

SFTOS Command Reference for the S2410

Version 2.4.1.0

Edition 2

April 2008



FORCE ™

Copyright 2008 Force10 Networks

All rights reserved. Printed in the USA. April 2008.

Force10 Networks reserves the right to change, modify, revise this publication without notice.

Trademarks

Force10 Networks® and E-Series® are registered trademarks of Force10 Networks, Inc. Force10, the Force10 logo, E1200, E600, E600i, E300, EtherScale, TeraScale, FTOS, and SFTOS are trademarks of Force10 Networks, Inc. All other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Force10 Networks reserves the right to make changes to products described in this document without notice. Force10 Networks does not assume any liability that may occur due to the use or application of the product(s) described herein.

USA Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designated to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance to the instructions, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures necessary to correct the interference at their own expense. Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Force10 Networks is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications in the equipment. Unauthorized changes or modification could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communication Statement

The digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Attention: Le présent appareil numérique n'émet pas de perturbations radioélectriques dépassant les normes applicables aux appareils numériques de la Class A prescrites dans le Règlement sur les interférences radioélectriques établi par le ministère des Communications du Canada.

European Union EMC Directive Conformance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Force 10 Networks can not accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of this product, including the fitting of non-Force10 option cards. This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/ European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.



Warning: This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case, the user may be required to take appropriate measures.

VCCI Compliance for Class A Equipment (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.



Danger: AC Power cords are for use with Force10 Networks equipment only, do not use Force10 Networks AC Power cords with any unauthorized hardware.

本製品に同梱いたしております電源コードセットは、本製品専用です。
本電源コードセットは、本製品以外の製品ならびに他の用途でご使用いただくことは出来ません。製品本体には同梱された電源コードセットを使用し、他製品の電源コードセットを使用しないで下さい。

Feedback on Documentation?
Send email to techpubs@force10networks.com

New Features

This preface describes SFTOS 2.4.1 by contrasting it to SFTOS 2.3.1.9.

Major Changes

Most of the differences in SFTOS 2.4.1 reflect the fact that SFTOS 2.4.1 is dedicated to supporting the S2410 models of the S-Series:

- **Layer 2 only:** The S2410 is limited to Layer 2 functionality, and therefore Layer 3 commands are not in the CLI, such as those for the OSPF and RIP protocols.
- **Stacking/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. Note, however, that some pre-existing example screenshots continue to show the *unit/slot/port* format.
- **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 [System Management Commands on page 55](#). You also have the option of managing the switch through the console port and management VLAN, which are common to all S-Series switches.
- **Speed commands:** All ports in the S2410 are fixed at 10GB, except the Ethernet Management port, which is set to auto-negotiate, so the speed and auto-negotiation commands in other versions of SFTOS are not included. See [System Configuration Commands on page 105](#).

Other Changes

SFTOS 2.4.1 contains some other differences, in comparison to SFTOS 2.3.1.9:

- **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.

- 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 15, LAG/Port Channel Commands, on page 249](#).
- Maximum Jumbo Frame size increased from 9216 to 10240.
- **IGMP Snooping**: The current S2410 hardware does not support IGMP Snooping, so the commands in the IGMP Snooping chapter appear in the CLI but do not function.
- ACLs, CoS, and QoS:
 - IP ACLs are not available.
 - The CoS traffic class range is four. See the commands using the *trafficclass* parameter in [Chapter 17, Quality of Service \(QoS\) Commands, on page 275](#).
 - QoS DiffServ is not supported.
 - The *ip_dscp* parameter of the **classofservice trust** command is not supported. See [classofservice trust on page 277](#).
 - Maximum number of ACLs increased from 100 to 1024.
 - Maximum MAC ACL rules per ACL increased from 8 to 64.
 - Only MAC ACLs with a source MAC are supported (cannot configure with a destination MAC)

Deprecated Commands

In SFTOS 2.4.1, the following VLAN commands, in the Global Config and Interface Config modes, exist in the CLI but are deprecated (They appear in the CLI, but do not work correctly in some situations, and will be removed in the next release.):

- **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 [Virtual LAN \(VLAN\) Commands on page 120](#).

- **[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 [port-channel staticcapability on page 253](#).

Contents

New Features	3
Major Changes	3
Other Changes	3
Deprecated Commands	4
Contents	5
About This Guide	21
Objectives	21
Audience	22
How to Use this Guide	22
Related Documents and Sources of Additional Information	23
Products and Services Liability	23
Contact Information	23
Documentation Feedback	24
The iSupport Website	24
Chapter 1	
SFTOS Overview	27
Switch Management Options	27
SFTOS 2.4.1 Features	28
Chapter 2	
Quick Start	31
Starting the Switch	31
Using the Boot Menu	32
System Info and System Setup	33
Physical Port Data	34
User Account Management	34
Management IP Address	35
Configuring the Management VLAN IP Address	36
Configuring the Ethernet Management Port	36
Uploading from the Switch through XMODEM	37
Downloading to the Switch through XMODEM	37
Downloading from a TFTP Server	38
Using Factory Defaults	38

Chapter 3	
Using the Command Line Interface	39
Command Syntax Conventions	39
Command Format	40
Command Parameters	40
“No” Form of a Command	41
Values	41
Addresses	42
Annotations	42
Keyboard Shortcuts	43
Obtaining Help at the Command Line	43
Using Command Modes	44
Mode-based Topology	45
Mode-based Command Hierarchy	48
Flow of CLI Operation	50
Chapter 4	
Using the Web User Interface	51
Configuring for Web Access	52
Web Page Layout	52
Starting the Web User Interface	52
Command Buttons	53
Chapter 5	
System Management Commands	55
General System Management and Information Commands	55
<i>dir</i>	56
<i>hostname</i>	57
<i>interface managementethernet</i>	58
<i>ip address (management)</i>	58
<i>mac-address</i>	59
<i>mac-type</i>	59
<i>management route default</i>	60
<i>mtu</i>	61
<i>network mac-address</i>	62
<i>network mac-type</i>	62
<i>network parms</i>	62
<i>network protocol</i>	62
<i>protocol</i>	63
<i>serviceport ip</i>	63
<i>serviceport protocol</i>	64
<i>show arp switch</i>	64
<i>show hardware</i>	65

<i>show interface</i>	65
<i>show interface ethernet</i>	67
<i>show interface managementethernet</i>	75
<i>show interface switchport</i>	76
<i>show interfaces</i>	77
<i>show logging</i>	78
<i>show mac-addr-table</i>	78
<i>show msglog</i>	80
<i>show network</i>	81
<i>show running-config</i>	81
<i>show serviceport</i>	82
<i>show sysinfo</i>	83
<i>show version</i>	84
<i>show tech-support</i>	86
<i>vlan participation (management)</i>	87
Telnet Commands	87
<i>ip telnet maxsessions</i>	88
<i>ip telnet timeout</i>	88
<i>ip telnet server enable</i>	89
<i>session-limit</i>	89
<i>session-timeout</i>	89
<i>show telnet</i>	90
<i>telnet</i>	90
<i>telnetcon timeout</i>	90
<i>telnetcon maxsessions</i>	91
Serial Commands	91
<i>lineconfig</i>	91
<i>serial baudrate</i>	91
<i>serial timeout</i>	92
<i>show serial</i>	92
SNMP Management Commands	94
<i>show snmpcommunity</i>	95
<i>show snmptrap</i>	95
<i>show trapflags</i>	96
<i>snmp-server</i>	97
<i>snmp-server community</i>	97
<i>no snmp-server community</i>	97
<i>snmp-server community ipaddr</i>	98
<i>snmp-server community ipmask</i>	98
<i>snmp-server community mode</i>	98
<i>snmp-server community ro</i>	99
<i>snmp-server community rw</i>	99
<i>snmp-server enable traps bcaststorm</i>	99

<i>snmp-server enable traps linkmode</i>	100
<i>snmp-server enable traps multiusers</i>	100
<i>snmp-server enable traps stpmode</i>	101
<i>snmp-server enable trap violation</i>	101
<i>snmp-server traps enable</i>	101
<i>snmptrap</i>	102
<i>snmptrap ipaddr</i>	102
<i>snmptrap mode</i>	102
<i>snmp trap link-status</i>	103
<i>snmp trap link-status all</i>	103
<i>snmptrap snmpversion</i>	103
Chapter 6	
System Configuration Commands	105
System Configuration Commands	105
<i>bridge aging-time</i>	106
<i>configure</i>	106
<i>enable</i>	107
<i>interface</i>	108
<i>interface range</i>	108
<i>monitor session</i>	112
<i>monitor session 1 mode</i>	113
<i>no monitor</i>	113
<i>no monitor session 1</i>	114
<i>show forwardingdb agetime</i>	114
<i>show mac-address-table</i>	114
<i>show mac-address-table multicast</i>	115
<i>show mac-address-table stats</i>	116
<i>show monitor session</i>	116
<i>show port</i>	117
<i>show port protocol</i>	119
<i>shutdown (Interface)</i>	119
<i>shutdown all</i>	119
Virtual LAN (VLAN) Commands	120
<i>clear vlan</i>	121
<i>description</i>	122
<i>encapsulation (VLAN)</i>	123
<i>interface vlan</i>	123
<i>makestatic</i>	124
<i>mtu (VLAN)</i>	125
<i>name (VLAN)</i>	125
<i>network mgmt_vlan</i>	126
<i>participation (VLAN)</i>	126

