the LAG in subsequent steps.)
4	**interface** *slot/port*	Global Config	Access a physical port to add to the LAG. (You cannot add a LAG to a LAG.)
5	**no shutdown**	Interface Config	Enable the LAG.*
6	**addport** *slot/port*	Interface Config	Add the port to the LAG designated by *slot/port*.
7		Global Config	Repeat steps 4-6 to add more ports to the LAG.
8		Global Config	Repeat sequence for another LAG.
9	**port-channel enable all**	Global Config	*If you do not enable a specific LAG with the **no shutdown** command, above, use this to command to enable all LAGs.
10	**port-channel staticcapability**	Global Config	(OPTIONAL) Create static LAGs.

LAG Configuration Example

This example is of configuring the S-Series to support LAGs to a server and to a Layer 2 switch.

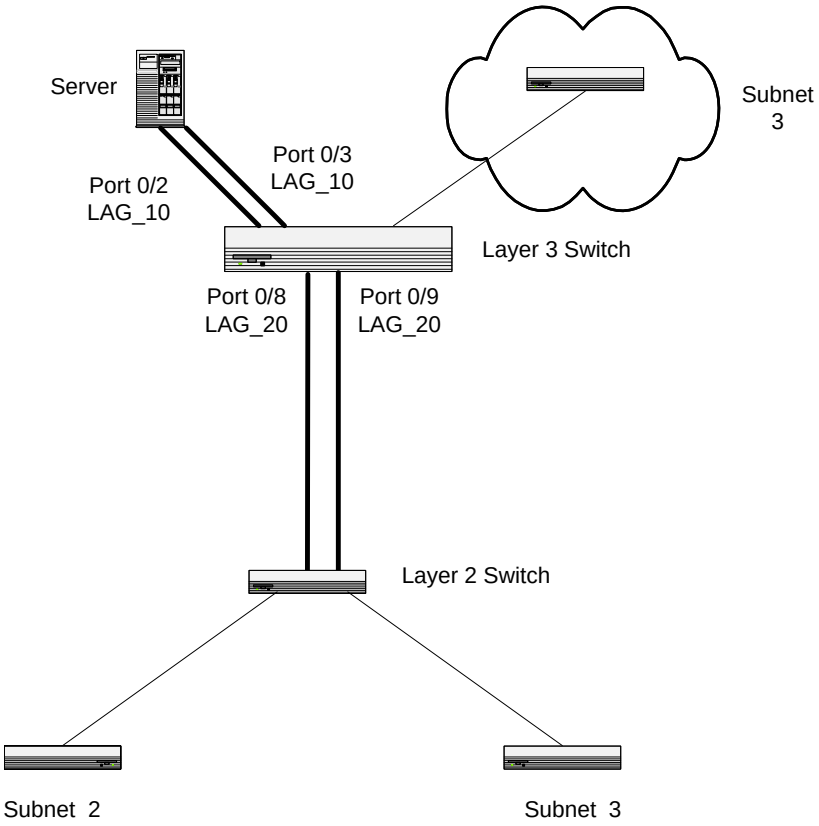


Figure 130 LAG Example in Network Diagram

1. Create two LAGs.

```
Force10 #config
Force10 (Config)#port-channel lag_10
Force10 (Config)#port-channel lag_20
```

2. Run the **show port-channel** command (see Figure 132 on page 162). This command returns the logical interface IDs that identify the LAGs in subsequent commands. Assume that lag_10 is assigned ID 1/1 and lag_20 is assigned ID 1/2.

3. Add the ports to the appropriate LAG.

```
Force10 (Config)#interface 0/2
Force10 (Interface 0/2)#addport 1/1
Force10 (Interface 0/2)#exit
Force10 (Config)#interface 0/3
Force10 (Interface 0/3)#addport 1/1
Force10 (Interface 0/3)#exit
Force10 (Config)#interface 0/8
Force10 (Interface 0/8)#addport 1/2
Force10 (Interface 0/8)#exit
Force10 (Config)#interface 0/9
Force10 (Interface 0/9)#addport 1/2
Force10 (Interface 0/9)#exit
```

For example, “0/2” is the port and “1/1” is the LAG to which it is being added.

Figure 131 Adding Ports to a LAG

4. Enable both LAGs. Link trap notification will be enabled by default.

```
Force10 (Config)#port-channel enable all
Force10 (Config)#exit
```

5. Verify the configuration with the **show port-channel** command.
6. At this point, the LAGs could be added to VLANs. See Adding a LAG to a VLAN on page 162.

The following example shows, in one sequence, the LAG creation commands described above. Here, the two LAGs created above (“test” and “test1”) already exist, and two more are being created:

```
!Example command sequence to configure LAG ports!
Force10 #show port-channel all
            Port-                  Link
Log.       Channel             Adm. Trap  STP           Mbr      Port    Port
Intf        Name        Link   Mode Mode  Mode   Type   Ports    Speed   Active
------ --------------- ------ ---- ---- ------ ------- ------ --------- ------
1/1  test            Down   En.  En.  Dis.   Dynamic0/2      Auto      False
                                                  0/3      Auto      False
1/2  test1           Down   En.  En.  Dis.   Dynamic0/8      Auto      False
                                                  0/9      Auto      False

Force10 #config
Force10 (Config)#port-channel Lag_10
Force10 (Config)#port-channel Lag_20
Force10 (Config)#exit
Force10 #show port-channel brief
Static Capability: Disabled
Logical Interface Port-Channel Name Link State Mbr Ports Active Ports
----------------- ---------------- ---------- --------- ------------
1/1             test              Down       0/2, 0/3
1/2             test1             Down      0/8, 0/9
1/3               Lag_10           Down
1/4               Lag_20           Down

Force10 (Config)#interface 0/5
Force10 (Interface 0/5)#addport 1/3
Force10 (Interface 0/5)#exit
Force10 (Config)#interface 0/6
Force10 (Interface 0/6)#addport 1/3
Force10 (Interface 0/6)#exit
Force10 (Config)#interface 0/7
Force10 (Interface 0/7)#addport 1/3
Force10 (Interface 0/7)#exit
Force10 (Config)#interface 0/8
Force10 (Interface 0/8)#addport 1/4
Force10 (Interface 0/8)#exit
Force10 (Config)#interface 0/9
Force10 (Interface 0/9)#addport 1/4
Force10 (Interface 0/9)#exit
Force10 (Config)#interface 0/10
Force10 (Interface 0/10)#addport 1/4
```

Figure 132 Example of LAG Creation and Configuration

Adding a LAG to a VLAN

You can add a Layer 2 LAG (port channel) to a VLAN, just as you do with physical interfaces. In the case of a LAG, however, the *slot/port* ID is the logical ID of the LAG (such as 1/1), which you learn from the **show port-channel all** command, as shown in Figure 132. Configure the LAG, as described above in Configuring a LAG on page 158). Then use the following commands to add the LAG to the VLAN
For details, see Creating the VLAN and Adding Ports on page 178.
For an example of adding a LAG to a VLAN, see Example of adding a LAG to a VLAN on page 183.)
To see which LAGs are members of VLANs, use the **show vlan** command (Privileged Exec mode). :

Command Syntax	Command Mode	Purpose
[**no**] **tagged** *slot/port* or [**no**] **untagged** *slot/port*	Interface VLAN Config	Add [or remove] an existing LAG in its logical slot/port format, such as 1/1 from the VLAN. Get the LAG ID from the **show port-channel all** output.

Using the Interface Range Mode

If you are applying the same configuration elements to a number of LAGs (also called bulk configuration), you can replicate the steps above for all of those LAGs from the Interface Range mode. The System Configuration chapter in the *SFTOS Command Reference* provides details on the command syntax used for the **interface range** command to define the range and access the mode.

The command families available from the VLAN Range and Port Channel Range prompts within that mode are displayed, respectively, in the following CLI example (Figure 133 on page 163).

```
Force10 (conf-if-range-vl-100-200)#?
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.
participation            Configure how ports participate in a specific VLAN.
priority                 Configure the priority for untagged frames.
protocol                 Configure the Protocols associated with particular Group Ids.
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-range-vl-100-200)#
Force10 (Config)#interface range port-channel 1/1-1/2
Force10 (conf-if-range-po-1/1-1/2)#?
addport                  Add this port to a port-channel.
auto-negotiate           Enables/Disables automatic negotiation on a port.
description              Add Description to the interface
exit                     To exit from the mode.
mtu                      Sets the default MTU size.
port-channel             Enable/Disable the port-channel's administrative mode.
port-security            Enable/Disable Port MAC Locking/Security for interface.
routing                  Enables routing for an interface, Use no form to disable.
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.

Force10 (conf-if-range-po-1/1-1/2)#
```

Figure 133 Commands Available in Interface Range Mode

Link Aggregation Control Protocol (LACP)

The Link Aggregation Control Protocol (LACP) provides a standardized means of exchanging information between two systems (also called partner systems) and dynamically establishing LAGs between the two partner systems.

LACP allows the exchange of messages on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the LAG to which the link belongs, move the link to that LAG, and enable the transmission and reception functions in an orderly manner.

The SFTOS implementation of LACP is based on the standards specified in the IEEE 802.3: "*Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*."

LACP works by constantly exchanging custom MAC PDUs across LAN Ethernet links. The protocol packets are only exchanged between ports that are configured to be LACP-capable.

See also Static LAG Requirements on page 157 and Static LAG CLI Management on page 158.

LACP Configuration

SFTOS enables the user to enable LACP and configure LACP timeout characteristics for the system and for a particular port. The following commands configure LACP:

Command Syntax	Command Mode	Purpose
port-channel staticcapability	Global Config	LACP is enabled by default. Use this command to disable LACP at the system level. Use the **no** form to revert to LACP.
[**no**] **port lacptimeout** {**short all | long all**}	Global Config	To configure the system LACP timeout.
[**no**] **port lacptimeout** {**short | long**}	Interface Config	To configure the LACP timeout at a port level.

Note: The **port lacpmode enable** and **port lacpmode enable all** commands are deprecated.

The following example shows the assignment of ports to a LAG and then the enabling of the LAGs:

```
Force10 (Config)#port-channel 2
Force10 (Config)#exit
Force10 #show port-channel all

Log.       Port-           Link
Slot/     Channel          Admin Trap  STP           Mbr      Port    Port
Port       Name       Link Mode  Mode  Mode   Type   Ports    Speed   Active
----- --------------- ---- ----- ---- ------ ------- ------ --------- ------
1/1      2            Down En.   En.   Dis.   Dynamic

Force10 #configure
Force10 (Config)#interface 0/6
Force10 (Interface 0/6)#addport 1/1
Force10 (Interface 0/6)#exit
Force10 (Config)#interface 0/7
Force10 (Interface 0/7)#addport 1/1
Force10 (Interface 0/7)#exit
Force10 (Config)#exit
Force10 #show port-channel all

Port- Link

Log.       Port-           Link
Slot/     Channel          Admin Trap  STP           Mbr      Port    Port
Port       Name       Link Mode  Mode  Mode   Type   Ports    Speed   Active
----- --------------- ---- ----- ---- ------ ------- ------ --------- ------
1/1     2             Down En.    En.  Dis.   Dynamic 0/6       Auto   False
                                                      0/7       Auto   False

Force10 (Config)#interface 0/6
Force10 (Interface 0/6)#no shut
Force10 (Interface 0/6)#exit
Force10 (Config)#interface 0/7
Force10 (Interface 0/7)#no shut
Force10 (Interface 0/7)#exit
Force10 (Config)#exit
Force10 #show port-channel all

Log.       Port-           Link
Slot/     Channel          Admin Trap  STP           Mbr      Port    Port
Port       Name       Link Mode  Mode  Mode   Type   Ports    Speed   Active
----- --------------- ---- ----- ---- ------ ------- ------ --------- ------
1/1     2             Up   En.    En.  Dis.   Dynamic 0/6       Auto    True
                                                     0/7       Auto    True

Force10 #configure
Force10 (Config)# port-channel staticcapability
```

"Dynamic" shows that the LAG is LACP-enabled.

Use this command if you want to convert all LAGs to static. Note that the LAG Type will be listed as "Dynamic" if no port in the LAG is active.

Figure 134 Example of Enabling of LACP with LAG Configuration

Displaying LAGs (Port Channels)

The example in Figure 134 takes a longer route to enable the ports in order to show the difference in two reports generated by the **show port-channel all** command—one generated before enabling the ports and one after. The LAG configuration resulting from the example in Figure 132 is shown in the following example screen (Figure 135).

```
Force10 #show port-channel all

Log.       Port-                Link
Slot/     Channel          Admin Trap  STP           Mbr      Port    Port
Port       Name       Link Mode  Mode  Mode   Type   Ports    Speed   Active
----- --------------- ---- ----- ---- ------ ------- ------ --------- ------
1/3 lag-10          Down En.   En.  En.    Dynamic 0/5 Auto      False
                                                   0/6 Auto       False
                                                   0/7 Auto       False

1/4 lag_20          Down En.   En.  En.    Dynamic 0/8    Auto      False
                                                   0/9 Auto       False
                                                   0/10 Auto      False
```

Figure 135 Displaying LAGs

MAC Addresses Displayed

To display MAC addresses, execute the **show mac-addr-table** command:

```
Force10 S2410#show mac-addr-table

      Mac Address        Interface  IfIndex     Status
----------------------  ---------  -------  ------------
00:01:00:01:00:00:00:37   0/1     1        Learned
00:01:00:03:00:00:00:03   0/2     2        Learned
00:01:00:D0:95:B7:CD:2E 3/1     25       Management
00:01:00:01:E8:07:10:18   1/1   26       Learned
```

Figure 136 Displaying LAG Configuration by MAC Address

Port IDs that start with 1, such as 1/1 in the Interface column in Figure 136 indicate LAGs.

The 3/1 in the Interface column of Figure 136 references the Ethernet Management port.

In the S2410, IfIndex values are:

Port Types	**IfIndex Range**
Physical ports	1 through 24 (24 ports)
Ethernet Management port (labelled *"10/100 Ethernet"*, also called *service port*):	25
LAGs (port channels)	26 to 37 (12 possible LAGs)

Display LACP Configuration

You can use either the **show port** or **show port all** commands to display LACP Configuration, as shown in Figure 137:

```
(Force10_S50) #show port 0/1

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

(Force10_S50) #show port all
             Admin   Physical   Physical   Link   Link    LACP
Intf   Type    Mode    Mode       Status   Status  Trap    Mode
------ ------ ------- ---------- ---------- ------ ------- -------
0/1         Enable  Auto                  Down   Enable  Enable
0/2         Enable  Auto       1000 Full  Up     Enable  Enable
0/3         Disable Auto                  Down   Enable  Enable
0/4         Disable Auto                  Down   Enable  Enable
0/5         Disable Auto                  Down   Enable  Enable
0/6         Disable Auto                  Down   Enable  Enable
0/7         Disable Auto                  Down   Enable  Enable
0/8         Disable Auto                  Down   Enable  Enable
0/9         Disable Auto                  Down   Enable  Enable
0/10        Disable Auto                  Down   Enable  Enable
0/11        Disable Auto                  Down   Enable  Enable
0/12        Disable Auto                  Down   Enable  Enable
0/13        Disable Auto                  Down   Enable  Enable
!---- output truncated ---------------!
```

Figure 137 Using show port command to display LACP Configuration

Chapter 11 Quality of Service

To support Quality of Service (QoS) policies, SFTOS 2.4.1 contains Class of Service commands (CoS) commands, but no DiffServ commands. For syntax details on those commands, see the Quality of Service (QoS) Commands chapter in the *SFTOS Command Reference*.