<i>priority (VLAN)</i>	126
<i>protocol group</i>	127
<i>protocol vlan group</i>	127
<i>protocol vlan group all</i>	128
<i>pvid (VLAN)</i>	128
<i>show vlan</i>	129
<i>show vlan port</i>	130
<i>tagged</i>	131
<i>untagged</i>	132
<i>vlan</i>	132
<i>vlan acceptframe</i>	133
<i>vlan database</i>	133
<i>vlan ingressfilter</i>	133
<i>vlan participation (interface)</i>	133
<i>vlan participation all</i>	134
<i>vlan port acceptframe</i>	134
<i>vlan port ingressfilter all</i>	134
<i>vlan port pvid all</i>	134
<i>vlan port tagging all</i>	135
<i>vlan port untagging all</i>	135
<i>vlan protocol group</i>	136
<i>vlan protocol group add protocol</i>	136
<i>vlan protocol group remove</i>	136
<i>vlan pvid</i>	137
<i>vlan tagging</i>	137
<i>vlan untagging</i>	137
System Utility Commands	138
<i>clear config</i>	138
<i>clear counters</i>	138
<i>clear port-channel</i>	139
<i>clear traplog</i>	139
<i>clear igmpsnooping</i>	139
<i>copy</i>	139
<i>copy (clibanner)</i>	141
<i>enable passwd</i>	142
<i>logout</i>	143
<i>quit</i>	143
<i>ping</i>	144
<i>reload</i>	144
<i>show terminal length</i>	144
<i>terminal length</i>	145
<i>traceroute</i>	145
<i>write</i>	146

Configuration Scripting	146
<i>script apply</i>	147
<i>script delete</i>	147
<i>script list</i>	147
<i>script show</i>	148
<i>script validate</i>	148
Chapter 7	
System Log	149
<i>logging buffered</i>	149
<i>logging buffered wrap</i>	150
<i>logging cli-command</i>	150
<i>logging console</i>	151
<i>logging host</i>	151
<i>logging host reconfigure</i>	152
<i>logging host remove</i>	152
<i>logging persistent</i>	152
<i>logging port</i>	152
<i>logging syslog</i>	153
<i>show logging</i>	153
<i>show logging buffered</i>	154
<i>show logging hosts</i>	155
<i>show logging traplogs</i>	156
Chapter 8	
User Account Commands	157
<i>clear pass</i>	157
<i>disconnect</i>	158
<i>show loginsession</i>	158
<i>show users</i>	158
<i>username passwd</i>	159
<i>users snmpv3 accessmode</i>	160
<i>users snmpv3 authentication</i>	160
<i>users snmpv3 encryption</i>	160
Chapter 9	
Security Commands	163
Port Security Commands	163
Implementation Notes	164
<i>port-security</i>	164
<i>port-security max-dynamic</i>	164
<i>port-security max-static</i>	165
<i>port-security mac-address</i>	165

<i>port-security mac-address move</i>	166
<i>show port-security</i>	166
<i>show port-security dynamic</i>	167
<i>show port-security static</i>	168
<i>show port-security violation</i>	168
Port-Based Network Access Control (IEEE 802.1X)	168
<i>authentication login</i>	169
<i>clear dot1x statistics</i>	170
<i>clear radius statistics</i>	170
<i>dot1x defaultlogin</i>	170
<i>dot1x initialize</i>	171
<i>dot1x login</i>	171
<i>dot1x max-req</i>	171
<i>dot1x port-control</i>	172
<i>dot1x port-control all</i>	172
<i>dot1x re-authenticate</i>	173
<i>dot1x re-authentication</i>	173
<i>dot1x system-auth-control</i>	174
<i>dot1x timeout</i>	174
<i>dot1x user</i>	175
<i>show authentication</i>	175
<i>show authentication users</i>	176
<i>show dot1x</i>	176
<i>show dot1x users</i>	179
<i>show users authentication</i>	179
<i>users defaultlogin</i>	180
<i>users login</i>	180
RADIUS Commands	180
<i>radius accounting mode</i>	181
<i>radius server host</i>	181
<i>radius server key</i>	182
<i>radius server msgauth</i>	183
<i>radius server primary</i>	183
<i>radius server retransmit</i>	183
<i>radius server timeout</i>	184
<i>show radius</i>	184
<i>show radius accounting statistics</i>	185
<i>show radius statistics (authentication)</i>	186
TACACS+ Commands	187
<i>tacacs-server host</i>	188
<i>tacacs-server key</i>	188
<i>tacacs-server timeout</i>	189
<i>key</i>	189

<i>port</i>	190
<i>priority</i>	190
<i>single-connection</i>	191
<i>show tacacs</i>	191
<i>timeout</i>	191
Secure Shell (SSH) Commands	192
<i>ip ssh maxsessions</i>	192
<i>ip ssh protocol</i>	193
<i>ip ssh server enable</i>	193
<i>ip ssh timeout</i>	194
<i>show ip ssh</i>	194
<i>sshcon maxsessions</i>	195
<i>sshcon timeout</i>	195
Hypertext Transfer Protocol (HTTP) Commands	195
<i>ip http javamode enable</i>	196
<i>ip http secure-port</i>	196
<i>ip http secure-protocol</i>	196
<i>ip http secure-server enable</i>	197
<i>ip http server enable</i>	197
<i>show ip http</i>	198
Broadcast Storm Control Commands	199
<i>show storm-control</i>	199
<i>storm-control broadcast</i>	200
<i>storm-control flowcontrol</i>	200

Chapter 10

DHCP Server Commands	203
<i>bootfile</i>	204
<i>clear ip dhcp binding</i>	204
<i>clear ip dhcp server statistics</i>	204
<i>clear ip dhcp conflict</i>	205
<i>client-identifier</i>	205
<i>client-name</i>	205
<i>default-router</i>	206
<i>dns-server</i>	206
<i>domain-name</i>	206
<i>hardware-address</i>	207
<i>host</i>	207
<i>ip dhcp bootp automatic</i>	208
<i>ip dhcp conflict logging</i>	208
<i>ip dhcp excluded-address</i>	208
<i>ip dhcp ping packets</i>	209
<i>ip dhcp pool</i>	209

<i>lease</i>	209
<i>network</i>	210
<i>netbios-name-server</i>	210
<i>netbios-node-type</i>	210
<i>next-server</i>	211
<i>option</i>	211
<i>service dhcp</i>	212
<i>show ip dhcp binding</i>	212
<i>show ip dhcp global configuration</i>	213
<i>show ip dhcp pool configuration</i>	213
<i>show ip dhcp server statistics</i>	214
<i>show ip dhcp conflict</i>	214
Chapter 11	
SNTP Commands	215
<i>sntp broadcast client poll-interval</i>	215
<i>sntp client mode</i>	216
<i>sntp client port</i>	216
<i>sntp unicast client poll-interval</i>	217
<i>sntp unicast client poll-timeout</i>	217
<i>sntp unicast client poll-retry</i>	217
<i>sntp server</i>	218
<i>show sntp</i>	218
<i>show sntp client</i>	219
<i>show sntp server</i>	220
Chapter 12	
VLAN-Stack Commands	221
<i>dvlan-tunnel ethertype</i>	221
<i>mode dot1q-tunnel</i>	222
<i>mode dvlan-tunnel</i>	222
<i>show dot1q-tunnel</i>	223
<i>show dvlan-tunnel</i>	224
Chapter 13	
GARP, GVRP, and GMRP Commands	225
GARP Commands	225
<i>set garp timer join</i>	225
<i>set garp timer leave</i>	226
<i>set garp timer leaveall</i>	227
<i>show garp</i>	227
GARP VLAN Registration Protocol (GVRP) Commands	228
<i>gvrp adminmode enable</i>	228

<i>gvrp interfacemode enable</i>	228
<i>gvrp interfacemode enable all</i>	229
<i>set gvrp adminmode</i>	229
<i>set gvrp interfacemode</i>	229
<i>set gvrp interfacemode all</i>	229
<i>show gvrp configuration</i>	229
GARP Multicast Registration Protocol (GMRP) Commands	231
GARP Multicast Registration Protocol (GMRP)	231
<i>gmrp adminmode</i>	231
<i>set gmrp adminmode</i>	232
<i>gmrp interfacemode enable all</i>	232
<i>set gmrp interfacemode</i>	233
<i>set gmrp interfacemode all</i>	233
<i>show gmrp configuration</i>	233
<i>show mac-address-table gmrp</i>	234

Chapter 14

IGMP Snooping Commands 235

<i>igmp enable (interface)</i>	236
<i>igmp enable (global)</i>	236
<i>igmp fast-leave (interface)</i>	237
<i>igmp groupmembership-interval (interface)</i>	237
<i>igmp interfacemode enable all</i>	238
<i>igmp maxresponse</i>	238
<i>igmp mcrtexpiretime (interface)</i>	239
<i>igmp mrouter (interface)</i>	240
<i>igmp mrouter interface enable</i>	240
<i>set igmp (interface)</i>	241
<i>set igmp (system)</i>	241
<i>set igmp fast-leave</i>	241
<i>set igmp groupmembership-interval (global)</i>	241
<i>set igmp groupmembership-interval (interface)</i>	242
<i>set igmp interface</i>	242
<i>set igmp interfacemode all</i>	242
<i>set igmp maxresponse (global)</i>	243
<i>set igmp maxresponse (interface)</i>	243
<i>set igmp mcrtexpiretime (global)</i>	244
<i>set igmp mcrtexpiretime (interface)</i>	244
<i>set igmp mrouter</i>	245
<i>show igmpsnooping</i>	245
<i>show igmpsnooping fast-leave</i>	246
<i>show igmpsnooping mrouter interface</i>	246
<i>show mac-address-table igmpsnooping</i>	247

Chapter 15

LAG/Port Channel Commands 249

<i>addport</i>	249
<i>deleteport (interface config)</i>	250
<i>deleteport (global config)</i>	251
<i>port-channel</i>	251
<i>port-channel enable all (global)</i>	251
<i>port-channel enable (interface)</i>	252
<i>port-channel linktrap</i>	252
<i>port-channel name</i>	253
<i>port-channel staticcapability</i>	253
<i>port lacpmode</i>	253
<i>port lacpmode enable all</i>	254
<i>port lacptimeout (global)</i>	254
<i>port lacptimeout (interface)</i>	255
<i>show port-channel brief</i>	255
<i>show port-channel</i>	256
<i>show port-channel summary</i>	257
<i>shutdown</i>	257

Chapter 16

Spanning Tree (STP) Commands 259

<i>show spanning-tree</i>	260
<i>show spanning-tree interface</i>	261
<i>show spanning-tree mst detailed</i>	262
<i>show spanning-tree mst port detailed</i>	262
<i>show spanning-tree mst port summary</i>	264
<i>show spanning-tree mst summary</i>	264
<i>show spanning-tree summary</i>	265
<i>show spanning-tree vlan</i>	265
<i>spanning-tree</i>	265
<i>spanning-tree bpdumigrationcheck</i>	266
<i>spanning-tree configuration name</i>	266
<i>spanning-tree configuration revision</i>	266
<i>spanning-tree edgeport</i>	267
<i>spanning-tree forceversion</i>	267
<i>spanning-tree forward-time</i>	268
<i>spanning-tree hello-time</i>	268
<i>spanning-tree max-age</i>	269
<i>spanning-tree max-hops</i>	269
<i>spanning-tree mst</i>	269
<i>no spanning-tree mst</i>	270
<i>spanning-tree mst instance</i>	271

<i>spanning-tree mst priority</i>	271
<i>spanning-tree mst vlan</i>	272
<i>spanning-tree port mode enable</i>	272
<i>spanning-tree port mode enable all</i>	273
Chapter 17	
Quality of Service (QoS) Commands	275
Class of Service (CoS) Commands	275
<i>classofservice dot1p-mapping</i>	276
<i>classofservice trust</i>	277
<i>cos-queue max-bandwidth</i>	277
<i>cos-queue min-bandwidth</i>	278
<i>cos-queue random-detect</i>	278
<i>cos-queue strict</i>	279
<i>random-detect exponential-weighting-constant</i>	279
<i>random-detect queue-parms</i>	280
<i>show classofservice dot1p-mapping</i>	281
<i>show classofservice trust</i>	281
<i>show interfaces cos-queue</i>	282
<i>show interfaces random-detect</i>	282
<i>show interfaces tail-drop-threshold</i>	283
<i>tail-drop queue-parms</i>	284
<i>traffic-shape</i>	285
Differentiated Services (DiffServ) Commands	285
Provisioning (IEEE 802.1p) Commands	285
<i>classofservice dot1pmapping</i>	285
<i>show classofservice dot1pmapping</i>	286
<i>vlan port priority all</i>	286
<i>vlan priority</i>	286
Chapter 18	
ACL Commands	287
Implementation Notes	288
<i>{deny permit}</i>	288
<i>mac access-list extended</i>	290
<i>mac access-list extended rename</i>	291
<i>mac access-group</i>	292
<i>show mac access-lists</i>	292
Index	295

List of Figures

Figure 1	Force10 Networks iSupport Website	24
Figure 2	Example of Accessing the Boot Menu with the reload Command	32
Figure 3	Example of Configuring the Ethernet Management Port	37
Figure 4	Partial Keyword Example	44
Figure 5	CLI Mode Diagram	46
Figure 6	Switch Navigation Icon in Web UI	53
Figure 7	Example of dir nvram Command Output	57
Figure 8	Example of Configuring Management Address	61
Figure 9	Output of the show interfaces unit/slot/port Command	66
Figure 10	Example of show interface ethernet switchport Output	68
Figure 11	Example of show interface ethernet unit/slot/port Output (truncated)	69
Figure 12	Output of the show interfaces description Command	78
Figure 13	Example of Output from the show mac-addr-table all Command	79
Figure 14	Example of Output from the show mac-addr-table count Command	80
Figure 15	Example of Output from the show mac-addr-table vlan Command	80
Figure 16	Using the show running-config command	82
Figure 17	show serviceport Command Output	83
Figure 18	lineconfig Command Example	91
Figure 19	configure Command Example	107
Figure 20	enable Command Example	107
Figure 21	Commands Available in Ethernet Range Mode	110
Figure 22	Bulk Configuration Warning Message	111
Figure 23	Single Range Bulk Configuration	111
Figure 24	Multiple Range Bulk Configuration for Gigabit Ethernet	111
Figure 25	Example of show forwardingdb agetime Command Output	114
Figure 26	Command Example: show mac-address-table stats	116
Figure 27	Command Example: show monitor session 1	117
Figure 28	show port all Command Output Example	118
Figure 29	show interfaces description Command Example	122
Figure 30	Using the interface vlan Command	124
Figure 31	Output of the show vlan Command	129
Figure 32	Output of the show vlan brief Command	130
Figure 33	Output of the show vlan id Command	130
Figure 34	Output of the show vlan port Command	131

Figure 35	Using the copy command to Upload the Event Log	141
Figure 36	Using the copy command to Download the CLI Banner	142
Figure 37	Sample Output from the show logging Command	153
Figure 38	Sample Output from the show logging Command	155
Figure 39	Example of show port-security all Command Output	167
Figure 40	Example of Output from the show dot1x detail Command	178
Figure 41	Example of Output from the show dot1x users Command	179
Figure 42	Example Output from the show users authentication Command	179
Figure 43	show radius accounting Command Example	185
Figure 44	show radius accounting statistics IP address Command Example	185
Figure 45	Example of show ip http Command Output	198
Figure 46	Command Example: show storm-control	199
Figure 47	show snmp Command Example	218
Figure 48	show snmp client Command Example	219
Figure 49	show snmp server Command Example	220
Figure 50	show gvrp configuration Command Output Example	230
Figure 51	Example of show port-channel brief Command Output	255

List of Tables

Table 1	Boot Menu Options	33
Table 2	Network Address Syntax	42
Table 3	Command Modes	47
Table 4	Interface ManagementEthernet Mode Command Families	58
Table 5	Fields in the Output of the show hardware Command	65
Table 6	Fields in Output of show interface <i>unit/slot/port</i> Command	66
Table 7	Fields in Output of show interface ethernet switchport Command	68
Table 8	Fields in Output of show interface ethernet <i>unit/slot/port</i> Command	70
Table 9	Fields in Output of show interface managementethernet command	75
Table 10	Fields in Output of show interface switchport Command	76
Table 11	Fields in Output of show serviceport command	83
Table 12	Fields in Output of show sysinfo Command	84
Table 13	Fields in Output of show version Command	84
Table 14	Fields of show serial Command Output	93
Table 15	Fields of show snmpcommunity Command Output	95
Table 16	Fields of show snmptrap Command Report	96
Table 17	Fields of show trapflags Command Report	96
Table 18	Commands in the Interface VLAN Mode	120
Table 19	show radius accounting Command Example Fields	185
Table 20	show radius accounting Command Example Fields	186
Table 21	Broadcast Storm Recovery Thresholds	200
Table 22	Default CoS Queue Prioritization	276
Table 23	Ethertype Keyword and 4-digit Hexadecimal Value	289

About This Guide

This guide describes configuration commands for SFTOS 2.4 software, which is dedicated to the S2410 models of the S-Series line of switches. The commands can be accessed from the SFTOS Command Line Interface (CLI), accessed through the console port or through a Telnet connection, and from the Node Manager component of Force10 Networks® Management System (FTMS).

This chapter covers the following topics:

- [Objectives](#)
- [Audience on page 22](#)
- [How to Use this Guide on page 22](#)
- [Related Documents and Sources of Additional Information on page 23](#)
- [Products and Services Liability on page 23](#)
- [Contact Information on page 23](#)
- [Documentation Feedback on page 24](#)
- [The iSupport Website on page 24](#)



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

Objectives

This document is intended as a reference guide for users of the SFTOS CLI commands — primarily for syntax information for constructing command input at the CLI. Also, in some cases, “screenshot” examples are provided.

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

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

Audience

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

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

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

How to Use this Guide

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

While you can infer a lot about the use of a command from its syntax statement, you are better served to see if the *SFTOS Configuration Guide* (Version 2.4) uses the command, because you can learn more about the context of its use.

Regarding RFCs and MIBs (management information base files) supported on the S2410 switch, syntax statements in this guide and related instructions in the *SFTOS Configuration Guide* cite the relevant RFCs. Also, an appendix in that guide contains a list of the RFCs and MIBs.

This guide is structured in this sequence:

- [New Features on page 3](#) is a quick way to access new and changed commands.
- [Chapter 1, SFTOS Overview](#) briefly introduces the S-Series hardware and SFTOS software.
- [Chapter 2, Quick Start](#) is an introduction to how to start and configure the S2410 using SFTOS software.
- Information on how this guide presents the CLI modes, syntax, conventions, and terminology is in [Chapter 3, Using the Command Line Interface, on page 39](#).
- The SFTOS Web User Interface (Web UI) is introduced in [Chapter 4, Using the Web User Interface](#).
- The CLI command syntax statements begin in [Chapter 5, System Management Commands](#). Chapters 6 through 11 describe commands that manage the system, while the later chapters describe commands specific to particular networking protocols. Beginning with Version 2.3, the CLI syntax statements that are new or changed include a Command History table.

Related Documents and Sources of Additional Information

The following documents provide information on using the S2410 switch and SFTOS 2.4 software. All of the documents are available on the Documents tab of iSupport (the Force10 Networks support website):

<http://www.force10networks.com/support>:

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

Except for the Tech Tips and FAQ documents, all of the documents listed above are also on the S2410 CD-ROM. Training slides are also on the CD-ROM.

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

Products and Services Liability

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

Contact Information

For technical support, see [The iSupport Website on page 24](#). For other questions, contact Force10 using the following address:

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

Documentation Feedback

Feedback on Documentation?
Send email to techpubs@force10networks.com

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

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

The iSupport Website

Access to some sections of the iSupport website do not require a password to access. However, if a section does require a password, you can request one at the website:

1. On the Force10 Networks website home page, www.force10networks.com, click the **Support** link, as highlighted at the top of [Figure 1](#).
2. Click the **Account Request** link.
3. Fill out the User Account Request form and click **Send**.
4. Click **Login**, and then enter the userid and password that you received by email.

The screenshot shows the Force10 Networks iSupport website. At the top, there is a navigation bar with links for LOGOUT, SEARCH, CONTACT, and HOME. Below this is a secondary navigation bar with links for PRODUCTS, APPLICATIONS, TECHNOLOGY, SUPPORT (highlighted), PARTNERS, NEWS/EVENTS, and COMPANY. A third bar contains links for UPDATE MY PROFILE and CUSTOMER SERVICE. The main header features the FORCE10 logo and the iSUPPORT logo. Below the header, there are tabs for HOME, SERVICE REQUEST, SOFTWARE CENTER, DOCUMENTS, and SUPPORT PROGRAMS. The main content area is titled "Customer Support" and includes a user profile for Draviam Paramasivan, a "My Open Cases" table, a "My Open RMA" section, and a "Hot Topics" list. There are also "Field Alerts" and "Announcements" sections.