The following QoS features are supported in SFTOS 2.4.1:

- Queuing based on dot1p priority values
  - Use the **classofservice dot1p-mapping** *userpriority trafficclass* command to configure. Select a *userpriority* from 0-7 and then pair it with a *trafficclass* from 0-3.
  - Use the **classofservice trust** *dot1p* command to set the class of service trust mode to Dot1p (802.1p).
  - Use the **show classofservice dot1p-mapping** [*slot/port*] command to display settings. There is no **show** command for queue counters.
- Traffic shaping (only in Global Config mode; no command in Interface Config mode)
  - Using the **traffic-shape** *bw* command (only for egress rate-shaping), set *bw* (the bandwidth percentage) as an increment of 5, up to 100 (percent).
- Rate limiting on queue basis (no **show** command for queue counters)
  - Using the [**no**] **cos-queue max-bandwidth** *bw-0…bw-3* command, the *bw* represents the maximum bandwidth assigned to the queue designated by the number suffix (one of the four S2410 queues). For example, enter **cos-queue max-bandwidth** 10-0 for a maximum bandwidth of 10% in queue 0.
  - The **cos-queue min-bandwidth** *bw-0… bw-3* command is for the minimum bandwidth assigned to the designated queue(s), as described above.
  - The [**no**] **cos-queue strict** *queue-id* [*queue-id* [*queue-id* [*queue-id*]]] command activates the strict priority scheduler mode for each specified queue.
  -
  - The **show interfaces cos-queue** [*slot/port*] command displays the class-of-service queue configuration for the specified interface.
- Weighted Random Early Detection (WRED) (no **show** command to see the queue counters)
  - [**no**] **cos-queue random-detect** *queue-id* [*queue-id* [*queue-id* [*queue-id*]]] activates WRED for each specified queue. The **no** version of this command disables WRED, thereby restoring the default tail drop operation for the specified queue(s). See also:
  - **random-detect exponential-weighting-constant** *1-15*: Set the decay exponent used by the WRED average queue depth calculation for the interface.
  - **random-detect queue-parms**: Set the WRED parameters for each drop precedence level supported by a queue.

The following QoS features are not supported in SFTOS 2.4.1:

- Rate policing
- Marking
- Queuing based on classification
- Redirection based on classification
- Mirroring based on classification

By default, SFTOS 2.4.1 configures its four egress queues in weighted round robin mode with equal minimum bandwidths. This means that no egress queue is given priority over any other. To change this, in weighted round robin mode, use the **cos-queue min-bandwidth** command to assign minimum bandwidths to each queue. You should then see queue 3 get the appropriate share of the bandwidth.

Alternatively, use the **cos-queue strict** command to force strict priority mode, which will give egress queue 3 absolute priority over all other queues.

This command is only for egress (output) rate shaping.

Chapter 12 Access Control Lists

This chapter contains the following major sections:

- SFTOS Support for Access Control Lists
- Using ACL Commands

SFTOS Support for Access Control Lists

SFTOS 2.4.1 supports only Layer 2 ACLs (MAC ACLs) — up to 1024 with 64 rules per ACL — so any statement in this book dealing with IP-based ACLs is not relevant.

Access control lists (ACLs) are used to control the traffic entering a network. They are normally used in a firewall router or in a router connecting two internal networks. You may selectively admit or reject inbound traffic, thereby controlling access to your network, or to specific resources on your network.

SFTOS supports two types of filtering: extended MAC ACLs and IP ACLs (MAC ACLs only in SFTOS 2.4.1). For both types, the general process for using them is the same:

1. Create the access list.
2. Apply the access list either globally to all ports or to an individual interface.

Implementation Notes

- If the CPU MA table (this MAC address table is separate from the software MAC address table) is filled so that the ACL logic cannot create another MA table entry, all frames from that source address will be dropped.
- If the ACL rules are changed, or ACLs are unapplied to the port, all CPU MA table entries associated with that port will be flushed from the table. If ACLs are unapplied (and port security is not enabled on the port), the hardware is configured to no longer trap frames from that port to the CPU.
- ACLs take precedence over port-based security configuration.
    - If port security is enabled on a port, and then an ACL is applied to the port, the ACL is given precedence and port security is ignored. For example, if port security is applied, and then an ACL with a permit rule for a particular source address is applied, frames with that source address will be permitted.
    - Logically, then, if a port that does not have port security enabled has an ACL applied, and then port security is enabled, the ACL takes precedence and port security is ignored, as above.

- In either case, if all ACLs are removed from the port, port security will become active if it is still configured as such.
- When port security is disabled on a port after having been enabled, all MAC table entries associated with that port are flushed.
- For more on port security, see the Security chapter of the *SFTOS Command Reference.*

Using ACL Commands

Note: For syntax details on ACL commands, see the ACL chapter in the *SFTOS Command Reference*.

MAC address-based Access Control Lists (MAC ACLs) ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The system supports only Ethernet II frame types.

  To create a MAC ACL identified by *name*:

  — **mac access-list extended** *name*

  ```
  Force10 (Config)#mac access-list extended ml-1
  ```

  Define rules for the selected MAC ACL, consisting of classification fields defined for the Layer 2 header of an Ethernet frame:

  — {**deny**|**permit**}{*srcmac srcmacmask*| **any**} {*dstmac* | **any**} [**assign-queue** *queue-id_0-6*] [**cos** *0-7*] [*ethertypekey*] [*0x0600-0xFFFF*] [**redirect** *slot/port*] [**vlan** {**eq** *0-4095*]

```
Force10 (Config)#mac access-list extended ml-1
Force10 (Config-mac-access-list)#permit 01:80:c2:00:00:00 any assign-queue 4
Force10 (Config-mac-access-list)#permit any 01:80:c2:00:00:FF assign-queue 3 redirect 0/10
```

Figure 138 Creating a Rule for a MAC Access List

The *srcmacmask* variable uses a wildcard called an *inverted mask*. In an inverted mask, a zero in a bit in the mask means “exact match required”. A one in a mask bit means “match anything here”. For example:

- To deny all traffic from MAC address 00:00:00:00:03:02, the mask is 00:00:00:00:00:00.
- To deny all traffic from 00:00:00:00:03:xx, the mask is 00:00:00:00:00:ff.

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.

Note: You can add new deny/permit list items to an existing list, but you cannot remove previously configured deny/permit list items. You must delete the list before recreating it as you want.

- Change the name of a MAC ACL. This command fails if a MAC ACL identified by the name *newname* already exists:
  - **mac access-list extended rename** *name newname*
- Attach a MAC ACL identified by name to the selected interface in the ingress direction. The *name* parameter must be the name of an existing MAC ACL. The optional *1-4294967295* parameter helps to set the order in which ACLs are applied to the interface if more than one ACL is assigned.
  - **mac access-group** *name* [*1-4294967295*] **in**

```
Force10 (Config)#interface 0/2
Force10 (Interface 0/2)#mac access-group ml-1 in
```

- Remove the assignment of a MAC ACL identified by name from the selected interface:
  - **no mac access-group** *name*
- Display a MAC ACL and all of the rules that are defined for the ACL. The *name* parameter identifies the MAC ACL to display:
  - **show mac access-list** *name*

```
Force10 #show mac access-list ml-1
Rule Number: 1
Action..................................... permit
Source MAC Address......................... 01:80:C2:00:00:00
Assign Queue............................... 4

Rule Number: 2
Action..................................... permit
Destination MAC Address.................... 01:80:C2:00:00:FF
Assign Queue............................... 3
Redirect Interface......................... 0/10

Force10 #
```

Figure 139 Sample Output from show mac access-list Command

- Display a summary of all defined MAC access lists in the system:
  - **show mac access-lists**

```
Force10 #show mac access-lists
Current number of all ACLs: 3  Maximum number of all ACLs: 100

     MAC ACL Name               Rules       Interface(s)        Direction
------------------------------ ----- ------------------------ ---------
ml-1                            2     0/2                     inbound
Force10 (Config-mac-access-list)#permit any 01:80:c2:00:00:FF assign-queue 3 redirect 0/10
```

Figure 140 Sample Output from show mac access-lists Command

ACL Configuration Example

```
Force10 S2410 (Config)#mac access-list extended mac1
Force10 S2410 (Config-mac-access-list)#deny 00:00:00:00:03:02 00:00:00:00:00:00
Force10 S2410 (Config-mac-access-list)#exit
Force10 S2410 (Config)#exit
Force10 S2410 #show mac access-lists mac1

MAC ACL Name: mac1

Rule Number: 1
Action..................................... deny Source MAC
Address.......................... 00:00:00:00:03:02 Source MAC
Mask............................. 00:00:00:00:00:00
```

Figure 141 ACL Configuration Example

Note: While the **extended** keyword in **mac access-list extended** suggests that the command is creating an extended ACL, SFTOS 2.4.1.0 supports only a standard ACL (using just the source MAC address).

Chapter 13 VLANs

This chapter describes the use of SFTOS 2.4.1 to create IEEE 802.1Q VLANs, in the following major sections:

- Introduction to VLAN Configuration
- VLAN Mode Commands on page 177
- Configuration Task List for VLANs on page 178
- Adding a LAG to a VLAN on page 182
- GARP and GVRP on page 185
- Using the Web User Interface for VLAN Configuration on page 189
- VLAN-Stack (DVLAN) Configuration on page 190
- Displaying VLAN Configuration Information on page 194

Introduction to VLAN Configuration

Virtual LAN (VLAN) support in SFTOS conforms to the IEEE 802.1Q specification, allowing a network to be logically segmented without regard to the physical location of devices on the network—one physical network becomes multiple logical networks. These logical networks may, or may not, correspond to subnets.

While maintaining Layer 2 forwarding speed, network segmentation provides:

- Better administration
- Better security
- Better management of multicast traffic

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

Important Points to Remember

- The default VLAN is VLAN 1.
- A VLAN can include port channels and ports on multiple switches in the stack.
- A port can be a member of only one untagged VLAN.
- SFTOS 2.3 does not permit both tagged and untagged VLANs on the same port.
- With the SFTOS VLAN implementation, ports may belong to multiple VLANs, and VLAN membership may be based on port or protocol.
- 1024 VLANs can be in operation at one time, any of which can have a VLAN ID up to 3965. The top 129 VLANs are reserved.

Implementing VLANs

Table 5 VLAN ID Options

VLAN ID	Limitations
0	Reserved for .1p
1	Default VLAN
2 - 3965	Configurable by user
3966 - 4094	Reserved for IP interfaces
4095	Reserved for Blackhole VLAN
4096	Total VLAN IDs

When an individual port is added to a LAG, any VLAN membership is suspended, however the membership is automatically restored when the port is removed from the LAG.

Forwarding Rules

Forwarding rules are based on the following attributes:

- VLAN membership
- Spanning tree state (forwarding)
- Frame type (unicast or multicast)
- Filters

Egress Rules

- Spanning tree state (forwarding)
- VLAN membership
- Untagged frames only forwarded if embedded addresses are canonical

Exempt Frames

(control frames that will be processed without regard to VLAN membership)

- Spanning tree BPDUs
- GVRP BPDUs
- Frames used for control purposes, such as LAG PDUs and flow control

VLAN Mode Commands

The starting point for VLAN command syntax statements in the *SFTOS Command Reference* is the Virtual LAN (VLAN) Commands section of Chapter 7, System Configuration Commands.

Executing the **interface vlan** *2-4094* command in Global Config mode either creates or selects a previously created VLAN (or use **[no] interface vlan** *2-4094* to delete a VLAN) and then enters the Interface VLAN mode, where you have access to commands that configure the identified VLAN. The basic commands are:

- To add an interface to the VLAN, use either the **tagged** *interface* or **untagged** *interface* command

Note: The **tagged** command takes the place of the **participation**, **priority**, and **pvid** commands; do not use them on the S50.
Note: Use **no tagged** to reverse the configuration of the **tagged** command, and use **no untagged** to reverse the configuration of the **untagged** command.

- To change a dynamically created VLAN to a static VLAN (permanently configure):
  - **makestatic** *2-4094* (in Interface VLAN mode)
- To [reset] assign a name to a VLAN (VLAN 1 is always named Default, while the default for other VLANs is a blank string.):
  - **[no] name** *name* (up to 32 alphanumeric characters)
- To configure the interface link layer encapsulation type:
  - **encapsulation**
- To configure IGMP Snooping parameters for the VLAN:
  - **igmp**
- To configure the protocols associated with particular group IDs:
  - **protocol group** *groupid*

The following VLAN commands in the Global Config and Interface Config modes are deprecated:

- **vlan acceptframe**
- **vlan ingressfilter**
- **vlan pvid**
- **vlan tagging**
- **vlan untagging**
- **vlan participation all**
- **vlan port acceptframe**
- **vlan port ingressfilter all**
- **vlan port pvid all**
- **vlan port tagging all**
- **vlan port untagging all**

Configuration Task List for VLANs

- Creating the VLAN and Adding Ports
- Clearing/Resetting a VLAN on page 182
- Adding a LAG to a VLAN on page 182
- Enabling Dynamic VLANs with GVRP on page 187

For more VLAN configuration examples, in the Getting Started chapter, see introduction to VLAN configuration, Creating VLANS on page 43.

Creating the VLAN and Adding Ports

The following instructions are the basic configuration tasks for creating the VLAN and adding ports to it:

Step	Command Syntax	Command Mode	Usage
1	**interface vlan** *2-4094*	Global Config	Specify a new or existing VLAN by VLAN number.
2	[**no**] **tagged** *slot/port*	Interface VLAN	To add tagged ports to the VLAN, specify a single port in *slot/port* format to add to the selected VLAN, or specify a sequential port range as *slot/port-slot/port*. Specify a non-sequential port range as *slot/port,slot/port,...* Specify a LAG ID as an integer (List LAG IDs with **show interface port-channel brief**.)
3	[**no**] **untagged** *slot/port*	Interface VLAN	To add untagged ports to the VLAN, specify either a port, port range, port channel, or port channel range, as described above.
4	**name** *VLAN-name*	Interface VLAN	(OPTIONAL) Name the VLAN.

Step	Command Syntax	Command Mode	Usage
5	**show vlan id** *vlanid*	Privileged Exec	Verify the configuration.