Case #	Title	Priority	Created On	Status
C-07026	test pl ignore	P4	05/28/2005	Close-Pending

Hot Topics

- [FAQs](#)
- [Force10 Service and Support Guide](#)
- [Technical Tip: Restricting VTY Access](#)
- [Technical Tip: Adjusting MTU and Configuring Jumbo Frames Settings](#)

Figure 1 Force10 Networks iSupport Website

The i-Support website (www.force10networks.com/support/) contains five tabs:

- **Home:** Summary of open cases, RMA management, and field notices (as shown above)
- **Service Request:** Case management
- **Software Center:** Software downloads, bug fixes, and bug tracking tool

-
- **Documents:** User documentation, FAQs, field notices, technical tips, and white papers
 - **Support Programs:** Information on the complete suite of Force10 support and professional support services.

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.

You can also contact the Force10 Technical Assistance Center (TAC) by email or phone. For details, click the **Contact Support** link on the **Support** page of <http://www.force10networks.com>.

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

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

Switch Management Options

SFTOS 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 a management IP address configured on the dedicated Ethernet Management port and/or the management VLAN). This book focuses on the syntax of the commands that you use in the CLI.



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.
- **SFTOS Web User Interface (Web UI):** See [Chapter 4, Using the Web User Interface](#).

SFTOS 2.4.1 Features



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

The SFTOS 2.4.1 software provides the following features through a limited version (no stacking) of its “Layer 2 Package” (also called the “Switching Package”).

- BootP (RFC951, 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)
- Link Aggregation (IEEE 802.3ad)
- 16k MAC Address Table
- Jumbo Frame Support

QoS

- 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)
- ACL Entries (L2)

VLAN

- IEEE 802.1q Support
- Port-based VLANs
- Frame Extensions (IEEE 802.3ac)
- Protocol-based VLANs
- GVRP, GARP, GMRP

Multicast Protocols

- IGMP Snooping
- Layer 2 Multicast Forwarding

Security and Packet Control Features

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

Management

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

This chapter summarizes the procedures to start and operate the switch. For more detail, see the Getting Started chapter in the *SFTOS Configuration Guide* (and the rest of that guide) or the *S2410 Quick Reference*.

This chapter covers the following topics:

- [Starting the Switch](#)
- [Using the Boot Menu on page 32](#)
- [System Info and System Setup on page 33](#)
- [Physical Port Data on page 34](#)
- [User Account Management on page 34](#)
- [Management IP Address on page 35](#)
- [Uploading from the Switch through XMODEM on page 37](#)
- [Downloading to the Switch through XMODEM on page 37](#)
- [Downloading from a TFTP Server on page 38](#)
- [Using Factory Defaults on page 38](#)

Starting the Switch

You can access the Command Line Interface (CLI) of SFTOS (S-Series Force10 Operating System — the switch management software) in the S2410 locally or from a remote workstation. For remote access, see [Management IP Address on page 35](#).

1. Connect the power cord to turn the power on.
2. From a console connection, allow the S2410 to load the software until the following options are presented, as shown in [Figure 2](#):

```
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):
```

3. If you want to access the Boot menu, quickly press **2** and **Enter**. See [Using the Boot Menu on page 32](#).
Otherwise, wait until SFTOS finishes loading and the “User:” prompt appears (If the “Unit” prompt appears first, wait.). The device initial state is called the default mode.
4. Type the word **admin** in the login area. Do not enter a password because there is no password in the default mode.

-
5. Press ENTER two times. The prompt of the User Exec mode of the CLI is displayed.
 6. Enter **enable** to switch to the Privileged Exec mode. You can run all **show** commands from this mode, while some **show** commands do not run from User Exec mode.
 7. Enter **configure** to access the Global Config mode to enter configuration commands.
 8. Enter **exit** if you need to return to any previous mode.

Using the Boot Menu

The Boot menu is part of the boot code system software that loads before SFTOS and is separate from SFTOS. After you plug the switch in to power or after you execute the **reload** CLI command, the boot code displays the following options, as shown in [Figure 2](#):

```
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. Press **2** and **Enter** quickly to access the Boot menu.

```
Forcel0 #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.
Forcel0 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]
```

Figure 2 Example of Accessing the Boot Menu with the reload Command

2. At the **[Boot Menu]** prompt, press the number and **Enter** of the option that you want.
The options are:

Table 1 Boot Menu Options

Boot Menu Options	Details
1 - Start operational code	Start SFTOS (the same option as presented in the two-option startup menu).
2 - Change baud rate	Invoke a menu that offers console speed settings from 9600 to 115kb.
3 - Retrieve event log using XMODEM (64KB).	Upload a text file of the event log to an external folder through Xmodem running on the console. After selecting this option, you are given the chance to cancel the transfer by typing Ctrl-x several times.
4 - Load new operational code using XMODEM	Download a new version of SFTOS from an external folder through Xmodem running on the console.
5 - Display operational code vital product data	Lists SFTOS version and installed modules.
6 - Update Boot Code	[not active]
7 - Delete operational code	Remove the installed version of SFTOS. You might do this if you need to remove a corrupted image or if the NVRAM is too full to download a new version of SFTOS.
8 - Reset the system	This is the same as power cycling.
9 - Restore Configuration to factory defaults (delete config files)	Replace the startup-config with the default config.

For details on other Xmodem options, see [Uploading from the Switch through XMODEM on page 37](#) and [Downloading to the Switch through XMODEM on page 37](#). In general, for more information on options related to the Boot menu options, see the section “Managing Configuration and Software Files” in the *SFTOS Configuration Guide*.

System Info and System Setup

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

Command Syntax	Command Mode	Purpose
show hardware	Privileged Exec	Displays the serial number, software version the device contains, burned-in MAC address, and other device information.

Physical Port Data

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

Command Syntax	Command Mode	Purpose
show port all	Privileged Exec	Displays the ports in <i>unit/slot/port</i> format and the following data for each port: Type - Indicates if the port is a special type of port Admin Mode - Selects the Port Control Administration State Physical Mode - Selects the desired port speed and duplex mode Physical Status - Indicates the port speed and duplex mode Link Status - Indicates whether the link is up or down Link Trap - Determines whether or not to send a trap when link status changes LACP Mode - Displays whether LACP is enabled or disabled on this port.

User Account Management

To configure switch administrator accounts, use the following commands:

Command Syntax	Command Mode	Purpose
show users	Privileged Exec	Displays all of the users that are allowed to access the switch Access Mode - Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the 'admin' user has Read/Write access. There can only be one Read/Write user and up to five Read Only users.
show loginsession	Privileged Exec	Displays all of the login session information
[no] username user passwd password	Global Config	This command adds a new user (account) if space permits, along with the user's password. The user name and password can each be up to eight alphanumeric characters in length. To remove a user, use the no username user command. To delete or change a password, remove and reenter the user with the new password.
write memory or copy system:running-config nvrnram:startup-config	Privileged Exec	This will save passwords and all other changes to the device. If you do not save the configuration, all configurations are lost when a power cycle is performed on the switch or when the switch is reset. For copy command syntax, see copy on page 139 .
logout	User Exec and Privileged Exec	Logs the user out of the switch.



Note: Keywords and parameters that are shown within braces in syntax statements must be entered in the CLI. Keywords and parameters that are shown separated by a bar in syntax statements require you to choose one. Parameters in italics are variables for which you substitute a value. see [Command Syntax Conventions on page 39](#).

Management IP Address

In addition to logging into the CLI to view and manage network parameters, you can use the following methods:

- Simple Network Management Protocol (SNMP)
- SSH
- Telnet
- SFTOS Web User Interface (Web UI) through a Web browser (See [Using the Web User Interface on page 51](#).)

Each of these methods require that you first use the CLI through the console port to configure a management IP address, subnet mask, and default gateway. The S2410 actually provides the ability to configure two management IP addresses:

- An IP address that accesses the Ethernet Management port, an RJ-45/Ethernet port dedicated to managing the switch: See [Configuring the Ethernet Management Port on page 36](#)).
- An IP address that accesses the management VLAN running on a configurable set of the other physical ports. See the following procedure.



Helpful Hint: After configuring the network parameters, execute **write memory** so that the configuration changes are not lost.

Alternatively, you can execute **copy system:running-config nvram:startup-config** (if you love to type).

Configuring the Management VLAN IP Address

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

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

For details on command syntax for the commands listed above, see [General System Management and Information Commands on page 55](#).

Configuring the Ethernet Management Port

To configure the IP address of the Ethernet Management port, use the following commands:

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 and then manually configure the 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.

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
ServPort Configured Protocol Current..... None
Burned In MAC Address..... 00:01:E8:99:99:9A

(Force10 S2410) #
```

Figure 3 Example of Configuring the Ethernet Management Port

Uploading from the Switch through XMODEM

To copy to a PC through the console port with XMODEM, use the following command.

Command Syntax	Command Mode	Purpose
copy {nvram:startup-config nvram:errorlog nvram:log nvram:traplog} xmodem:// filepath/filename	Privileged Exec	The options/file types are: config — configuration file errorlog — error (Event) log log — System log system trace — system trace traplog — trap log This starts the upload and also displays the mode of uploading and the type of upload it is and confirms the upload is taking place. If you are using HyperTerminal, specify which file is to be sent to the switch.

Downloading to the Switch through XMODEM

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

Command Syntax	Command Mode	Purpose
copy xmodem://filepath/ filename {nvram:startup-config system:image}	Privileged Exec	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). If you are using HyperTerminal, specify which file is to be sent to the switch. The switch will restart automatically after the code has been downloaded.