Note: Enable each port added to the VLAN.

Example of creating a VLAN and assigning interfaces

The diagram in this example shows four S-Series switches, R1, R2, R3, and R4, each configured with VLAN 2 to handle traffic destined for R1.

This example creates VLAN 2 to connect four switches, with each switch having an interface that connects through VLAN 2 to switch R1.

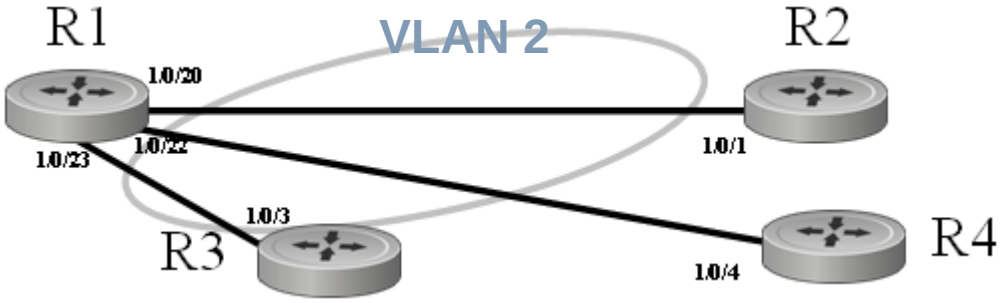


Figure 142 VLAN Topology

1. Create VLAN 2 on switch R1 and assign ports 20, 22, and 23:

```
R1 #config
R1 (Config)#interface vlan 2
R1 (Conf-if-vl-2)#untagged 0/20
R1 (Conf-if-vl-2)#untagged 0/22
R1 (Conf-if-vl-2)#untagged 0/23
```

2. Create VLAN 2 on switch R2 and assign port 1:

```
R5 #config
R5 (Config)#interface vlan 2
R5 (Conf-if-vl-2)#untagged 0/1
```

3. Create VLAN 2 on switch R3 and assign port 3:

```
R3 #config
R3 (Config)#interface vlan 2
R3 (Conf-if-vl-2)#tagged 0/3
```

4. Create VLAN 2 on switch R4 and assign port 4:

```
R4 #config
R4 (Config)#interface vlan 2
R4 (Conf-if-vl-2)#untagged 0/4
```

5. Optionally, after creating the VLAN, you can name it using the **name** command. For example, if R1 in this example is providing access to the Internet, you might name the VLAN “Internet_through_R1” on each participating switch.
6. Verify the configuration with the **show vlan** commands, or any of the other commands listed in Displaying VLAN Configuration Information on page 194.

Notes:

- Note that VLAN2 on R1 has some untagged ports and some tagged ports. The tagging type (either untagged or tagged) must match those of their directly connected ports on the other switches unless **vlan acceptframe all** is configured on an interface.
- In SFTOS 2.3, an interface may include one or more tagged VLANs, but only one untagged VLAN. SFTOS 2.3 does not permit mixed tagged and untagged VLANs on an interface.

Assign an interface to multiple VLANs

The diagram in Figure 143 shows five S-Series switches, R1, R2, R3, R4, and R5, in a trunking relationship, where port 20 on R1 is connected through R5 on separate VLANs to the other three switches.

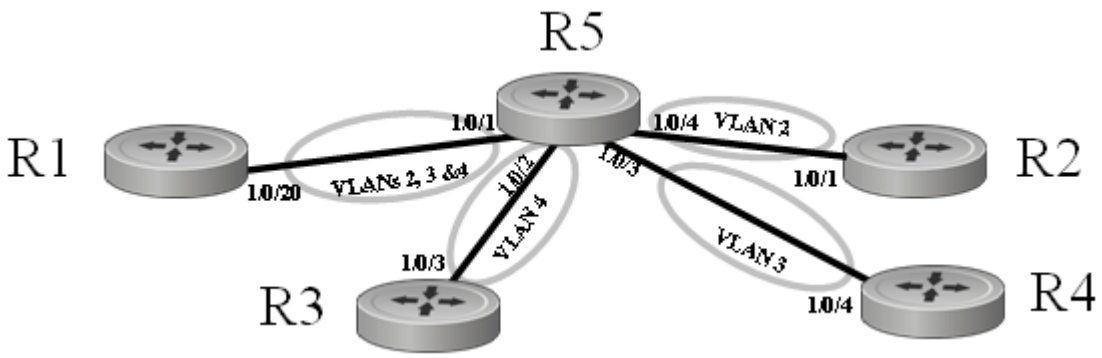


Figure 143 Switch Connected to Other Switches through Multiple VLANs

1. To create the topology shown in Figure 143, first create VLANs 2, 3, and 4 on switch R1, and assign port 20 to each VLAN.

```
R1 #config
R1 (Config)#interface vlan 2
R1 (Conf-if-vl-2)#tagged 0/20
R1 (Conf-if-vl-2)#exit
R1 (Config)#interface vlan 3
R1 (Conf-if-vl-3)#tagged 0/20
R1 (Conf-if-vl-3)#exit
R1 (Config)#interface vlan 4
R1 (Conf-if-vl-4)#tagged 0/20
```

2. Create VLAN 2 on switch R2 and assign port 1.

```
R2 #config
R2 (Config)#interface vlan 2
R2 (Conf-if-vl-2)#tagged 0/1
```

3. Create VLAN 4 on switch R3 and assign port 3.

```
R3 #config
R3 (Config)#interface vlan 4
R3 (Conf-if-vl-4)#tagged 0/3
```

4. Create VLAN 3 on switch R4 and assign port 4:

```
R4 #config
R4 (Config)#interface vlan 3
R4 (Conf-if-vl-3)#tagged 0/4
```

5. Create VLANs 2, 3, and 4 on switch R5 to connect to each member switch in the topology:

```
R5 #config
R5 (Config)#interface vlan 2
R5 (Conf-if-vl-2)#tagged 0/1
R5 (Conf-if-vl-2)#tagged 0/4
R5 (Conf-if-vl-2)#exit
R5 (Config)#interface vlan 3
R5 (Conf-if-vl-3)#tagged 0/1
R5 (Conf-if-vl-3)#tagged 0/3
R5 (Conf-if-vl-3)#exit
R5 (Config)#interface vlan 4
R5 (Conf-if-vl-4)#tagged 0/1
R5 (Conf-if-vl-4)#tagged 0/2
```

6. Verify the configuration with the **show vlan** commands, or any of the other commands listed in Displaying VLAN Configuration Information on page 194.

Notes:

- R1 has interface 0/20 in multiple VLANs.
- R5 has interface 0/1 in multiple VLANs.
- Note that all VLANs in this example are tagged, because an interface can be a member of multiple tagged VLANs, but not multiple untagged VLANs.

Clearing/Resetting a VLAN

To clear the VLAN configuration parameters to the factory defaults, issue the **clear vlan** command from Privileged Exec mode:

```
Force10 #clear vlan
```

Figure 144 Example of Removing VLANs

The **clear vlan** command removes all VLAN information from the running configuration.

Note: Recovery of VLAN information from the startup configuration would then require reloading the switch.

Adding a LAG to a VLAN

To add a Link Aggregation Group (LAG) (also called a port channel) to a VLAN, you create the LAG, as detailed in the LAG chapter (Configuring a LAG on page 158), and then add the LAG to the VLAN, using the **tagged** or **untagged** command, just as you do when you add a port to a VLAN (see Creating the VLAN and Adding Ports on page 178). In the case of a LAG, *slot/port* is the logical ID of the LAG. :

The following instructions are the basic configuration tasks for creating the VLAN:

Step	Command Syntax	Command Mode	Usage
1	**port-channel** *name*	Global Config	Create the LAG. For details, see Link Aggregation on page 155.
2	**show interface port-channel brief**	Privileged Exec	Learn the LAG ID in *slot/port* format, such as 1/1.
3	**interface** *slot/port*	Global Config	Access the LAG configuration mode. In this case, *slot/port* represents the logical ID of the LAG.
4	**port-channel enable**	Interface Config	Enable the LAG.
5	**interface** *slot/port*	Global Config	Access the interface that you want to add to the LAG.
6	**addport** *slot/port*	Interface Config	Add the interface to the LAG identified by *slot/port.*
7			Repeat steps 5 and 6 for each port that you want to add to the LAG.
8	**interface vlan** *2-4094*	Global Config	Specify a new or existing VLAN by VLAN number.

Step	Command Syntax	Command Mode	Usage
9	**tagged** *slot/port* or **untagged** *slot/port*	Interface VLAN Config	Add the LAG in logical slot/port format, such as 1/1.
10	**show vlan id** *vlanid*	Privileged Exec	Verify the configuration.

Example of adding a LAG to a VLAN

Figure 145 Adding a LAG to a VLAN

Figure 148 shows the use of the **show port-channel all** command to learn the logical IDs of configured LAGs, following by the command sequence shown above.

1. To create the topology shown in Figure 145, first create the LAG by name on switch R1, and discover its logical port number.

```
R1 (Config)#port-channel admin1
R1 (Config)#exit
R1 #show port-channel all

            Port-                   Link
Log.       Channel            Adm. Trap  STP           Mbr      Port    Port
Intf        Name        Link  Mode Mode  Mode   Type   Ports    Speed   Active
------ --------------- ------ ---- ---- ------ ------- ------ --------- ------
1/1  admin1          Down   En.  En.  Dis.   Dynamic
```

Figure 146 Creating a LAG and learning its ID

Note: In SFTOS 2.3 and before, after the LAG is created, it is referred to by its logical interface number, not its name. When configuring, use the interface number, in this case, 1/1.

2. Enable the LAG and add physical interfaces to it on switch R1.

```
R1 (Config)#interface 1/1
R1 (Interface 1/1)#no shutdown
R1 (Interface 1/1)#exit

R1 (Config)#interface  0/5
R1 (Interface 0/5)#addport 1/1
R1 (Interface 0/5)#exit

R1 (Config)#interface  0/6
R1 (Interface 0/6)#addport 1/1
R1 (Interface 0/6)#exit

R1 (Config)#interface  0/7
R1 (Interface 0/7)#addport 1/1
R1 (Interface 0/7)#exit
```

Figure 147 Adding ports to a LAG

Note: In SFTOS 2.3, the [**no**] **shutdown** command is equivalent to the [**no**] **port-channel enable** command when enabling or disabling LAGs. The representation of the command in the configuration (the output of **show running-config**) is inconsistent. If the **port-channel enable** command is used, **no shutdown** appears in the running-config. Conversely, if the **shutdown** command is used to disable the LAG, **no port-channel enable** appears in the running-config.
Note: A physical interface added to a LAG appears twice in the running-config — in the interface section and in the port-channel section.

3. Create VLAN 300 and add the LAG to it on switch R1.

```
R1 (Config)#interface vlan  300
R5 (Conf-if-vl-300)#tagged 1/1
```

Figure 148 Adding a LAG to a VLAN

4. Repeat the sequence above on switch R2.

5. Verify the operation on both switches.

```
R2 #show vlan id 300

Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface

   Vlan Id  Status     Q    Ports
   -------  ---------  -  --------
   300      Active     T  E  1/1
R2 #show port-channel 1/1

            Port-                  Link
Log.       Channel            Adm. Trap  STP           Mbr      Port    Port
Intf        Name        Link  Mode Mode  Mode   Type   Ports    Speed   Active
------ --------------- ------ ---- ---- ------ ------- ------ --------- ------
1/1  admin1          Up     En.  En.  Dis.   Dynamic 0/5 Auto      True
                                                    0/6 Auto      True
                                                    0/7 Auto      True
```

Figure 149 Verifying a LAG in a VLAN with show vlan id and show port-channel id

GARP and GVRP

This sections contains these major subsections:

- GARP VLAN Registration Protocol (GVRP)
- GARP Timers on page 186
- GARP Commands on page 186
- Using GVRP on page 187
- Enabling Dynamic VLANs with GVRP on page 187
- Displaying GARP, GVRP, GMRP Properties on page 189

Generic Attribute Registration Protocol (GARP) provides a generic attribute dissemination protocol used to support other protocols such as GVRP (GARP VLAN Registration Protocol. GARP is used to register and deregister attribute values with other GARP participants within bridged LANs. When a GARP participant declares or withdraws a given attribute, the attribute value is recorded with the applicant state machine for the port from which the declaration or withdrawal was made.

A GARP participant exists per port per GARP application (e.g. GVRP). For details on GARP, GVRP, and GMRP (GARP Multicast Registration Protocol) command syntax, see the GARP, GVRP, and GMRP Commands chapter in the *SFTOS Command Reference*.

GARP VLAN Registration Protocol (GVRP)

- GVRP propagates VLAN membership throughout a network.
- GVRP allows end stations and switches to issue and revoke declarations relating to VLAN membership.

- VLAN registration is made in the context of the port that receives the GARP PDU and is propagated to the other active ports.
- GVRP is disabled by default; you must enable GVRP for the switch and then for individual ports.
- Dynamic VLANs are aged out after the LeaveAll Timer expires three times without receipt of a join message.

GARP Timers

The following are GARP timers:

- Join Timer:
  - Controls the interval of a GMRP PDU transmission
  - Default value: 20 centiseconds
- Leave Timer:
  - Controls the time period after the de-registration process is started for a registered attribute. It should be at least twice the Join Timer.
  - Default value: 60 centiseconds
- LeaveAll Timer:
  - Controls the frequency with which a LeaveAll event GARP PDU is transmitted. It should be considerably longer than the Leave Timer.
  - Default value: 1000 centiseconds

GARP Commands

In Global Config mode, you can enable GVRP, or GMRP, or both for the switch:

gvrp adminmode enable

gmrp adminmode enable: `enables GARP Multicast Registration Protocol (GMRP) on the system`

gmrp interfacemode enable all: `enables GARP Multicast Registration Protocol on all interfaces`

In Interface Config mode, enable GVRP for a port:

gvrp interfacemode enable

In Interface Config, Global Config, or Interface Range mode, set the timer values in centiseconds. For interface-level changes, go to the individual interfaces to apply changes.

set garp timer join *10-100*: `The default is 20.`

set garp timer leave *20-600*: `The default is 60.`

set garp timer leaveall *200-6000*: `The default is 1000.`

Using GVRP

GVRP is used to exchange a VLAN number—in this example, VLAN 3—dynamically from the switch on which it is configured to the switch on which GVRP is enabled.

- GVRP must be enabled globally and on selected interfaces.
- One end must have a VLAN configured on an interface in order to establish a dynamic VLAN connection on the other end. In the following example, R2 has VLAN 3 configured.
- Two switches link through a port, 0/2 in this case.

Enabling Dynamic VLANs with GVRP

Use the following command sequence on each switch participating in the dynamic VLAN:

Step	Command Syntax	Command Mode	Usage
1	**gvrp adminmode enable**	Global Config	Enable GVRP on each switch and on each port that is to be part of the GVRP VLAN.
2	**interface vlan** *vlan_id*	Global Config	Specify a new or existing VLAN by VLAN number, from 2–4094.
3	**tagged** *slot/port*	Interface VLAN Config	Add one or more ports to the VLAN.
4	**no shutdown**	Interface VLAN Config	Enable each port added to the VLAN.
5	**show garp**	Privileged Exec	Verify the GARP admin mode.
6	**show gvrp configuration all**	Privileged Exec	Verify the GARP interface.
7	**show vlan brief**	Privileged Exec	Verify the VLAN.

Example of Creating a Dynamic VLAN through GVRP

In this case, after enabling GVRP globally and on specific ports, and then creating a VLAN on R2 with one of those ports:

- Switch 1 (“R1”) learns VLAN 3 from R2.
- Port 0/2 on R1 will become VLAN 3, and VLAN 3 traffic can go through.

Figure 150 Diagram of VLAN between Switches

```
Force10 (Config)#hostname R1
R1 (Config)#gvrp adminmode enable
R1 (Config)#interface 0/2
R1 (Interface 0/2)#no shutdown
R1 (Interface 0/2)#gvrp interfacemode enable
R1 (Interface 0/2)#exit
```

Figure 151 Enabling GVRP on Switch and Interface on Switch 1

```
Force10 (Config)#hostname R2
R2 (Config)#gvrp adminmode enable
R2 (Config)#interface 0/1
R2 (Interface 0/1)#no shutdown
R2 (Interface 0/1)#gvrp interfacemode enable
R2 (Interface)#exit
R2 (Config)#interface vlan 3
R2 (conf-if-vl-vlan-3)#tagged 0/1
R2 (conf-if-vl-vlan-3)#exit
```

Figure 152 Setting up the VLAN and GVRP on Switch 2

Using show vlan id 3 to verify the dynamically created VLAN

```
(R1) #show vlan id 3
Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface
Vlan Id  Status     Q    Ports
-------  ---------  -  --------
G  3        Active     T  E  0/2
```

Figure 153 Using the show vlan id Command

Notes:

- The ‘G’ indicates that this VLAN was dynamically created via GVRP on R1.
- If you execute **show vlan id 3** on R2, you will not see the G in the output, because the VLAN was actually configured on R2, not dynamically negotiated.
- To make the VLAN permanent on R1, use the **makestatic** command under **interface vlan 3**.

Displaying GARP, GVRP, GMRP Properties

These Privileged Exec and User Exec mode commands display GARP, GVRP, and GMRP information:

- **show garp** (Figure 154)
  - — Displays admin mode for GVRP and GMRP
- **show gmrp configuration** {*slot/port* | **all**}
- **show gvrp configuration** {*slot/port* | **all**} (Figure 154)
  - — Port admin mode for GVRP and GMRP
  - — Timer values

See also the **show vlan id** command shown above (Figure 153).

show garp and show gvrp configuration all commands

```
(R2) #show garp

GMRP Admin Mode.............................. Disable
GVRP Admin Mode.............................. Enable

(R2) #show gvrp configuration all

              Join     Leave    LeaveAll      Port
 Slot/Port    Timer    Timer     Timer      GVRP Mode
-----------  -------  -------  ----------  -----------
0/1          20       60       1000        Enabled
0/2          20       60       1000        Enabled
0/3          20       60       1000        Enabled
0/4          20       60       1000        Enabled
0/5          20       60       1000        Enabled
0/6          20       60       1000        Enabled
!---------output truncated--------!
```

Figure 154 Using the show garp and show gvrp configuration all Commands

Using the Web User Interface for VLAN Configuration

Use the following sequence of Web UI panels to configure VLANs:

- To create VLANs and specify port participation: **Switching** --> **VLAN**--> **Configuration**
- To specify the handling of untagged frames on receipt, and whether frames will be transmitted tagged or untagged: **Switching** --> **VLAN** --> **Port Configuration**

For more on the Web UI, see Using the Web User Interface on page 65.

VLAN-Stack (DVLAN) Configuration

VLAN-Stack commands, also called Double VLAN (DVLAN) commands, support tunneling. In more detail, with the VLAN-Stack feature, you can “stack” VLANs into one tunnel and switch them through the network. This feature is a way to pass VLAN traffic from one customer domain to another through a metro core in a simple, cost-effective manner.

The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when the traffic enters their own 802.1Q domains. The 4-byte tag precedes the VLAN tag and carries:

- Protocol ID (Ethertype field)
- Customer ID (VLAN ID field)

DVLAN Tagging Considerations

- **Frame size**: If the port is enabled for DVLAN tagging and maximum length frames are expected, jumbo frame support should also be enabled (Use the **mtu** command in Interface Config mode).
- **Port types**: DVLAN tagging may be enabled for a LAG, but not for LAG members, VLAN routing ports, or probe ports.
- **Control frames**: Control frames (e.g. GARP, LACPDUs) will be double-tagged.
- **Ethertypes for DVLAN tags** (“DVLAN tag” is sometimes shortened to *DVT*):
    - 802.1Q tag (0x8100)
    - vMAN tag (0x88A8)
    - Custom tag (any valid value)
- The tunnel port (core port; uplink port) cannot be a routed port.
- After the outer tag is added, QoS on the inner tag is not supported.

DVLAN Configuration Sequence

If you have created the required VLANs and you want to associate access and trunk ports with a particular DVLAN bridging instance, you must enable the system for DVLAN tagging, define the access and trunk ports, and then enable tagging on the trunk (core) port.

Step	Command Syntax	Command Mode	Purpose
1	**dvlan-tunnel ethertype** {**802.1Q** | **vman** | **custom** *0-65535*}	Global Config	Enables the system for DVLAN tagging with the selected etherType (**vman** by default).
2	**interface** *slot/port*	Global Config	By default, all ports become trunk (core) ports. Select ports to configure as DVLAN access ports.

Step	Command Syntax	Command Mode	Purpose
3	**mode dvlan-tunnel** (same as **mode dot1q-tunnel**)	Interface Config	Enable DVLAN tagging for the access ports.
4	**show dvlan-tunnel** (identical in functionality to **show dot1q-tunnel**)	Privileged Exec	Display DVLAN-enabled VLAN tagging.
5	**show dvlan-tunnel interface {***slot/port* **| all}** (same as **show dot1q-tunnel interface** {*slot/port* **| all**})	Privileged Exec	Display detailed information for a specific interface.

STP BPDU tunneling: The l2pdu-forwarding mode, used for BPDU tunneling, is enabled by default. Use **no dvlan-tunnel l2pdu-forwarding enable** to disable forwarding. The default forwarding MAC address is 01:01:E8:00:00:00. Use **dvlan-tunnel l2pdu-forwarding mac-address** *mac-addr* to change the MAC address. Inspect settings with **show dvlan-tunnel l2pdu-forwarding**, as shown in Figure 155.

```
Force10 S50 #show dvlan-tunnel l2pdu-forwarding

L2Pdu-Forwarding Mode: enabled.
L2Pdu-Forwarding Mac: 01:01:E8:00:00:00
```

Figure 155 Example of Use of show dvlan-tunnel l2pdu-forwarding Command

DVLAN configuration example

The example in this section of VLAN stacking shows how to configure VLANs so that VLAN traffic from switches R4 and R5 is encapsulated in frames tagged with VLAN 3 going through switch R7.

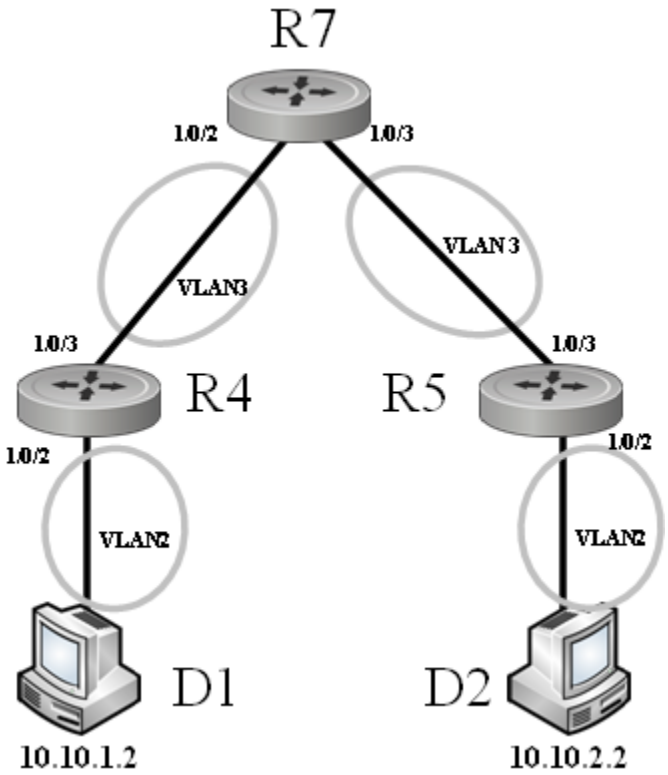


Figure 156 DVLAN Example Topology

Configure switch R4:

```
R4 (Config)#dvlan-tunnel ethertype vman

!---------Access port:-----------!
R4 (Config)#interface 0/2
R4 (Interface 0/2)#no shutdown
R4 (Interface 0/2)#mode dvlan-tunnel
R4 (Interface 0/2)#exit

!---------Trunk port:----------!
R4 (Config)#interface 0/3
R4 (Interface 0/3)#no shutdown
R4 (Interface 0/3)#exit

!--------Participating VLANs----------!
R4 (Config)#interface vlan 2
R4 (Conf-if-vl-2)#untagged 0/2
R4 (Conf-if-vl-2)#tagged 0/3
R4 (Conf-if-vl-2)#exit

R4 (Config)#interface vlan 3
R4 (Conf-if-vl-3)#tagged 0/3
R4 (Conf-if-vl-3)#exit
```

Figure 157 VLAN-Stack Configuration Sequence on R4

Note: The first command in Figure 157 and in Figure 158 configures a dvlan-tunnel ethertype of vman, but you can assign a custom ethertype, which controls the encapsulation of the tunneled traffic, as long as the ethertype matches on both end switches (R4 and R5 here).
Note: The tunneled VLAN (VLAN 2 here) must be configured on both the source and trunk (uplink) ports, even though it is not configured on the remote end of the uplink (R7 here).
Note: The source port must be untagged in the source VLAN.
Note: If you are sending large frames, make sure you configure the mtu appropriately.

Configure switch R5:

```
R5 (Config)#dvlan-tunnel ethertype vman

!---------Access port:-----------!
R5 (Config)#interface 0/2
R5 (Interface 0/2)#no shutdown
R5 (Interface 0/2)#mode dvlan-tunnel
R5 (Interface 0/2)#exit

!---------Trunk port:----------!
R5 (Config)#interface 0/3
R5 (Interface 0/3)#no shutdown
R5 (Interface 0/3)#exit

!--------Participating VLANs----------!
R5 (Config)#interface vlan 2
R5 (Conf-if-vl-2)#untagged 0/2
R5 (Conf-if-vl-2)#tagged 0/3
R5 (Conf-if-vl-2)#exit

R5 (Config)#interface vlan 3
R5 (Conf-if-vl-3)#tagged 0/3
R5 (Conf-if-vl-3)#exit
```

Figure 158 VLAN-Stack Configuration Sequence on R5

Configure switch R7:

```
!---------Trunk ports:----------!
R7 (Config)#interface 0/2
R7 (Interface 0/2)#no shutdown
R7 (Interface 0/2)#exit

R7 (Config)#interface 0/3
R7 (Interface 0/3)#no shutdown
R7 (Interface 0/3)#exit

!--------Participating VLAN----------!
R7 (Config)#interface vlan 3
R7 (Conf-if-vl-3)#tagged 0/2
R7 (Conf-if-vl-3)#tagged 0/3
R7 (Conf-if-vl-3)#exit
```

Figure 159 VLAN-Stack Configuration Sequence on R7

Displaying VLAN Configuration Information

The **show port**, **show running-config** (see Figure 160, below), and **show vlan** commands provide most of the information about the VLAN configuration. The **show vlan** command has the following options:

- (no option entered) Display summary information for all configured VLANs. See Figure 161, below.
- **association** Display associations to VLANs.
- **brief** Display switch VLANs.
- **id** Display VLAN configuration and configure VLANs. See Figure 162, below.
- **name** Display VLAN configuration for a VLAN with optional name.
- **port** Display 802.1Q port parameters. See Figure 163, below.

Figure 160 shows the use of the commands **show running-config** and **show vlan brief** to display VLAN settings. Note in the **show vlan brief** output that VLAN 1 exists even though it was not configured (VLAN 1 is the default VLAN, and all interfaces are members of VLAN 1 by default.):

```
Force10 #show running-config
!Current Configuration:
![excerpt showing just the vlan elements in the report]!

interface vlan  1
exit
interface vlan 2
exit
interface vlan 3
exit
Force10 #show vlan brief

VLAN        Name        STG         MAC AgingIP Address
---------  ----------  --------    ----------------    ---------------
1            abc         0 1800               unassigned
2            egf         0         1800               unassigned
3            sss         0         1800               unassigned
```

Figure 160 Using the show running-config and show vlan brief Commands

Use the **show vlan** command, without parameters, to view the system VLAN configuration:

```
Force10#show vlan

Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface

Vlan Id  Status     Q  Ports
   -------  ---------  -  --------
*  1        Inactive   U  E  0/1 ,0/2 ,0/3 ,0/4 ,0/5 ,0/6 ,0/7
                              0/8 ,0/9 ,0/10,0/12,0/13,0/14,0/15
                              0/16,0/17,0/18,0/19,0/20,0/21,0/22
                              0/23,

   100      Active     U  E  0/24

   400      Inactive   T  E  1/1
```

Figure 161 Example Output from show vlan Command

Using the **show vlan id** *vlan-id* command, used here to display one VLAN comprised of a LAG and another VLAN comprised of a port:

```
Force10# show vlan id 11
Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface
Vlan Id Status Q Ports
--------- ---------- - ------
11     Inactive T E 1/2

Force10# show vlan id 100

Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface

   Vlan Id  Status     Q    Ports
   -------  ---------  -  --------
   100      Active     U  E  0/4
```

Figure 162 Example Output from show vlan id Command

Use the **show vlan port** command, with an interface or **all** parameter, to learn the association between individual ports and VLANs:

```
Force10-S50 #show vlan port 0/1
          Port    Acceptable   Ingress             Default
Interface VLAN ID Frame Types  Filtering    GVRP   Priority
--------- ------- ------------ ----------- ------- --------
0/1     1       Admit All    Enable      Disable     0

Protected Port .............................. False

Force10-S50 #show vlan port all
          Port    Acceptable   Ingress             Default
Interface VLAN ID Frame Types  Filtering    GVRP   Priority
--------- ------- ------------ ----------- ------- --------
0/1     1       Admit All    Enable      Disable     0
0/2     1       Admit All    Enable      Disable     0
0/3     1       Admit All    Enable      Disable     0
0/4     1       Admit All    Enable      Disable     0
0/5     1       Admit All    Enable      Disable     0
0/6     1       Admit All    Enable      Disable     0
0/7     1       Admit All    Enable      Disable     0
0/8     1       Admit All    Enable      Disable     0
0/9     1       Admit All    Enable      Disable     0
0/10    1       Admit All    Enable      Disable     0
!----output truncated--------!
```

Figure 163 Example Output from show vlan Command

Chapter 14 IGMP Snooping

Note: Although the IGMP Snooping commands appear in the CLI, limitations in current S2410 hardware makes them nonfunctional.