Downloading from a TFTP Server

1. Before starting a TFTP server download, configure the management IP address of the switch; see [Management IP Address on page 35](#).
2. To download from a TFTP server, use the following command:

Command Syntax	Command Mode	Purpose
copy tftp://ip address/ {nvram:startup-config system:image} (See copy on page 139 .)	Privileged Exec	Set the destination (download) datatype: For the SFTOS software image, use system:image . For a configuration file, use nvram:startup-config . The URL is specified as: tftp://ipAddr/filepath (where <i>filepath</i> includes the filename, such as S2410/2410software.bin)

Using Factory Defaults

To load factory defaults, use either of the following commands:

Command Syntax	Command Mode	Purpose
clear config	Privileged Exec	Enter y at the prompt that asks if you want to clear all the configurations made to the switch.
reload (or cold boot of the switch)	Privileged Exec	Alternatively, use this command to restart the system and access the Boot menu, where you can select an option to load factory defaults. See Using the Boot Menu on page 32 . Enter y at the prompt that asks if you want to reset the system. Choose to reset the switch or cold boot the switch—both work effectively.

The SFTOS command line interface (CLI) is one of the three major ways to manage the S2410, and is the most complete. The SFTOS Web User Interface (Web UI) is discussed in [Chapter 4, Using the Web User Interface](#), and SNMP is addressed in [SNMP Management Commands on page 94](#) in the Management chapter.

This chapter covers the following topics:

- [Command Syntax Conventions on page 39](#)
- [Keyboard Shortcuts on page 43](#)
- [Obtaining Help at the Command Line on page 43](#)
- [Using Command Modes on page 44](#)
- [Mode-based Topology on page 45](#)
- [Mode-based Command Hierarchy on page 48](#)
- [Flow of CLI Operation on page 50](#)

Command Syntax Conventions

This guide uses the following conventions to describe command syntax:

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

The following conventions apply to the command name:

- The command name is displayed in bold font. It must be entered exactly as shown.
- When you have entered enough letters of a command name to uniquely identify the command, you can press the **space bar** or **Tab** key to cause the system to complete the word. For more keyboard shortcuts (speedkeys), see [Keyboard Shortcuts on page 43](#).

Command Format

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

snmp-server location *loc*

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

ip address *ipaddr subnetmask*

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

mtrace *sourceipaddr* [*destination*] [*group*]

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

mac-type {*local* | *burnedin*}

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

Command Parameters

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

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

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

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

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

“No” Form of a Command

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

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

Values

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

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

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

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

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

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

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

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

logical unit/slot/port—Logical unit, slot and port number. This is applicable in the case of a link aggregation group (LAG; also called a port channel). The operator can use the *logical unit/slot/port* to configure the LAG.

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

Addresses

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

Table 2 Network Address Syntax

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

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

Empty strings are not valid user-defined strings.

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

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

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

Annotations

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

Keyboard Shortcuts

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

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

Obtaining Help at the Command Line

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

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

- Type a partial keyword followed by a ?
A display of keywords beginning with the partial keyword is listed.

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

```
(Force10) #show ?
access-lists      Display Access List information.
arp               Display Address Resolution Protocol cache.
authentication    Display ordered methods for authentication lists
bootpdhcprelay   Display the value of BOOTP/DHCP relay parameters.
class-map        Display DiffServ Class information.
classofservice    Display class of service information.
diffserv         Display DiffServ information.
dot1q-tunnel     Display double VLAN Tunneling configuration.
dot1x            Display dot1x information.
dvlan-tunnel     Display double VLAN Tunneling configuration.
forwardingdb     Display Forwarding Database aging time.
garp             Display Generic Attribute Registration Protocol
                information.
gmrp             Display GMRP interface information.
gvrp             Display GARP VLAN Registration Protocol parameters.
hardware         Display vital product data.
igmpsnopping     Display IGMP Snooping information.
interface        Display summary statistics for a specific port or for
                the entire switch.
interfaces       Display Interfaces Information.
ip              Display IP information.
logging          Display logging and eventlog parameters.
--More-- or (q)uit

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

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

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

Figure 4 Partial Keyword Example

Using Command Modes

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

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

Mode-based Topology

As detailed above, the CLI is built on a mode concept, where related commands are grouped together within modes that you access with particular mode-access commands. The mode-access commands are listed in [Table 3 on page 47](#). Access to the modes is depicted in a tree format in [Figure 5](#).



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

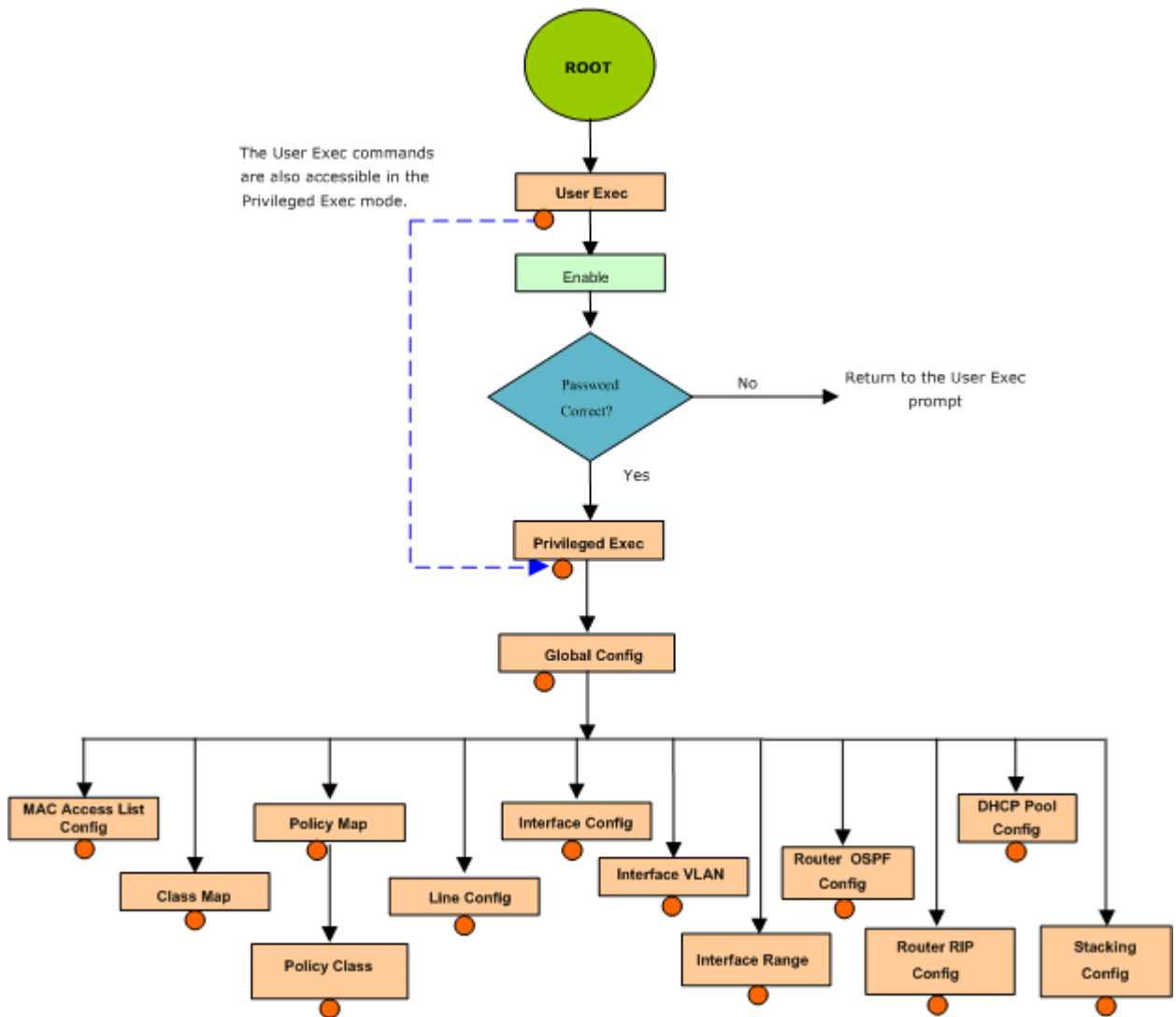


Figure 5 CLI Mode Diagram



Note: In Release 2.4.1, you access the Interface VLAN mode from the Global Config mode with the command **interface vlan *vlanid***.

Note: Some modes listed in [Table 3](#) are unavailable in SFTOS 2.4.1, including the Stacking mode and Layer 3 protocol modes, such as OSPF and RIP.

Access to all commands beyond the User Exec mode can be restricted through the **enable** password, which you set with the **enable passwd** command. See [enable passwd](#) on [page 142](#).

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

The *hostname* in the Prompt column is a placeholder for the prompt name that you create using the **hostname** command. For example, if you use “Speedy”, the User Exec prompt is **Speedy>**, the Privileged Exec prompt is **Speedy#**, and the Global Config prompt is **Speedy (Config) #**. For details, see [Figure 5 on page 46](#) and [Mode-based Command Hierarchy on page 48](#).

Table 3 Command Modes

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

Table 3 Command Modes

Command Mode	Mode Access Method	Prompt	Exit or Access Previous Mode
Mac Access List Config	In the Global Config mode, enter the mac access-list extended command	<i>hostname</i> (Mac-Access-List Config)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.
TACACS Config	In the Global Config mode, enter the tacacs-server host ip-address command.	<i>hostname</i> (Tacacs)#	To exit to the Global Config mode, enter the exit command. To return to the User Exec mode, enter Ctrl-Z.

Mode-based Command Hierarchy

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

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

The CLI provides the following modes:

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

Command Prompt: *hostname* >



Note: The *hostname* here is a placeholder for the prompt that you create using the **hostname** command. See [hostname](#) on page 57.

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

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

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

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

In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to the router interface configuration commands.

Command Prompt: *hostname (Interface)#*

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

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

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

Line Config Mode. Use this mode to configure the console interface. You may configure the interface from the directly connected console or the virtual terminal used with Telnet.

Command Prompt: *hostname (Line)#*

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

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

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

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

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

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

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

```
hostname (Config)# router ospf  
hostname (Config router)#
```

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