Typically, a switch employing IGMP Snooping forwards multicast packets out all ports in a VLAN until it receives an IGMP membership report.

Enabling IGMP Snooping

The typical configuration involves the following steps. For more IGMP Snooping commands and for details on these, see the IGMP Snooping chapter in the *SFTOS Command Reference*.

1. From Global Config mode, enable IGMP Snooping on the switch: **igmp enable**
2. Enable IGMP Snooping on all or specific interfaces:

   igmp enable interfacemode enable all
   - In Global Config mode for all interfaces

   igmp enable
   - In Interface VLAN mode or Interface Config mode for selected interfaces

3. Set timers:

   set igmp groupmembership-interval *2-3600*
   - Sets the IGMP group membership interval time globally in Global Config mode
   - Default 260 seconds

   igmp groupmembership-interval *2-3600*
   - Sets the IGMP group membership interval time for selected interface
   - In Interface Config mode or Interface VLAN mode
   - Default 260 seconds

   igmp maxresponse *1-3599*
   - Sets the IGMP maximum response time on a selected port or VLAN
   - Default 10 seconds

set igmp maxresponse *1-3599*

— Sets the IGMP maximum response time in Global Config mode

— Default 10 seconds

set igmp mcrtexpiretime *0-3600*

— In Global Config mode, sets the Multicast router present expiration time for all routers

— Default 0 seconds (no expiration)

igmp mcrtexpiretime *0-3600*

— In Interface Config mode or Interface VLAN mode, sets the Multicast router present expiration time for the selected interface

— Default 0 seconds (no expiration)

Monitoring IGMP Snooping

As shown in the following sample Telnet output, use the **show igmpsnooping** command from the Privileged Exec mode to inspect your settings.

```
Force10 #show igmpsnooping ?

<cr>                  Press Enter to execute the command.
<slot/port>           Enter interface in slot/port format.
mrouter               Display IGMP Snooping Multicast Router information.
<1-3965>              Display IGMP Snooping valid VLAN ID information.

Force10 #show igmpsnooping

Admin Mode.............................Enable
Multicast Control Frame Count.............0
Interfaces Enabled for IGMP Snooping......0/10
Vlans enabled for IGMP snooping...........20
```

Figure 164 Report from show igmpsnooping Command

Use the **show mac-address-table igmpsnooping** command to display the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

```
Force10 #show mac-address-table igmpsnooping

MAC Address              Type       Description     Interfaces
-----------------------  -------    -------------   -----------
00:01:01:00:5E:00:01:16  Dynamic    Network Assist  Fwd: 0/7
00:01:01:00:5E:00:01:18  Dynamic    Network Assist  Fwd: 0/7
00:01:01:00:5E:37:96:D0  Dynamic    Network Assist  Fwd: 0/7
00:01:01:00:5E:7F:FF:FA  Dynamic    Network Assist  Fwd: 0/7
00:01:01:00:5E:7F:FF:FE  Dynamic    Network Assist  Fwd: 0/7
```

Figure 165 Report from show mac-address-table igmpsnooping Command

Chapter 15 Port Mirroring

This chapter contains the following sections:

- Port Mirroring Features and Limitations
- Port Mirroring Commands on page 200
- Port Mirroring Configuration Examples on page 200
- Verifying Port Mirroring on page 202

Port Mirroring Features and Limitations

- Enables you to monitor network traffic with an external network analyzer
- Forwards a copy of each incoming and outgoing packet to a specific port that you designate
- Is used as a diagnostic tool, debugging feature, or means of fending off attacks
- The mirrored port (also called a source port) and the destination port (also called a probe port or mirroring port) can only be members of the same VLAN, and if you first add the probe port to a VLAN before configuring it as the probe port.
- There is a limit of one port mirroring session and one probe port. More than one mirrored port can be designated, but the percentage of the source traffic accepted on the probe port is likely to decline with each added source, depending on the amount of traffic — to roughly 50% each for two source ports, 33% per port for three, and so on.

Inbound or outbound packets will switch to their destination and will be copied to the probe port.

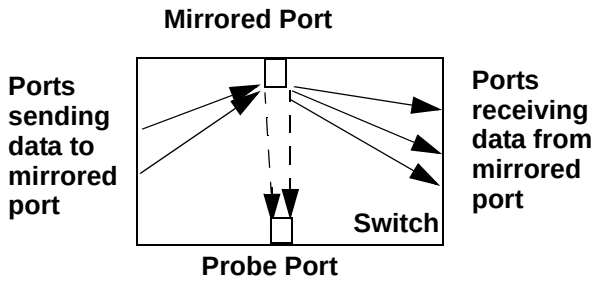


Figure 166 Port Mirroring Diagram

Port Mirroring Commands

The following are the core port mirroring commands, using Figure 166 as a model:

- Enable port mirroring session (default is disable):
  monitor session 1 mode
- Configure mirrored port:
  monitor session 1 source interface 0/2
- Configure destination port/probe port:
  monitor session 1 destination interface 0/3
  (Remove an existing destination port before replacing it with another.)
- Disable monitor session mode before revising probe and mirrored port configuration:
  no monitor session 1 mode
- Unconfigure mirrored port:
  no monitor session 1 source interface 0/2
- Unconfigure probe port before configuring another probe port:
  no monitor session 1 destination 0/3
- Disable port mirroring:
  no monitor

For details on port mirroring command syntax, see the System Configuration chapter of the *SFTOS Command Reference*.

Port Mirroring Configuration Examples

The following are port mirroring configuration examples:

Preparing to Configure Port Mirroring

Typically, before configuring mirroring sessions, you would inspect existing conditions.

Use the **show monitor session 1** command to display the session—ID, admin mode, probe port, and mirrored port:

```
Force10 #show monitor session 1

Session ID  Admin Mode   Probe Port   Mirrored Port
----------  ----------   ----------   -------------
1           Enable       0/5          0/4
```

Figure 167 Using the show monitor session command

Configuring the mirrored port and destination port

When enabled, the probe port monitors all traffic received and transmitted on the monitored port.

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.

1. Specify the source and destination mirror ports:

```
Force10 (Config) #monitor session 1 source interface 0/4
Force10 (Config) #monitor session 1 destination interface 0/5
```

Figure 168 Example of Specifying Source and Destination Mirror Ports

2. Enable port security from the Interface Config mode for the specific interface. Access the mode with the command **interface** *slot/port*. Then use the **port-security** command, as shown in Figure 169. (For more on port-based security, which is also known as port MAC locking, see the Security chapter of the *SFTOS Command Reference*.)

```
Force10 (Interface 0/4) #port-security ?

<cr>             Press Enter to execute the command.
mac-address      Add Static MAC address to the interface.
max-dynamic      Set Dynamic Limit for the interface.
max-static       Set Static Limit for the interface.

Force10 (Config)(Interface 0/4)#port-security max-static ?

<0-20>        Set Static Limit for the interface.

Force10 (Interface 0/4)#port-security max-static 5
Force10 (Interface 0/4)#port-security max-dynamic 10
```

Figure 169 Example of Enabling Port Security

Starting a mirroring session

```
Force10 (Config)#monitor session 1 mode
```

Figure 170 Command Example: Starting a Port Mirroring Session

Stopping the mirroring session and removing probe and mirrored ports

```
Force10 (Config)#no monitor session 1 mode
Force10 (Config)#no monitor session source
Force10 (Config)#no monitor session destination
```

Figure 171 Command Examples: Removing port mirroring configuration

Note: Alternatively, you can use the **no monitor** command to disable port mirroring, which automatically removes the mirror and probe configuration from the source and destination ports. Then, reenabling port mirroring requires designating the source and destination ports again.

Verifying Port Mirroring

Use the following commands from the Privileged Exec mode to inspect port mirroring settings:

- **show monitor session 1**: See Figure 172
- **show port all**: See Figure 172
- **show running-config**: See Figure 174
- **show port**: See Figure 175

Verifying port mirroring session status

```
Force10 #show monitor session 1

Session ID   Admin Mode   Probe Port   Mirrored Port
----------   ----------   ----------   -------------
1            Enable       0/24         0/1
                                       0/11
```

Figure 172 show monitor session 1 Command Output

Using other commands that show port mirroring status

You can use the **show port all** command to show all existing probe ports and mirrored ports, along with their operational status:

```
Force10 S50 #show port all

                    Admin   Physical   Physical   Link   Link    LACP
Interface   Type    Mode    Mode       Status   Status  Trap    Mode
---------- ------ ------- ---------- ---------- ------ ------- -------
0/1      Mirror  Enable  Auto       1000 Full   Up     Enable  Enable
0/2              Disable Auto                  Down   Enable  Enable
0/20              Disable Auto                  Down   Enable  Enable
0/215             Disable Auto                  Down   Enable  Enable
0/22      Probe    Enable  Auto       1000 Full  Up     Enable  Enable
0/23              Disable Auto                  Down   Enable  Enable
0/24              Disable Auto                  Down   Enable  Enable
```

Figure 173 Example of show port all Showing Port Mirroring

```
Force10 S50 #show running-config
!---------<snip>---------------!
monitor session 1 destination interface 0/22
monitor session 1 source interface 0/1
monitor session 1 mode
```

Figure 174 Using show running-config Command Output to Show Port Mirroring

Also, you can use the **show port** *interface* command for information on whether a specific port is the mirror or probe port and what is enabled or disabled on it.

```
Force10 #show port 0/4
              Admin   Physical Physical  Link    Link    LACP
Intf    Type  Mode    Mode     Status    Status  Trap    Mode
----    ----  ------  -------- --------  ------  ----    ----
0/4     Mirror Enable Auto               Down    Enable  Enable

Force10 #show port 0/5
              Admin   Physical Physical  Link    Link    LACP
Intf    Type  Mode    Mode     Status    Status  Trap    Mode
----    ----  ------  -------- --------  ------  ----    ----
0/5     Probe  Enable Auto               Down    Enable  Enable
```

Figure 175 Using the show port command

Chapter 16 Troubleshooting

This chapter describes how to identify and resolve software problems related to SFTOS on an S-Series switch. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack. Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide. This chapter consists of these sections:

- Recovering from Flash File System Corruption on page 205
- Recovering from a Software Upgrade Failure on page 206
- Recovering from a Lost Password on page 206
- Preventing Auto-negotiation Mismatches on page 207
- Managing 10 Gigabit Interfaces on page 207
- Troubleshooting No Output on the Console on page 208

Recovering from Flash File System Corruption

The S50 stores the startup configuration in an NVRAM section of flash memory. The startup configuration can become corrupted and unreadable if the write-to-memory operation does not succeed. You can recognize this condition via the event log messages in Figure 176 on page 205, which may appear after executing the **write memory** command.

```
0xe536bd0 (Cnfgr_Thread ): dosFsLib.c : Malformed boot sector. Offset 0, value 2 55.
0xe536bd0 (Cnfgr_Thread ): dosFsLib.c : Problem finding volume data, trying to u se the next block as boot block.
0xe536bd0 (Cnfgr_Thread ): dosFsLib.c : Malformed boot sector. Offset 0, value 2 49.
0xe536bd0 (Cnfgr_Thread ): dosFsLib.c : Ensure this device is formatted and part itions are properly handled.
Verifying CRC of file in Flash File System


TFTP receive complete... storing in Flash File System...
File transfer operation completed successfully.
```

Figure 176 Downloading Software to the Switch

Use one of the following procedures to resolve this condition:

- Clear the configuration in flash by resetting the switch to factory defaults. See Restoring the System to the Default Configuration File on page 57.

- If the first procedure fails, you can format the flash using the Boot Code Utility menu: During the reload, when prompted, press **2** (Boot Menu), then **6** (Run flash diagnostics). Or press **2**, then **30** (Boot Code Utility Menu), then **14** (Format File System).

Caution: If you are not patient during the formatting, you WILL corrupt the code by interrupting or rebooting.

Recovering from a Software Upgrade Failure

When an image is downloaded to flash, as shown in Figure 177, SFTOS verifies the image CRC. Switch software can be corrupted during an upgrade by downloading the wrong file to the switch or by deleting the image file.

```
Force10 S50 #copy tftp://192.168.20.63/F10r2v3m1b9_switching.opr system:image
Mode..................................... TFTP
Set TFTP Server IP..... 192.168.20.63
TFTP Path.....
TFTP Filename..... F10r2v3m1b9_switching.opr
Data Type..... Code
Management access will be blocked for the duration of the transfer Are you sure you want to start? (y/n) y
TFTP code transfer starting
Verifying CRC of file in Flash File System
TFTP receive complete... storing in Flash File System...
File transfer operation completed successfully.
```

Figure 177 Downloading Software to the Switch

Recovering from a Lost Password

The default CLI user, *admin*, has read/write access, with no password until you create one. Once created, the only way to recover from a lost admin password is to reload the switch using facory defaults. See Restoring the System to the Default Configuration File on page 57.

Alternatively, if the user is not admin, then you can assign a new password to the user. See Creating a User and Password on page 39.

Preventing Auto-negotiation Mismatches

Note: The S2410 uses only 10-gigabit ports, which are auto-sensing and auto-negotiating, so the tips that are presented in this section in the configuration guides for other S-Series models are not relevant here.

Managing 10 Gigabit Interfaces

10-GE Interfaces

If a 10-Gigabit Ethernet (10-GE) interface does not reach a link up state, use the following steps:

1. Verify that you are using the correct XFP type. Optical specifications are available on the Force10 Networks Web site:

   http://www.force10networks.com/products/specifications.asp

2. Reseat the XFP or swap it with a known good one.
3. If you are using an XFP, connect one single fiber cable (as opposed to a pair) linking the Tx and Rx of the same XFP.
4. Cross-connect two 10-GE ports.

CX4 Interfaces

If you are using a CX4 module in an S50, S50V or S25P, adjust the preemphasis values with the **cx4-cable-length** {**long** | **medium** | **short**} command. Reducing the drive strength lowers the intensity (amplitude) of the signal being driven to the other end.

The S2410 automatically adjusts for the cable length, so the cx4 command set is not in SFTOS 2.4.1.

Software Forwarding

The process discussed above is often referred to as “software forwarding”, and sometimes “forwarded by the CPU” or “CPU routing”, where the system receives a unicast packet whose destination IP address cannot be resolved in the hardware, and so the packet is sent to the CPU to forward.

The routing software first looks for the destination MAC address in the ARP table, which it maintains. If it finds the address in the ARP table, it sends the packet to the Layer 2 application, which resolves it and finds the egress port from which to send it. If the software cannot find the destination in the ARP table, it sends an ARP request. After receiving the ARP reply, the Layer 2 tables can be updated, and subsequent packets can be routed by the hardware. In normal situations, the ARP request requires a small CPU hit, and CPU utilization drops once the destination is resolved.

Possible situations that require software forwarding for an extended period of time include:

- The system receives a lot of traffic with unresolvable destinations. The software constantly sends ARP requests for these packets, but no replies are received.
- The system receives packets with destination MAC addresses that cannot be resolved in the MAC Address table, but the destination IP address can be resolved in the ARP table. In this case, the hardware keeps sending the packets up to the CPU to retrieve ARP table entries to return to the Layer 2 application, but the Layer 2 application cannot find an associated egress interface from the MAC Address table.

The root cause, in most of these cases, is that the MAC Address table entry (Layer 2) times out earlier than the ARP Table entries (Layer 3). Make sure that the Layer 2 timeout period is longer than the Layer 3, and make sure that the ARP is configured to be a dynamic renew (the default).

In most network topologies, traffic flows are bidirectional. Therefore the Layer 2 table entries are constantly relearned/refreshed. However, in some cases, where the traffic flows are uni-directional, the Layer 2 entries time out before the Layer 3 entries, so the packets go to the CPU until the Layer 3 entries are timed out and new ARP requests are sent.

Configuring default/static routes does not help. Default routes create a static Layer 3 entry, but Layer 2 entries are still subject to timeouts in SFTOS.

Troubleshooting No Output on the Console

Your console might experience a temporary or seemingly permanent inability to display output. This symptom may be caused by one of the following transitory conditions:

- The switch is experiencing very high CPU utilization — a large number of frames for which there is no hardware forwarding entry or a large number of protocol packets being forwarded to the CPU for processing.
- Data is being transferred to or from the switch via TFTP, or the running configuration is being written to non-volatile memory. During these operations, all management access to the switch is blocked.
- A remote connection to the switch console via a communication server has been lost. To determine whether this symptom is occurring, ping the communications server. If the pings succeed, attempt to log into the server and kill the session connecting to your switch. Then re-connect.
- A topology loop is occurring in the network and flooding a large number of broadcasts or unknown unicast frames to all working interfaces in the same VLAN. Such excessive frame flooding can lead to high CPU utilization as the switch becomes overwhelmed with processing the unwanted frames. To prevent unwanted flooding, try the following:
  - — Enable Spanning Tree. In SFTOS, Spanning Tree is disabled by default.
  - — Shut down any ports not being used.

— Exclude VLAN 1 from all ports except the port used as the management port, as shown in the following example configuration for SFTOS Version 2.3.1.

```
Force10 S50 #config
Force10 S50 (Config)#interface  1/0/26
Force10 S50 (Interface 1/0/26)#no shutdown
Force10 S50 (Interface 1/0/26)#exit
Force10 S50 (Config)#interface vlan  10
Force10 S50 (Conf-if-vl-10)#untagged 1/0/26
Force10 S50 (Conf-if-vl-10)#exit
Force10 S50 (Config)#interface managementethernet
Force10 S50 (Config-if-ma)#ip address 10.16.128.167 255.255.255.0
Force10 S50 (Config-if-ma)#vlan participation 10
Force10 S50 (Config-if-ma)#exit
Force10 S50 (Config)#management route default 10.16.128.254
Force10 S50 (Config)#exit
Force10 S50 #ping 10.16.128.254
Send count=3, Receive count=3 from 10.16.128.254
!---Able to reach beyond the default gateway so:----!
Force10 S50 #ping 10.16.24.3
Send count=3, Receive count=3 from 10.16.24.3
Force10 S50 #
```

Figure 178 Dedicating a Management Port on a Non-Default VLAN

Use the following steps to troubleshoot the symptom of no output at the switch console:

1. Verify that a rollover cable is connected to the S2410 console port (a straight-through cable is used to the console port of all other S-Series models). To connect the switch's console port to a PC, use the included DB-9 connector. For details, see Connecting to the Console Port on page 31.
2. Verify your terminal emulation software is set to the following values (Note: If you are using Hyperterminal, select **Restore Defaults** to configure these values.):

```
Force10 S50 #show serial
Serial Port Login Timeout (minutes)..... 0
Baud Rate (bps)............................. 9600
Character Size (bits)....................... 8
Flow Control................................ Disable
Stop Bits................................... 1
Parity...................................... none
```

Figure 179 Using the show serial Command to Determine Terminal Settings

3. If you contact the Force10 Technical Assistance Center, please have the following information:

- How long did it take for the switch to show a response to a keystroke?
- Was the switch able to pass user traffic while the issue was occurring?
- What was the LED status? (If the switch remains able to pass traffic, the port LEDs should continue to blink. In particular, during a broadcast storm, all of the port LEDs should be blinking.)

- Do the link LEDs continue to be lit on removal of the cable connected to the port?
- Was the switch accessible via Telnet, SNMP, and/or HTTP?
- What type of traffic was flowing through the system?
- Were any other S50s in the network experiencing the same problem? If not, are they positioned in the network differently? Are they passing different kinds of traffic?

In addition, as a best practice, configure a remote management approach, such as SSH or HTTPS, to access an S-Series switch when console access is not possible but the switch is actively forwarding data traffic.

Appendix A IEEE, RFCs, and SNMP

This appendix contains these sections:

- IEEE Compliance
- RFC Compliance on page 212
- Industry MIBs Supported by SFTOS 2.4.1 on page 214
- Force10 MIBs on page 216
- SNMP-related RFCs on page 216
- SNMP Traps on page 218

This appendix contains auxiliary information to the section Setting up SNMP Management on page 87 in the Management chapter and the techtip “What Should I Poll with SNMP?” on the iSupport website: https://www.force10networks.com/csportal20/KnowledgeBase/ToolTipsSSeries.aspx

For more on SNMP commands, see the SNMP Community Commands section in the Management chapter of the *SFTOS Command Reference*.

IEEE Compliance

SFTOS 2.4.1 conforms to:

- 802.3ae—10 Gigabit Ethernet
- 802.3ab—1000Base-T
- 802.1D—Spanning Tree
- 802.1p — Ethernet Priority with User Provisioning & Mapping
- 802.1Q — Virtual LANs with Port based VLANs
- 802.1s — Multiple Spanning Tree Protocol
- 802.1v — Protocol-based VLANs
- 802.1w—Rapid Spanning Tree Protocol
- 802.1X — Port Based Authentication
- 802.3ad—Link Aggregation
- 802.3x — Flow Control
- GMRP — Dynamic L2 Multicast Registration
- GVRP — Dynamic VLAN Registration

RFC Compliance

The following is a list of the RFCs supported by SFTOS, listed by related protocol. The RFC categories under headings that include the parenthetical phrase “in Layer 3 Package only” are supported only in the Layer 3 Package (Routing) of SFTOS 2.5.1.

General Switching Protocols

- RFC 768 — UDP
- RFC 783 — TFTP
- RFC 791 — IP
- RFC 792 — ICMP (SFTOS aligns to the updated requirements in RFC 1812.)
- RFC 793 — TCP
- RFC 826 — ARP
- RFC 951 — BootP
- RFC 1213 — Management Information Base for Network Management of TCP/IP-based internets (MIB II)
- RFC 1321 — Message Digest Algorithm
- RFC 1493 — Definitions of Managed Objects for Bridges (Bridge MIB)
- RFC 1534 — Interoperation between BootP and DHCP
- RFC 2030 — Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2131 — (DHCP Client/Server component)
- RFC 2132 — DHCP Options and BootP Vendor Extensions
- RFC 2674 — The Q-BRIDGE of Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions (VLAN MIB)
- Draft-ietf-magma-snoop-10.txt — IGMP Snooping

Management

- HTML 4.0 Specification — December, 1997 (Compliant with 'HTML 4.01 Specification - December, 1999')
- Java and Java Script 1.3
- RFC 854 — Telnet
- RFC 855 — Telnet Option
- RFC 1155 — SMI v1
- RFC 1157 — SNMP v1/v2/v3
- RFC 1867 — HTML/2.0 Forms with file upload extensions
- RFC 2068 — HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
- RFC 2616 — HTTP/1.1
- RFC 2295 — Transparent Content Negotiation
- RFC 2296 — Remote Variant Selection; RSVA/1.0 State Management “cookies” (draft-ietf-http-state-mgmt-05)

- RFC 2572 — Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 2573 — SNMP v3 Applications
- RFC 2574 — User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 2575 — View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 2576 — Co-existence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework
- RFC 2578 — SMI v2
- RFC 2579 — Textual Conventions for SMI v2
- RFC 2580 — Conformance statements for SMI v2
- RFC 2246 — The TLS Protocol, Version 1.0
- RFC 2818 — HTTP over TLS
- RFC 3268 — AES Ciphersuites for Transport Layer Security

QoS

- RFC 2474 — Definition of the Differentiated Services Field (DS Field) in IPv4 Headers
- RFC 2475 — An Architecture for Differentiated Services
- RFC 2597 — Assured Forwarding PHB Group
- RFC 3246 — An Expedited Forwarding PHB (Per-Hop Behavior)
- RFC 3260 — New Terminology and Clarifications for DiffServ

RMON

- RFC 2819 — Remote Network Monitoring MIB: Ethernet Statistics Table, Ethernet History Control Table, Ethernet History Table, Alarm Table, Event Table, Log Table

Security

- MAC Address Security
- Port Access Control
- RFC 2865—RADIUS
- RFC 2866 — RADIUS Accounting
- RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 — RADIUS Extensions
- RFC 3579 — RADIUS Support for Extensible Authentication Protocol (EAP)
- rfc2869bis — RADIUS Support for Extensible Authentication Protocol (EAP)
- RFC 3580 — 802.1X RADIUS Usage Guidelines
- RFC 3128 — Protection Against a Variant of the Tiny Fragment Attack
- RFC 3164 — The BSD Syslog Protocol
- SSH v1/v2:

— Draft-ietf-secsh-transport-16 — SSH Transport Layer Protocol
— Draft-ietf-secsh-userauth-17 — SSH Authentication Protocol
— Draft-ietf-secsh-connect-17 — SSH Connection Protocol
— Draft-ietf-secsh-architecture—14 — SSH Protocol Architecture
— Draft-ietf-secsh-publickeyfile-03 — SECSH Public Key File
— Draft-ietf-secsh-dh-group-exchange-04 — Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol

MIBs

Industry MIBs Supported by SFTOS 2.4.1

You can display this list of industry MIBs supported by SFTOS in the report generated by the **show sysinfo** command:

Table 6 Industry MIBs Supported by SFTOS

MIB	Description
BRIDGE-MIB — RFC 1493	Definitions of Managed Objects for Bridges (dot1d)
DIFFSERV-DSCP-TC — RFC 3289	Management Information Base for the Textual Conventions used in DIFFSERV-MIB
DIFFSERV-MIB — RFC 3289	Management Information Base for the Differentiated Services Architecture
ENTITY-MIB — RFC 2737	Entity MIB (Version 2)
Etherlike-MIB — RFC 3635	Definitions of Managed Objects for the Ethernet-like Interface Types
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X
IF-MIB — RFC 2863	The Interfaces Group MIB using SMIv2
LAG-MIB	The Link Aggregation module for managing IEEE 802.3ad
P-BRIDGE-MIB — RFC 2674	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998
Q-BRIDGE-MIB — RFC 2674	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB (RFC 2620)
RADIUS-AUTH-CLIENT-MIB	RADIUS Authentication Client MIB (RFC 2618)
RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RMON-MIB — RFC 2819	Remote Network Monitoring Management Information Base

Table 6 Industry MIBs Supported by SFTOS (continued)

MIB	Description
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
SNMPv2-MIB — RFC 1907	The MIB module for SNMPv2 entities
USM-TARGET-TAG-MIB	User Security Model Target Module
Industry MIBs **not** listed in the output of the **show sysinfo** or **show version** commands:	
INTEGRATED-SERVICES-MIB	The MIB module to describe the Integrated Services Protocol
SNMP-PROXY-MIB	This MIB module defines MIB objects that provide mechanisms to remotely configure the parameters used by a proxy forwarding application.
SNMPV2-CONF	This management information base module includes definitions for conformance groups.
SNMPV2-SMI	This MIB module defines MIB objects for the Structure of Management Information (SMI).
SNMPV2-TC	The SNMPv2 textual conventions
SNMPV2-TM	The SNMPv2 over transport domain
Internet Addresses MIB	RFC 2851 — Used as a reference MIB for inetAddress Textual Conventions.
IANA-ifType-MIB	Used as a reference MIB for IANAifType Textual Convention.
IANA-RTP-PROTO-MIB	Used as a reference MIB for IANAipRouteProtocol, IANAipMRouteProtocol Textual Conventions.
RFC 2271 — SNMP Framework MIB	

Force10 MIBs

You can see this list of Force10-specific MIBs in the **show sysinfo** report:

Table 7 Force10-specific MIBs

MIB	Description
FORCE10-REF-MIB	Force10 Reference MIB
F10OS-POWER-ETHERNET-MIB	F10OS Power Ethernet Extensions MIB
F10OS-SWITCHING-MIB	F10OS Switching - Layer 2
F10OS-INVENTORY-MIB	F10OS Unit and Slot configuration
F10OS-PORTSECURITY-PRIVATE-MIB	Port Security MIB
F10OS-RADIUS-AUTH-CLIENT-MIB	F10OS Radius MIB
F10OS-MGMT-SECURITY-MIB	F10OS Private MIB for Management Security
F10OS-QOS-MIB	F10OS Flex QOS Support
F10OS-QOS-ACL-MIB	F10OS Flex QOS ACL
F10OS-QOS-DIFFSERV-EXTENSIONS-MIB	F10OS Flex QOS DiffServ Private MIBs' definitions
F10OS-QOS-DIFFSERV-PRIVATE-MIB	F10OS Flex QOS DiffServ Private MIBs' definitions
Force10 MIBs not listed in the output of the **show sysinfo** or **show version** commands:	
F10OS-DHCPSERVER-PRIVATE-MIB	The Force10 Networks Private MIB for S-Series DHCP Server
F10OS-OUTBOUNDTELNET-PRIVATE-MIB	The Force10 Networks Private MIB for SFTOS Outbound Telnet
F10OS-QOS-MIB	The MIB definitions for Quality of Service Flex package
F10OS-QOS-COS-MIB	The MIB definitions for Quality of Service - CoS Flex package
F10OS-SNTP-CLIENT-MIB	This MIB module defines a portion of the SNMP MIB under the Force10 Networks enterprise OID pertaining to SNTP client configuration and statistical collection.
F10OS-KEYING-PRIVATE-MIB	The Force10 Networks Private MIB for SFTOS Keying Utility