```
hostname (Config)# router rip  
hostname (Config router)#
```

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

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

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

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

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



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

Flow of CLI Operation

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

The parsing process is initiated whenever you type a command and press **ENTER**. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins.

For instance, the Privileged Exec mode has the command **show arp brief**. If you attempt to execute the command, but you enter an extra “p” in “arp”, then the output message displays the ^ marker under the extra “p”, followed by “*Invalid input detected at '^' marker.*”

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

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

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

This chapter covers the following topics:

- [Configuring for Web Access on page 52](#)
- [Web Page Layout on page 52](#)
- [Starting the Web User Interface on page 52](#)
- [Command Buttons on page 53](#)

This chapter is a brief introduction to the SFTOS Web User Interface (Web UI), enabling you to manage your switch through a Web browser and Internet connection. To access the switch, the Web browser must support:

- HTML version 4.0 or later
- HTTP version 1.1 or later
- JavaScript^(TM) version 1.2 or later

This chapter explains how to set up the switch for the Web UI, accessing the Web UI, and a brief introduction to the organization of the Web UI.

For details, see the Getting Started and Web User Interface chapters in the *SFTOS Configuration Guide*, along with sample Web UI screenshots in the other chapters of that book. Also, some command syntax statements in this book are followed by a field called Web User Interface that displays the equivalent panel in the Web UI.

It is important to note that there are equivalent functions in the Web UI to the terminal interface (that is, there are usually the same menus to accomplish a task). For example, when you log in, there is a Main Menu with the same functions available, and so on. To terminate the Web login session, close the browser.

There are several differences between the Web UI and terminal interfaces. For example, on the Web UI the entire forwarding database can be displayed, and the terminal interface only displays 10 entries starting at specified addresses.

Configuring for Web Access

To enable Web browser access to the switch:

1. Configure the switch for in-band connectivity. See [Management IP Address on page 35](#).
2. Enable HTTP Web access to the switch with either the **ip http server enable** command or **ip http secure-server enable** (for details, see [Hypertext Transfer Protocol \(HTTP\) Commands on page 195](#)).

Web Page Layout

An SFTOS Web UI panel consists of three frames.

Frame 1, across the top, displays a banner graphic of the switch.

Frame 2, at the bottom-left, displays a hierarchical tree view. The tree consists of a combination of folders, subfolders, and configuration and status HTML pages. You can think of the folders and subfolders as branches and the configuration and status HTML pages as leafs. Only the selection of a leaf (not a folder or subfolder) will cause Frame 2 to display a new HTML page. A folder or subfolder has no corresponding Frame 3 HTML page.

Frame 3, the bottom-right frame, displays the currently selected panel displaying either the device configuration status or the user configurable information that you have selected from the tree view of Frame 2, or both. You can resize each of these frames. There are no fixed-sized frames.

Also, if you enable the Java functionality, the frame displays the navigable switch graphic shown in [Figure 6 on page 53](#).

Starting the Web User Interface



Note: You must configure the IP address of the switch before using the Web interface.

Follow these steps to bring up the switch Web UI:

1. Enter the IP address of the switch in the Web browser address field.
2. When the Login panel is displayed, enter the appropriate User Name and Password. The User Name and associated password are the same ones used for the terminal interface. Click on the Login button. The navigation tree is displayed in Frame 2, and the System Description Menu is displayed in Frame 3.

3. Make your selection by clicking on the appropriate item in the navigation tree in Frame 2.

Command Buttons

The following command buttons are used throughout the Web UI panels:

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 next to the Apply button in Web interface panels refreshes the data on the panel.

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

The Web UI also has an optional switch navigation icon:

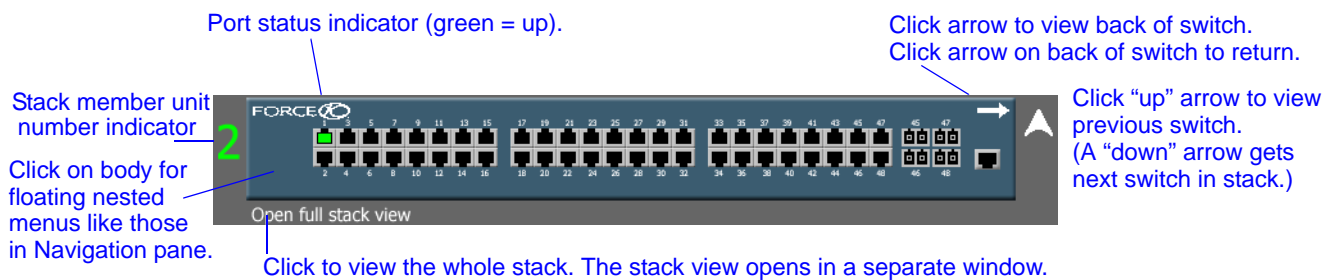


Figure 6 Switch Navigation Icon in Web UI

To enable the icon, execute the command **ip http javamode enable** from Global Config mode. Alternatively, you can use the Network Connectivity Configuration panel. Traverse the Navigation tree (left side of page) in this sequence:

System >> Configuration >> Network Connectivity Configuration

For details, see the Web User Interface chapter in the *SFTOS Configuration Guide*.

System Management Commands

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

This chapter contains the following major sections:

- [General System Management and Information Commands](#)
- [Telnet Commands on page 87](#)
- [Serial Commands on page 91](#)
- [SNMP Management Commands on page 94](#)



Note: For information on system configuration and utility commands (such as the **copy** command), see [System Configuration Commands on page 105](#).

For information on configuring and accessing the SFTOS Web User Interface (Web UI), see [Using the Web User Interface on page 51](#).

General System Management and Information Commands

This section describes the following commands:

- [dir on page 56](#)
- [hostname on page 57](#)
- [interface managementethernet on page 58](#)
- [ip address \(management\) on page 58](#)
- [mac-address on page 59](#)
- [mac-type on page 59](#)
- [management route default on page 60](#)
- [mtu on page 61](#)
- [network mac-address on page 62](#)
- [network mac-type on page 62](#)
- [network parms on page 62](#)

- [network protocol on page 62](#)
- [protocol on page 63](#)
- [serviceport ip on page 63](#)
- [serviceport protocol on page 64](#)
- [show arp switch on page 64](#)
- [show hardware on page 65](#)
- [show interface on page 65](#)
- [show interface ethernet on page 67](#)
- [show interface managementethernet on page 75](#)
- [show interface switchport on page 76](#)
- [show interfaces on page 77](#)
- [show logging on page 78](#)
- [show mac-addr-table on page 78](#)
- [show msglog on page 80](#)
- [show network on page 81](#)
- [show running-config on page 81](#)
- [show serviceport on page 82](#)
- [show sysinfo on page 83](#)
- [show version on page 84](#)
- [show tech-support on page 86](#)

dir

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

Syntax	dir nvram
Default	none
Mode	Privileged Exec
Command History	<hr/> Version 2.3 Introduced <hr/>

Example

```

Force10 #dir nvram

RamDiskVol:filesystem>
.
..
sslt.rnd                               1024
dhcpLeases.cfg                         85088
startup-config                         6392

Filesystem size 4179968
Bytes used      92504
Bytes free     4087464

CodeStorVol:>

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

Filesystem size 20022272
Bytes used      131040
Bytes free     19891232

Force10#

```

Figure 7 Example of dir nvram Command Output

hostname

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

Syntax	hostname <i>hostname</i>
Parameters	<i>hostname</i> Enter the desired text for the prompt, up to 64 alphanumeric characters.
Default	Force10 S50 (For example, the User Exec prompt appears as “(Force10 s50) >”.)
Mode	Global Config
Command History	Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode.
	Version 2.2 Replaced set prompt command.

interface managementethernet

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

Syntax `interface managementethernet`

Mode Global Config

Command History

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

Usage Information This command provides access to the following network configuration command groups:

Table 4 Interface ManagementEthernet Mode Command Families

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

Related Commands

ip address (management)	Configures the IP address of the management interface.
mac-address	Configure the MAC address of the management interface.
mac-type	Configure the MAC type of the management interface.
management route default	Set the IP gateway of the switch
protocol	Set the network protocol of the management interface.
show interface	Display a summary of statistics for a specific port, including the management port, or a count of all CPU traffic based upon the argument.
ip http server enable	Enable access to the switch through the Web User Interface (Web UI) of SFTOS.
vlan participation (management)	Set the VLAN ID of the management interface.

ip address (management)

This command configures the IP address of the management interface.

Syntax `ip address ipaddr subnetmask`

The value for *ipaddr* is the IP Address of the management interface. This is the IP address that you would enter in your Web browser to access the SFTOS Web User Interface.

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

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

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

mac-address

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

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

mac-type


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

Syntax **mac-type** {**local** | **burnedin**}

Default	None
Mode	Interface ManagementEthernet
Command History	Version 2.3 Introduced. Replaces the network mac-type command.
Related Commands	interface managementethernet Invokes the Interface ManagementEthernet mode, the (Config-if-ma)# prompt.

management route default

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

Syntax	management route default <i>gateway</i>
Parameters	<i>gateway</i> Valid IP address
	Use no management route default to remove the gateway.
Mode	Global Config
Command History	Version 2.3 Introduced: Replaces the network parms command for the gateway part of the management address.
Usage Information	Use this command along with the ip address command to configure the management address of the switch. Execute the interface managementethernet command from Global Config mode to access the ip address command, as shown in the following example.
	 Note: The IP Address and the gateway must be on the same subnet.

Example

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

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

Figure 8 Example of Configuring Management Address**Related
Commands**

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

mtu

This command sets the maximum transmission unit (MTU) size (in bytes) for physical and LAG (port channel) interfaces.

Syntax `[no] mtu 1518-10240`

For the standard implementation, the range of the MTU size is a valid integer between 1518-10240.

The **no mtu** command sets the default maximum transmission unit (MTU) size (in bytes) for the interface.

Default 1518



Note: 10-Gigabit ports use a chipset that does not automatically allow for the length of a tag. For 10-Gigabit ports, the default setting of 1518 means 1518 untagged or tagged. The maximum is 10240 bytes.

Mode Interface Config

network mac-address

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

Mode	Privileged Exec
Command History	<hr/> Version 2.3 Introduced. Replaced by the mac-address command. <hr/>

network mac-type

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

Mode	Privileged Exec
Command History	<hr/> Version 2.3 Introduced. Replaced by the mac-type command. <hr/>

network parms

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

network protocol

This command is replaced by the [protocol](#) command in Version 2.3.

Mode	Privileged Exec
Command History	<hr/> Version 2.3 Introduced. Replaces the protocol command. <hr/>

protocol

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

Syntax **protocol** {**none** | **bootp** | **dhcp**}

If you modify this value, the change is effective immediately. The **bootp** keyword indicates that the switch periodically sends requests to a Bootstrap Protocol (BootP) server or a DHCP server until a response is received. The **none** keyword indicates that the switch should be manually configured with IP information.

Default **none**

Mode Interface ManagementEthernet

Command History

Version 2.3	Introduced. Replaces the network protocol command.
-------------	--

Related Commands

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

serviceport ip

This command configures the IP address of the *Ethernet Management port (service port)*.

Syntax **serviceport ip** *ipaddr netmask* [*gateway*]

For *ipaddr*, designate an IP address of the Ethernet Management port. This is the IP address that you would enter in your Web browser to access that port through the SFTOS Web User Interface. The default is 0.0.0.0.

For *netmask*, designate a 4-digit dotted-decimal number that represents the subnet mask of the Ethernet Management port IP address.

The value for *gateway* is the gateway IP address to the Ethernet Management port IP address. The default is 0.0.0.0.

Enter **no serviceport ip address** to remove the IP address configuration.

Mode Global Config mode

Command History

Version 2.4.1	Introduced
---------------	------------

Related Commands	serviceport protocol	Set the network configuration protocol to be used for configuring access to the Ethernet Management port.
	show serviceport	Display the IP configuration and MAC address of the Ethernet Management port.

serviceport protocol

This command specifies the network configuration protocol to be used for configuring access to the Ethernet Management port.

Syntax `serviceport protocol {none | bootp | dhcp}`

If you modify this value, the change is effective immediately.

Use the **bootp** keyword to require the switch to periodically send requests to a Bootstrap Protocol (BootP) server for an IP address for the port, or use **dhcp** to call a DHCP server until a response is received. The **none** keyword indicates that the Ethernet Management port should be manually configured with IP information.

Default `none`

Mode Global Config

Command History	Version 2.4.1	Introduced.
------------------------	---------------	-------------

Related Commands	serviceport ip	Set the IP, subnet mask, and IP gateway of the Ethernet Management port.
	show serviceport	Display the IP configuration and MAC address of the Ethernet Management port.

show arp switch

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

Syntax `show arp switch`

Mode Privileged Exec

Usage Report fields include:

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

IP Address—The IP address assigned to each interface

unit/slot/port—Valid unit, slot and port number separated by forward slashes.

show hardware

This command displays inventory information for the switch.

Syntax **show hardware**

Mode Privileged Exec

Table 5 Fields in the Output of the show hardware Command

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

show interface

This command displays a summary of statistics for a specific port.

Syntax **show interface** *unit/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.

Mode Privileged Exec

Web User Interface Inventory Information panel, accessed from the System node

Usage Information The **show interface** command accepts other keywords besides *unit/slot/port*. See those syntax statements following this one.

Figure 9 shows an example of the **show interface** report when the argument is *unit/slot/port*. Table 6 contains an explanation of the report fields.

Example

```
Force10#show interface 1/0/2
Packets Received Without Error..... 0
Packets Received With Error..... 0
Broadcast Packets Received..... 0
Packets Transmitted Without Errors..... 579
Transmit Packet Errors..... 0
Collision Frames..... 0
Time Since Counters Last Cleared..... 0 day 0 hr 18 min 58 sec
```

Figure 9 Output of the show interfaces unit/slot/port Command

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

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

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

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

show interface ethernet

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

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

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

Mode Privileged Exec

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

[Figure 10 on page 68](#) shows an example of the **show interface ethernet** report when the keyword **switchport** is added. [Table 7 on page 68](#) contains an explanation of the report fields.

[Figure 11](#) shows an example of the **show interface ethernet** report when the argument is *unit/slot/port*. [Table 8](#) contains an explanation of the report fields.

Example 1

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

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

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

Figure 10 Example of show interface ethernet switchport Output

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

Table 7 Fields in Output of show interface ethernet switchport Command

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

Table 7 Fields in Output of show interface ethernet switchport Command (continued)

Field	Description
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot
Address Entries Currently in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared

Example 2

```
(Force10) #show interface ethernet 1/0/1
Type..... Normal
Admin Mode..... Enable
Physical Mode..... Auto
Physical Status..... Up
Speed..... 1 Gig
Link Status..... Up
MAC Address..... 0001.E8D5.A0F8
Total Packets Received (Octets)..... 15508603844
Packets Received > 1522 Octets..... 0
Packets RX and TX 64 Octets..... 0
Packets RX and TX 65-127 Octets..... 216200946
Packets RX and TX 128-255 Octets..... 2441
{More}
```

Figure 11 Example of show interface ethernet unit/slot/port Output (truncated)

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

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

Field	Description
Packets Received	
Type	Indicates current type of use of the port, such as "PC Mbr" to indicate port channel member, "Mirror" to indicate source port for port-mirroring, "Probe" to indicate destination port for mirroring, and, most commonly, "Normal".
Admin Mode	Whether the port is administratively enabled or disabled
Physical Mode	Whether the port is physically up or down
Physical Status	Whether the port is physically connected or disconnected
Speed	The port speed setting
Link Status	Whether the link is up or down.
MAC Address	MAC address of the port
Total Packets Received (Octets)	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ---- The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.
Packets Received < 64 Octets	The total number of packets (including bad packets) received that were < 64 octets in length (excluding framing bits but including FCS octets).
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Received 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Table 8 Fields in Output of show interface ethernet *unit/slot/port* Command (continued)

Field	Description
Packets Received 1519-1522 Octets	The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received > 1522 Octets	The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	
Total	The total number of packets received that were without errors
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received with MAC Errors	
Total	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments/Undersize Received	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
Rx FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow
Received Packets not forwarded	
Total	A count of valid frames received which were discarded (i.e. filtered) by the forwarding process

Table 8 Fields in Output of show interface ethernet *unit/slot/port* Command (continued)

Field	Description
Local Traffic Frames	The total number of frames dropped in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.
VLAN Membership Mismatch	The number of frames discarded on this port due to ingress filtering.
VLAN Viable Discards	The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.
Multicast Tree Viable Discards	The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.
Reserved Address Discards	The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.
Broadcast Storm Recovery	The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled
CFI Discards	The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.
Upstream Threshold	The number of frames discarded due to lack of cell descriptors available for that packet's priority level.
Packets Transmitted Octets	
Total Bytes	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets)
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets)

Table 8 Fields in Output of show interface ethernet *unit/slot/port* Command (continued)

Field	Description
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 1519-1522 Octets	The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets)
Max Info	The maximum size of the Info (non-MAC) field that this port will receive or transmit
Packets Transmitted Successfully	
Total	The number of frames that have been transmitted by this port to its segment
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent
Transmit Errors	
Total Errors	The sum of Single, Multiple, and Excessive Collisions
Tx FCS Errors	The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Oversized	The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission
Transmit Discards	
Total Discards	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions
Port Membership	The number of frames discarded on egress for this port due to egress filtering being enabled

Table 8 Fields in Output of show interface ethernet *unit/slot/port* Command (continued)

Field	Description
VLAN Viable Discards	The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured
Protocol Statistics	
BPDU's received	The count of BPDUs (Bridge Protocol Data Units) received in the spanning tree layer
BPDU's Transmitted	The count of BPDUs (Bridge Protocol Data Units) transmitted from the spanning tree layer
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDU's Received	The count of GVRP PDUs received in the GARP layer
GVRP PDU's Transmitted	The count of GVRP PDUs transmitted from the GARP layer
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed
GMRP PDU's received	The count of GMRP PDU's received in the GARP layer
GMRP PDU's Transmitted	The count of GMRP PDU's transmitted from the GARP layer
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received
RST BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received
Dot1x Statistics	
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared

**Related
Commands**

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

show interface managementethernet

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

Syntax **show interface managementethernet**

Mode Privileged Exec

Command History

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

Usage Information

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

Table 9 Fields in Output of show interface managementethernet command

Field	Description
IP Address	The IP address of the interface. The factory default value is 0.0.0.0
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0
Burned In MAC Address	The burned in MAC address used for in-band connectivity
Java Mode	Enable or Disable. Specifies if the switch should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is disabled.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgIdentifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	Specifies which MAC address should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.
Management VLAN ID	Specifies the management VLAN ID.
Network Configuration Protocol Current	Indicates which network protocol is being used. The options are bootp dhcp none.
Web Mode	Enable or Disable

Related Commands	ip address (management)	Configures the IP address of the management VLAN.
	show interface	Displays detailed statistics for a specific port or for all CPU traffic based upon the argument.
	show interface switchport	Displays a summary of statistics on Layer 2 interfaces.
	show interface ethernet	Displays detailed statistics for a specific ethernet port or for all CPU traffic based upon the argument.
	show serviceport	Displays the configuration of the Ethernet Management port.

show interface switchport

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

Syntax **show interface switchport**

Mode Privileged Exec

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

Table 10 Fields in Output of show interface switchport Command

Field	Description
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.

Table 10 Fields in Output of show interface switchport Command

Field	Description
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

Related Commands

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

show interfaces

This command displays information about a selected interface or VLAN.

Syntax	show interfaces { description { <i>unit/slot/port</i> 1-3965} cos-queue [<i>unit/slot/port</i>]}				
Parameters	<table border="1"> <tbody> <tr> <td>description {<i>unit/slot/port</i> 1-3965}</td> <td>(OPTIONAL) Enter the keyword description followed by a VLAN ID to display information for that VLAN, or to report on a particular interface, identify the interface in the form <i>unit/slot/port</i>.</td> </tr> <tr> <td>cos-queue [<i>unit/slot/port</i>]</td> <td>(OPTIONAL) For details on this option, see show interfaces cos-queue on page 282.</td> </tr> </tbody> </table>	description { <i>unit/slot/port</i> 1-3965}	(OPTIONAL) Enter the keyword description followed by a VLAN ID to display information for that VLAN, or to report on a particular interface, identify the interface in the form <i>unit/slot/port</i> .	cos-queue [<i>unit/slot/port</i>]	(OPTIONAL) For details on this option, see show interfaces cos-queue on page 282 .
description { <i>unit/slot/port</i> 1-3965}	(OPTIONAL) Enter the keyword description followed by a VLAN ID to display information for that VLAN, or to report on a particular interface, identify the interface in the form <i>unit/slot/port</i> .				
cos-queue [<i>unit/slot/port</i>]	(OPTIONAL) For details on this option, see show interfaces cos-queue on page 282 .				
Mode	Privileged Exec				
Command History	Version 2.3 Modified: Added description [<i>unit/slot/port</i>] parameter.				

Usage Information

The following example shows sample output of the **show interfaces description** command with an interface specified in the *unit/slot/port* form:

Example