SNMP-related RFCs

The following is a list of other SNMP-related RFCs supported by SFTOS:

- RFC 1157: SNMP v1
- RFC 1212: Concise MIB Definition
- RFC 1213: SNMP v2 (MIB-II)
- 1492 TACACS+

- RFC 1493: Bridge MIB
- RFC 1643: Ethernet-like MIB
- RFC 1724: RIP v2 MIB extension
- RFC 1850: OSPF v2 MIB
- RFC 1901: Community based SNMPv2
- RFC 1905: Protocol Operations for SNMPv2
- RFC 1906: Transport Mappings for SNMPv2
- RFC 1907: Management Information Base for SNMPv2
- RFC 1908: Coexistence between SNMPv1 and SNMPv2
- RFC 2096: IP forwarding table MIB
- RFC 2233: The Interfaces Group MIB using SMI v2
- RFC 2570: SNMP v3
- RFC 2571: An Architecture for Describing SNMP Management Frameworks
- RFC 2665: Ethernet-like interfaces
- RFC 2674: VLAN MIB
- RFC 2787: Definitions of Managed Objects for the Virtual Router Redundancy Protocol (VRRP MIB)
- RFC 2819: RMON (Groups 1, 2, 3, 9)
- draft-ietf-magma-mgmd-mib-03.txt — Multicast Group Membership Discovery MIB
- Draft-ietf-idmr-dvmrp-mib-11.txt — DVMRP MIB

SNMP Traps

SNMP traps are the messages that are sent to designated trap receivers; they also appear in the report generated by the **show logging traplogs** command, an abbreviated sample of which appears in Figure 180. A replication of the trap also appears in the System log, as described in Displaying the SNMP Trap Log on page 99.

```
Force10 #show logging traplogs

Number of Traps Since Last Reset.............. 60926
Trap Log Capacity............................. 256
Number of Traps Since Log Last Viewed......... 59852

Log System Up Time           Trap
--- ------------------------ ------------------------------------------------
  0 3 days 10:23:55          Last or default VLAN deleted: VLAN: 10
  1 3 days 10:23:55          Last or default VLAN deleted: VLAN: 1
  2 1 days 05:27:21          Link Up: Unit: 1 Slot: 0 Port: 48
  3 1 days 05:18:11          Failed User Login: Unit: 1 User ID: ker.
  4 1 days 05:18:11          Failed User Login: Unit: 1 User ID: ker.
  5 1 days 05:18:10          Failed User Login: Unit: 1 User ID: th.
  6 1 days 05:18:09          Failed User Login: Unit: 1 User ID: ker.
  7 1 days 05:18:09          Failed User Login: Unit: 1 User ID: ngth.
  8 1 days 05:18:07          Failed User Login: Unit: 1 User ID: % Inva
  9 1 days 05:18:07          Failed User Login: Unit: 1 User ID: ngth.
 10 1 days 05:18:05          Failed User Login: Unit: 1 User ID: ker.
 11 1 days 05:18:04          Failed User Login: Unit: 1 User ID: ngth.
 12 1 days 05:18:02          Failed User Login: Unit: 1 User ID: ker.
```

Figure 180 Using the show logging traplogs Command

Note that the report states that the trap log capacity is 256 traps. So, if the capacity is reached, the log wraps; in other words, newer traps replace the oldest ones.

For more on SNMP management, see the Setting up SNMP Management on page 87. For more on logging, see the Syslog chapter, most specifically Displaying the SNMP Trap Log on page 99.

Index

Symbols
{deny|permit} 172

Numerics
10 GigE 26
10/100 Ethernet 3, 41
10/100 Ethernet port 81, 166
1000 Base-T (IEEE 802.3ab) 26
16k MAC Address Table 26

A
Access Control Lists (ACLs) 171
access control servers 38
ACL 171
ACL Interface Configuration (Web UI) 72
ACL Interface Configuration panel 72
ACL maximums 171
Adding a Port-channel to a VLAN 162, 182
addport 158, 161
addport interface range command 163
admin user 38
ARP requests 208
ARP table 207
audience 21
authentication login command 126, 127
authentication methods 121
auto-negotiate interface range command 163
Auxiliary port 30

B
baudrate command 32
books 22
Boot Code Utility menu 206
Boot Code, update 86
Boot Menu 57, 86, 206
boot sequence, system 57
BootP 26
BootP/DHCP relay agent 118
bootpdhcprelay command 119
bootpdhcprelay enable command 119
bootpdhcprelay maxhopcount command 119
bootpdhcprelay minwaittime command 119
bootpdhcprelay serverip command 119
BPDU tunneling 191
bridge 175
BRIDGE-MIB 214
Broadcast Storm Control, Enabling 133
Broadcast Storm Recovery (Web UI) 73
bulk configuration 163

C
cable, required 4
cable, straight-through 209
CD-ROM, S-Series 121
Changing Management VLAN from Default 83
Class of Service commands (CoS) 169
classofservice trust command 4
clear config command 55, 62
clear counters command 112
clear pass command 39
Clearing the Running Configuration 55
Clearing/resetting, VLAN 182
CLI command modes 33
CLI Overview 33
CLI pagination 34
config command 32
config file management 85, 86
configuration file, delete 57
configuration guide 22
configuration, restore to factory defaults 57
configuration, restoring to factory defaults 86
Configuring a Port Channel 158
Configuring a RADIUS Connection 124
Configuring from the Network 56
Connecting a Cable to the Console Port 31
console hang 208
console port 209
console troubleshooting 208
Contact and Patents Information 23
copy command 59
copy nvram 59
copy tftp 129
core port 190
CoS traffic class range 3
counter MIBs 87
CPU routing 207
Creating a User and Password 39
Creating the Management Port IP 81
crossover cable 4
CX4 cable configuration 3
CX4 module 207
CX4 pre-emphasis commands 3
cx4-cable-length command 207

D
DB-9 connector 209
Default Gateway 36, 82

default gateway 36
default management address 41
default routes 208
default user 38
default VLAN 41, 83, 176
default-router command 117
Delete 86
delete configuration file 57
deleteport 158
deny permit, QoS 172
description interface range command 163
Designated Root (DR) 149, 150
destination MAC 4
destination port (mirroring port) 199
DHCP pool 116
DHCP server 115
DHCP/BootP relay agent 115
DiffServ 3
DIFFSERV-DSCP-TC 214
DIFFSERV-MIB 214
Displaying GARP Properties 189
Displaying GARP, GVRP, GMRP 189
Displaying LAGs (Port Channels) 166
Displaying Logs 62
Displaying Statistics 38
Displaying Supported Features 37
Displaying System Uptime 37
dns-server command 117
Document conventions 22
DOS Protection 27
dot1p priority values 169
dot1x defaultlogin command 126
dot1x port-control command 126
dot1x system-auth-control command 126
dot3adTablesLastChanged 157
Double VLAN commands 190
Downloading Files 48
DSA 129
dvlan-tunnel l2pdu-forwarding enable command 191
dvlan-tunnel l2pdu-forwarding mac-address command 191

E

edge port enabling 141, 144
edge port feature 141, 144
egress queues 170
egress rate shaping 169, 170
Egress Rules, VLAN 177
enable CLI command mode 33
enable command 32
enable passwd command 40
enabling admin mode using Web UI 74
enabling all ports 40
Enabling Broadcast Storm Control 133
Enabling IGMP Snooping 197
Enabling Secure Management with SSH or SSL 128
Enabling Traps 88
enabling traps using Web UI 74
encapsulation command 163
encapsulation command (VLAN) 177
end station 175
ENTITY-MIB 214
Etherchannel group 155
Etherlike-MIB 214
Ethernet Management port 3, 30, 81, 166
Exempt Frames, VLAN 177

F

F10OS-DHCPSERVER-PRIVATE-MIB 216
F10OS-INVENTORY-MIB 216
F10OS-KEYING-PRIVATE-MIB 216
F10OS-MGMT-SECURITY-MIB 216
F10OS-PORTSECURITY-PRIVATE-MIB 216
F10OS-POWER-ETHERNET-MIB 216
F10OS-QOS-ACL-MIB 216
F10OS-QOS-COS-MIB 216
F10OS-QOS-DIFFSERV-EXTENSIONS-MIB 216
F10OS-QOS-DIFFSERV-PRIVATE-MIB 216
F10OS-QOS-MIB 216
F10OS-RADIUS-AUTH-CLIENT-MIB 216
F10OS-SNTP-CLIENT-MIB 216
F10OS-SWITCHING-MIB 216
flags, trap 88
Flow Control (802.3x) 110
Flow Control (IEEE 802.3x) 26
Flow Mode 110
Force10 MIBs 37
FORCE10-REF-MIB 216
Force10-specific MIBs 216
Forceversion Command 137
Format File System 206
forwarding database, differences between the terminal and Web interfaces 65
Forwarding Rules, VLAN 176
Forwarding, Aging, and Learning 135

G

GARP (Generic Attribute Registration Protocol) 185
GARP Commands 186
GARP Timers 185
gateway, default 36
generate-keys.sh 129
generate-pem.sh 129
generating SSL certificates 129
Generic Attribute Registration Protocol (GARP) 185
Global Config CLI command mode 33
Global Config Mode (SNMP traps) 89

GMRP (GARP Multicast Registration Protocol) 185
gmrp adminmode enable command 186
GMRP commands 186
gmrp interfacemode enable all command 186
Group IDs 177
GVRP 186
GVRP (GARP VLAN Registration Protocol) 185
gvrp adminmode enable command 186
GVRP commands 186
gvrp interfacemode enable command 186
GVRP, Using 187

H

hardware installation guide 22
hashing algoritm, traffic distribution 156
help commands 34
Host Name, Setting the 85
hostname command 85
HTML 42, 65
HTML-based Management 27
HTTP 42, 65
HTTPS 121, 128
HTTPS/SSL 27
Hyperterminal 209

I

IEEE 802.1d 26
IEEE 802.1q 26
IEEE 802.1Q tag 176
IEEE 802.1Q VLANs 175
IEEE 802.1s 26
IEEE 802.1w 26
IEEE 802.1X 121
IEEE 802.1x 27
IEEE 802.3 MAC interfaces 155
IEEE 802.3ab 26
IEEE 802.3ad 26
IEEE 802.3ae 26
IEEE 802.3x 26
IEEE8021-PAE-MIB 214
IfIndex values 166
IF-MIB 214
igmp command 163
igmp command (VLAN) 177
igmp enable command 197
igmp groupmembership-interval command 197
igmp interfacemode enable all command 197
igmp maxresponse command 197
igmp mcrtexpiretime command 198
IGMP Snooping 27
IGMP Snooping commands 197
industry MIBs 214
Ingress Rate Limiting 27
Installing the S2410 System 22
INTEGRATED-SERVICES-MIB 215
interface 161
interface command 126
interface command (VLAN) 84
Interface Config CLI command mode 33
interface managementethernet command 41, 83, 84
Interface modes
  Layer 2 103
interface range command 163
Interface Range mode 163
interface range port-channel command 163
interface slot/port command 201
Interface types
  100/1000 Ethernet 108
  10-Gigabit Ethernet 103
  Management 108
  management 103
  Port Channel 104
  VLAN 104
interface vlan 177
Interface VLAN CLI command mode 33
interface vlan command 84
interfaces
  clearing counters 111
Inventory Information (Web UI) 67
inverted mask 172
IP ACL Configuration panel 72
IP ACLs 3
ip address command 41
ip command family 163
ip dhcp excluded-address command 116, 117
ip dhcp pool command 117
ip dvmrp trapflags command 89
ip http javamode enable command 69
ip http secure-server command 131
ip pim-trapflags command 89
ip ssh command 130
iSupport 22
iSupport (SNMP information) 87, 89

J

Java mode, enable 69
JavaScript(TM) 42, 65
Jumbo Frame size 3
Jumbo Frame Support 26

L

LACP 165
LACP (Link Aggregation Control Protocol) 164
LACP enabling using Web UI 74
LACP Mode 110
LACP PDU 157

LAG described 155
LAG Implementation 156
LAG Load Distribution 156
LAG logical ID 162
LAG maximums 156
LAG-MIB 214
Layer 2 header 175
Layer 2 Multicast Forwarding 27
Line Config mode 32
lineconfig command 32
Link Aggregation Commands 157
Link Aggregation Control Protocol (LACP) 164
Link Aggregation Control Protocol Protocol Data Unit (LACP PDU) 157
Link Aggregation Groups (LAGs) 155
Link Aggregation MIB Support 157
Link Aggregation—IEEE 802.3 155
Link Status 110
Link Trap 110
Link trap notification 161
load-balancing algorithm, traffic 156
logging 63
  buffered 96
  persistent (Event log) 98
logging buffered command 96
logging buffered wrap command 96
logging cli-command command 96
logging console command 96
logging host command 100, 101
logging host reconfigure command 100
logging host remove command 100
logging syslog command 100
logical segments 175
Login Access Control 27
logs 63
loopback interface 103

M

MAC Access Control List (ACL) 172
mac access-group 173
mac access-list extended 172
mac access-list extended rename 173
MAC ACLs 4
MAC address 149
MAC Addresses 166
MAC-based Port Security 27
makestatic command 163, 188
makestatic command (VLAN) 177
Management 27
management access to the switch 128
management interface 103
management IP address 83
management IP interface 41, 87
Management Port icon (Web UI) 69
management route default command 41
management VLAN 83, 84
managing config files 85
managing running-config and system-config files 86
Managing SNMP Traps 88
maximum frame size (using Web UI) 74
maximum Jumbo Frame size 3
maximum LAG ports 3
Maximum MAC ACL rules 4
Maximum number of ACLs 4
maximum number of LAGs 3
MD5 121
MIB list, supported 37
MIB OIDs 87
MIBs 214
MIBs, counter 87
MIBs, Force10-specific 216
MIBs, supported industry 214
mirrored port (source port) 199
mode dot1q-tunnel command 191
modes, Global Config (SNMP traps) 89
modes, Privileged Exec (SNMP traps) 89
monitor session 1 201
monitor session 1 destination command 200
monitor session 1 mode command 200
monitor session 1 source interface command 200
Monitoring IGMP Snooping 198
MST CLI Management 143
MST Regions (Multiple Spanning Tree regions) 142
MSTP (IEEE 802.1s) 26
MSTP Implementation 142
MSTP Standards 142
mtu command 163, 190
mtu interface range command 163
Multicast Protocols (Layer 2) 27
Multiple Spanning-Tree Protocol 141

N

name command (VLAN) 84, 163, 177
network command 117
Network Connectivity Configuration (Web UI) 70
Network Connectivity Configuration panel 70
 157, 158
no monitor command 200
no monitor session 202
no monitor session 1 destination command 200
no monitor session 1 mode command 200
no monitor session 1 source interface command 200
no port-channel 158
no shutdown command 40
no spanning-tree edgeport 158
null interface 103
number of LAGs 3

O
objectives 21
OpenSSH URL 129
OpenSSL URL 129
operational code, delete 86

P
packet-forwarding distribution algorithm 156
pagination, controlling CLI 34
participation (VLAN) 163
partitions 175
password control options 38
patents 23
P-BRIDGE-MIB 214
persistent log (Event log) 98
Physical Mode 110
Physical Status 110
port 175
Port Access Control Port Configuration (Web UI) 77
port channel 155
port channel configuration 158
Port Channel Range 163
port channel, adding to a VLAN 162
Port channels
  defaults 104
Port Configuration (Web UI) 74
Port Configuration Panel 74
Port Detailed Statistics panel (Web UI) 71
Port ID format 3
port lacpmode enable all command 164
port lacpmode enable command 157, 164
port MAC locking 121, 201
Port Mirroring 27
Port Mirroring Configuration 200
port security 171
port security configuration 121
Port Security Interface Configuration (Web UI) 77
Port Summary Statistics panel (Web UI) 71
port type 109
port-based security 121, 171, 201
port-channel 157
port-channel command 159
port-channel enable all 157, 158
port-channel enable all command 159, 161
port-channel interface range command 163
port-channel linktrap 157
port-channel name 157
port-channel staticcapability 158, 164
port-channel staticcapability command 159, 165
Portfast 141
port-security 201
port-security command 201
port-security interface range command 163
preemphasis (CX4) 207
pre-emphasis commands 3
priority command (VLAN) 163
Privileged Exec CLI command mode 33
Privileged Exec Mode (SNMP traps) 89
probe port 199
protocol command (VLAN) 163
protocol group command (VLAN) 177

Q
Q-BRIDGE-MIB 214
QoS
  ACLs 26
  Priority Queues 26
QoS DiffServ 3
Quality of Service (QoS) policies 169
queue counters 169
queues 170
Quick Reference 22

R
RADIUS 27, 38, 121
radius accounting mode command 125, 126
RADIUS Configuration (Web UI) 78
RADIUS Connection, Configuring a 124
RADIUS Server Configuration panel 128
radius server host acct command 126
radius server host auth command 126, 127
radius server host command 125
radius server key acct command 126
radius server key auth command 126, 127
radius server key command 125
radius server msgauth command 125
radius server primary command 125, 127
radius server retransmit command 125
radius server timeout command 125
RADIUS-ACC-CLIENT-MIB 214
RADIUS-AUTH-CLIENT-MIB 214
Rapid Spanning Tree (IEEE 802.1w) 26
Rate limiting 169
Read/Write Access Using SNMP V3 39
Refresh button 67
Related Documents 22
release notes 22
reload command 55, 57
Remote Authentication Dial-In User Service (RADIUS) 124
restore configuration to factory defaults 57
Restoring the Configuration to Factory Defaults 85
RFC 1122 26
RFC 1157 212, 216
RFC 1212 216
RFC 1213 212, 216

RFC 1493 212, 214, 217
RFC 1534 115
RFC 1542 26, 115
RFC 1643 217
RFC 1724 217
RFC 1850 217
RFC 1901 217
RFC 1905 217
RFC 1906 217
RFC 1907 37, 215, 217
RFC 1908 217
RFC 2096 217
RFC 2131 26, 115, 212
RFC 2132 115
RFC 2233 217
RFC 2241 115
RFC 2242 115
RFC 2570 217
RFC 2571 217
RFC 2572 213
RFC 2574 213
RFC 2575 213
RFC 2576 213
RFC 2665 217
RFC 2674 212, 214, 217
RFC 2737 214
RFC 2787 217
RFC 2819 37, 90, 213, 214, 217
RFC 2863 214
RFC 2865 213
RFC 3289 214
RFC 3635 214
RFC 768 26, 212
RFC 783 212
RFC 791 26, 212
RFC 792 26, 212
RFC 793 26, 212
RFC 854 212
RFC Compliance 212
RFC list 212
RFC list, supported 37
RFC1213-MIB 214
RMON 27
RMON (Remote Network Monitoring) MIB 90
RMON-MIB 37, 214
rollover cable 4
routing interface range command 163
RSA1 129
RSA2 129
Run flash diagnostics 206
Running Configuration, Clearing 55
running-config and system-config files, managing 85, 86

S

S2410 management ports 30
S2410 Switch Navigation Icon (Web UI) 69
Save button 67
Saving the Startup Config to the Network 56
script apply command 61
script apply startup-config command 55
script delete command 60
script list command 62
script show scriptname.scr 59
Secure HTTP Configuration (Web UI) 78
Secure SHell (SSH) 121, 128
Secure Shell Configuration (Web UI) 79
Secure Sockets Layer (SSL) 121, 128
Security and Packet Control Features 27
Serial Port Configuration (Web UI) 69
serial session-limit command 32
serial session-timeout command 32
serial timeout command 32
service dhcp command 117
service port 30, 81, 166
Service Port Configuration panel 69
serviceport commands 3
serviceport ip 82
serviceport ip command 82
serviceport protocol command 82
session-limit command 32
session-timeout command 32
set garp timer join command 186
set garp timer leave command 186
set garp timer leaveall command 186
set igmp groupmembership-interval command 197
set igmp maxresponse command 198
set igmp mcrtexpiretime command 198
set interface range command 163
Setting Network Parms 41
Setting the Enable Password 40
Setting the Host Name 85
Setting Up a Management VLAN 44
SFTOS Command Reference 22
SFTOS Configuration Guide 22
shell script, generate-keys.sh 129
shell script, generate-pem.sh 129
show authentication command 122
show bootpdhcprelay command 119
show dot1q-tunnel command 191
show dvlan-tunnel command 191
show dvlan-tunnel l2pdu-forwarding command 191
show garp command 189
show gmrp configuration command 189
show gvrp configuration all command 187
show gvrp configuration command 189
show hardware command 35
show igmpsnooping 198

show interface 38
show interface ethernet 38
show interface ethernet command 148, 153
show interface ethernet switchport 38
show interface managementethernet command 36, 41, 84
show interface switchport 38
show ip dhcp server statistics command 118
show ip http command 131
show ip interface brief command 108
show ip ssh command 130
show logging buffered command 97, 130
show logging buffered example 97
show logging command 98
show logging example 98
show logging hosts command 101
show logging hosts example 101
show logging traplogs command 99
show logging traplogs example 99, 218
show mac access-list 173
show mac access-lists 173
show mac-address-table igmpsnooping command 198
show mac-addr-table command 166
show monitor 202
show monitor session 1 200
show monitor session command example 200
show network command 36
show port 203
show port all 203
show port command 111, 194
show port command example 203
show port-channel all command 158, 166
show port-channel brief 158
show port-channel brief command 159
show port-channel command 160, 161
show radius accounting statistics command 125
show radius command 125
show radius statistics command 125
show running-config 58
show running-config command 84, 194
show serial command 32
show serviceport 82
show serviceport command 36, 82, 87
show slot command 110
show snmpcommunity command 88
show snmptrap command 88
show sntp client command 91
show sntp server command 92
show spanning-tree brief command 143, 149
show spanning-tree interface command 143, 148
show spanning-tree mst detailed command 143
show spanning-tree mst port detailed command 143, 151
show spanning-tree mst port summary command 143, 150, 151, 152
show spanning-tree mst port summary report 150, 152
show spanning-tree mst summary command 143
show spanning-tree summary command 143, 148
show spanning-tree vlan command 143
show storm-control command 133
show switch command 34
show sysinfo command 35, 214, 216
show tacacs command 122
show tech-support command 35, 99
show terminal command 34
show trapflags command 89
show users command 39
show version command 35
show vlan association command 194
show vlan brief command 187, 188, 194
show vlan command 194
show vlan command example 195, 196
show vlan id command 83, 194
show vlan id command example 195
show vlan name command 194
show vlan port command 194
Showing Created Users 39
Showing Network Settings 36
shutdown interface range command 163
Simple Network Time Protocol (SNTP) 90
slot/port format 3
SNMP Community Configuration (Web UI) 68
SNMP Community Configuration panel 68
snmp interface range command 163
SNMP Management, Setting up 87
SNMP traps defined 87
SNMP Traps, Managing 88
SNMP v1/v2c 27
SNMP-COMMUNITY-MIB 215
SNMP-FRAMEWORK-MIB 215
SNMP-MPD-MIB 215
SNMP-NOTIFICATION-MIB 215
snmp-server command 88
snmp-server community command 87
snmp-server community ipaddr command 88
snmp-server community ipmask command 88
snmp-server community mode command 88
snmp-server community ro command 88
snmp-server community rw command 88
snmp-server enable trap violation command 88
snmp-server enable traps bcaststorm command 89
snmp-server enable traps linkmode command 89
snmp-server enable traps multiusers command 89
snmp-server enable traps stpmode command 89
snmp-server interface range command 163
snmp-server traps enable command 89
SNMP-TARGET-MIB 215
snmptrap command 87

snmptrap ipaddr command 88
snmptrap mode command 88
snmptrap snmpversion command 89
SNMP-USER-BASED-SM-MIB 215
SNMPv2-MIB 37, 215
SNMPV2-TC 215
SNMPV2-TM 215
SNMP-VIEW-BASED-ACM-MIB 215
SNTP 27, 90
sntp broadcast client poll-interval command 91, 92
sntp client mode broadcast command 91
sntp client mode command 92
sntp client mode unicast command 91
sntp client port command 91
SNTP Global Configuration panel of the Web UI 92
SNTP Global Status panel of the Web UI 93
sntp server command 91
SNTP Server Configuration Panel 94
SNTP Server Configuration panel of the Web UI 93
SNTP Server Status panel of the Web UI 94
sntp unicast client poll-interval command 92
sntp unicast client poll-retry command 92
sntp unicast client poll-timeout command 92
software forwarding 207
source port 199
Spanning Tree CST Port Config/Status panel 46, 74
Spanning Tree MST Configuration/Status (Web UI) 75
Spanning Tree MST Port Configuration/Status panel 76
Spanning Tree MSTPort Configuration/Status (Web UI) 76
Spanning Tree Protocol (IEEE 802.1d) 136
Spanning Tree Protocol (STP) 139
Spanning Tree Protocol (Web UI) 74
Spanning Tree Switch Configuration/Status panel 46
spanning-tree command 139, 143
spanning-tree configuration name command 143
spanning-tree configuration revision command 143
spanning-tree edgeport command 75, 144
spanning-tree forceversion command 143
spanning-tree forward-time command 143
spanning-tree hello-time command 143
spanning-tree interface range command 163
spanning-tree max-age command 143
spanning-tree mst command 143
spanning-tree mst cost command 74, 144
spanning-tree mst port-priority command 75, 144
spanning-tree mst priority command 143
spanning-tree mst vlan command 144
spanning-tree msti cost command 140
spanning-tree msti external-cost command 140
spanning-tree msti priority command 140
spanning-tree port mode all command 74, 143
spanning-tree port mode command 74, 144
spanning-tree port mode enable all command 139
spanning-tree port mode enable command 139
speed commands 3
S-Series CD-ROM 121
S-Series training 121
S-Series troubleshooting 205
SSH keys 128
SSH2 Server Support 27
SSHv2 27
SSL certificates 128
Stack Port Summary panel 71
startup configuration 55
startup-config file 55
Static LAG CLI Management 158
Static LAG Requirements 157
static route 208
status, link 110
status, physical 110
storm control, enabling 133
storm-control broadcast command 73, 133
STP (Spanning Tree Protocol) 26
STP BPDU tunneling 191
STP enabling using Web UI 74
STP, configure 74
straight-through cable 209
Subnet Mask 36, 82
Switch Configuration (Web UI) 73
Switch Configuration Panel 73
switch management access 128
switch navigation icon 69
Syslog 27
syslog host settings, changing 100
system boot sequence 57
System Description (Web UI) 66
system log command set 95
system reset 86

T

TACACS Server Host Configuration Options 124
TACACS+ 38
    Choosing TACACS+ as an Authentication Method 121
    deleting a server host 124
tagged command (VLAN) 163, 177
Tech Tips and FAQ, S-Series 22
Telnet (RFC 854) 27
terminal emulation 209
terminal length command 34
TFTP 128
TFTP (RFC 783) 27
TFTP procedure 49
timeout command 32
timeout, set console inactivity 32
traffic distribution algorithm 156
Traffic shaping 169

training, S-Series 121
Transferring Files 49
transport command 32
Trap Management 88
traps, enabling (using Web UI) 74
Troubleshooting 211
troubleshooting S-Series 205
trunking 155, 180
tunnel port 190
Type (port) 109

U
UDP 26
unit/slot/port format 3
untagged command (VLAN) 163, 177
Upgrading the Software Image 49
uplink port 190
user authentication methods 121
User Exec CLI command mode 33
User Management 38
username passwd command 39
users defaultlogin command 122, 127
Using GVRP 187
USM-TARGET-TAG-MIB 215

V
Verifying Management Port Connectivity 85
Verifying Management Port Network 84
Verifying Switch Numbers and OS Version 35
Viewing Software Version 34
Virtual LAN (VLAN) 175
VLAN 1 41, 176
vlan acceptframe command 178
VLAN configuration using Web UI 189
VLAN Configuration, Showing 194
vlan database 179, 180, 181
VLAN Database Mode Commands 177
vlan ingressfilter command 178
vlan interface range command 163
vlan participation all command 178
vlan participation command 83
vlan participation command (management VLAN) 84
vlan port acceptframe command 178
vlan port ingressfilter all command 178
vlan port pvid all command 178
vlan port tagging all command 178
vlan port untagging all command 178
vlan pvid command 178
VLAN Range 163
VLAN switch 175
vlan tagging command 178
vlan untagging command 178
VLAN, default 83
VLAN, IEEE 802.1Q 175
VLAN, management 83
VLANs 104
  adding a port channel 162
VLANs Implementation 176
VLAN-stack commands 190

W
Web UI
  ACL Interface Configuration 72
  command buttons 67
  introduction 65
  Inventory Information 67
  Network Connectivity Configuration 70
  online help 66
  Port Access Control Port Configuration 77
  Port Configuration 74
  Port Detailed Statistics panel 71
  Port Security Interface Configuration 77
  Port Summary Statistics 71
  RADIUS Configuration 78
  Secure HTTP Configuration 78
  Secure Shell Configuration 79
  Serial Port Configuration 69
  SNMP Community Configuration 68
  SNTP Global Configuration 92
  SNTP Global Status panel 93
  SNTP Server Configuration Panel 94
  SNTP Server Configuration panel 93
  SNTP Server Status panel 94
  Spanning Tree MST Configuration/Status 75
  Spanning Tree MSTPort Configuration/Status 76
  Switch Configuration 73
  System Description 66
Web UI to configure VLANs 189
Weighted Random Early Detection (WRED) 169
What Should I Poll with SNMP? 89
WRED 169
write memory command 205

X
Xmodem procedure 49

Z
zip file, SSH and SSL 129