```

Force10#show interfaces description 1/0/1


Interface.....1/0/1
IfIndex.....1
Description....1/0/1 is access port
MAC Address....00:01:E8:D5:BA:C0
Bit Offset Val..1
    
```

Figure 12 Output of the show interfaces description Command

Related Commands

description	User-entered description of the selected interface
show interfaces cos-queue	The class-of-service queue configuration for the specified interface
show port	The configuration and status of the specified interface or of all interfaces
show port-channel	The configuration and status of the specified LAG or of all LAGs

show logging

 **Note:** See the various versions of the **show logging** command in the Syslog chapter ([System Log on page 149](#)).

Related Commands

show logging	Displays a combination of the system log and event log (buffered log).
show logging buffered	Displays buffered logging (the System log)
show logging hosts	Displays configured logging hosts (syslog servers).
show logging traplogs	Displays trap summaries (number of traps since last reset and last view) and trap details.

show mac-addr-table

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

Syntax

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

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

Mode Privileged Exec

Example

```
(S50-TAC-8) #show mac-addr-table all
-----
      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 13 Example of Output from the show mac-addr-table all Command

Field Descriptions

Mac Address—A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system, the MAC address is displayed as 8 bytes.



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

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



Note: The “3/1” in the Interface column references the Ethernet Management port. See [Figure 13](#) and [Figure 15](#).

If Index—This object indicates the IfIndex of the interface table entry associated with this port.

In the S2410, If Index values are:

Headings	Explanation
Physical ports	1 through 24 (24 ports)
Ethernet Management port (labelled “10/100 Ethernet”, also called <i>service port</i>):	25
LAGs (port channels)	26 to 37 (12 possible LAGs)

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

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

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

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

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

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

Example 2

```
Force10 #show mac-addr-table count
Dynamic Address count..... 0
Static Address (User-defined) count..... 0
Total MAC Addresses in use..... 0
Total MAC Addresses available..... 16384
```

Figure 14 Example of Output from the show mac-addr-table count Command

Example 3

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

Figure 15 Example of Output from the show mac-addr-table vlan Command

Related Commands

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

show msglog

Command History

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

Related Commands

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

show network

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

show running-config

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

When a script name is provided, the output is redirected to a configuration script. The option **[all]** will also enable the display/capture of all commands with settings/configurations that include values that are the same as the default values. If the optional *<scriptname>* is provided with a file name extension of “.scr”, the output will be redirected to a script file.

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

Mode Privileged Exec

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

Example

```
(S50-TAC-5) #show running-config all
!Current Configuration:
!
hostname "S50-TAC-5"
no set gmrp adminmode
no set gvrp adminmode
telnetcon timeout 5
telnetcon maxsessions 5
ip telnet server enable
network protocol none
network parms 172.17.1.222 255.255.255.0 172.17.1.254
network mac-type burnedin
network mgmt_vlan 1
no network javamode
vlan database
set igmp groupmembership-interval 1 260
set igmp maxresponse 1 10
set igmp mcrtrexpiretime 1 0
```

Figure 16 Using the show running-config command



Note: This sample of the output is just a small part of the many thousands of lines generated when the **all** option is used.

Usage Information

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

Related Commands

script apply	Applies the commands in the designated script to the switch.
script delete	Deletes a specified script.
script list	Lists all scripts present on the switch as well as the total number of files present.
script show	Displays the contents of a designated script file.
script validate	Validates a designated configuration script file.

show serviceport

This command displays information about the management address of the Ethernet Management port.

Syntax **show serviceport**

Mode Privileged Exec

Command History

Version 2.4.1	Introduced
---------------	------------

Example

```
(Force10 S2410) #show serviceport
IP Address..... 10.11.197.177
Subnet Mask..... 255.255.0.0
Default Gateway..... 10.11.197.190
ServPort Configured Protocol Current..... None
Burned In MAC Address..... 00:01:E8:99:99:9A
Link Status..... Up
```

Figure 17 show serviceport Command Output**Table 11** Fields in Output of show serviceport command

Field	Description
IP Address	The IP address of the Ethernet Management port. The default value is 0.0.0.0
Subnet Mask	The IP subnet mask for the Ethernet Management port. The default value is 0.0.0.0
Default Gateway	The default gateway for the Ethernet Management port. The default value is 0.0.0.0.
ServPort Configured Protocol Current	Indicates if the IP configuration of the Ethernet Management port should be manually entered, or if it should be configured through DHCP or Bootp. The default value is none (manually configured).
Burned In MAC Address	The MAC address of the Ethernet Management port
Link Status	Ethernet Management port link up or down

Related Commands

serviceport ip	Configures the IP configuration of the Ethernet Management port.
serviceport protocol	Set the network configuration protocol to be used for configuring access to the Ethernet Management port.
show interface managementethernet	Displays the configuration of the management VLAN.

show sysinfo

This command displays switch information.

Syntax **show sysinfo**

Mode Privileged Exec

Table 12 Fields in Output of show sysinfo Command

Field	Description
Switch Description	Text used to identify this switch
System Name	Name used to identify the switch
System Location	Text used to identify the location of the switch. May be up to 31 alpha-numeric characters. The factory default is blank
System Contact	Text used to identify a contact person for this switch. May be up to 31 alpha-numeric characters. The factory default is blank
System ObjectID	The base object ID for the switch's enterprise MIB
System Up Time	The time in days, hours and minutes since the last switch reboot
MIBs Supported	A list of MIBs supported by this agent

show version

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

Syntax **show version**

Mode Privileged Exec

Table 13 Fields in Output of show version Command

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

Table 13 Fields in Output of show version Command (continued)

Headings	Explanation
Burned in MAC Address	Universally assigned network address
Software Version	The release.version.revision number of the code currently running on the switch
Additional Packages	This displays the additional packages that are incorporated into this system, such as SFTOS Multicast.
10/100 Ethernet/802.3 interface(s)	
Gig Ethernet/802.3 interface(s)	
10Gig Ethernet/802.3 interface(s)	
Virtual Ethernet/802.3 interface(s)	
System Name	
System Location	
System Contact	
System Object ID	
System Up Time	
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)

Table 13 Fields in Output of show version Command (continued)

Headings	Explanation
RFC 2863 - IF-MIB	The Interfaces Group MIB using SMIPv2
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
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X
F10OS-RADIUS-AUTH-CLIENT-MIB	F10OS Radius MIB
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB
RADIUS-AUTH-CLIENT-MIB	RADIUS Authentication Client 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
RFC 3289 - DIFFSERV-DSCP-TC	Management Information Base for the Textual Conventions used in DIFFSERV-MIB
RFC 3289 - DIFFSERV-MIB	Management Information Base for the Differentiated Services Architecture
F10OS-QOS-DIFFSERV-EXTENSIONS-MIB	F10OS Flex QOS DiffServ Private MIBs' definitions
F10OS-QOS-DIFFSERV-PRIVATE-MIB	F10OS Flex QOS DiffServ Private MIBs' definitions

Related Commands

show hardware	Inventory information for the switch
show sysinfo	Switch information

show tech-support

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

```

----- show version -----
[The output fields are displayed in “Fields in Output of show
version Command” on page 84.]
-----show hardware-----
    
```

Syntax **show tech-support**

Mode Privileged Exec

Related Commands	show hardware	Inventory information for the switch
	show logging	Trap log maintained by the switch, and event log, containing error messages from the system
	show port	Port information
	show running-config	Updated configuration maintained by the switch.
	show version	Details of the software/hardware present on the system

vlan participation (management)

This command assigns the management VLAN of the switch.

Syntax `[no] vlan participation vlan_id`

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

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

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

Command History	Version 2.3	Introduced: Replaces the network mgmt_vlan command.
------------------------	-------------	---

Related Commands	management route default	Sets the IP gateway of the switch.
	interface managementethernet	Invokes the Interface ManagementEthernet mode, the (Config-if-ma)# prompt.
	show interface	Displays a summary of statistics for a specific port, including the management port, or a count of all CPU traffic based upon the argument.

Telnet Commands

This section describes the following SFTOS Telnet commands:

- [ip telnet maxsessions on page 88](#)
- [ip telnet timeout on page 88](#)
- [session-limit on page 89](#)
- [session-timeout on page 89](#)
- [show telnet on page 90](#)
- [telnet on page 90](#)

- [telnetcon maxsessions on page 91](#)
- [telnetcon timeout on page 90](#)

ip telnet maxsessions

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

Syntax `ip telnet maxsessions 0-5`

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

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

Default 5

Mode Global Config

Command History

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

ip telnet timeout

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



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

Syntax `ip telnet timeout 1-160`

The time is a decimal value from 1 to 160.

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

Default 5 (minutes)

Mode Global Config

Command History	Version 2.3	Changed from telnetcon timeout and moved from Privileged Exec mode to Global Config.
------------------------	-------------	---

ip telnet server enable

Enable or disable Telnet services.

Syntax **[no] telnet server enable**

Mode Global Config

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

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

session-limit

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

Syntax **session-limit 0-5**

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

Default 5

Mode Line Config

session-timeout

This command sets the outbound Telnet session timeout value.

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

The timeout value unit of time is minutes.

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

Default 1 (minute)

Mode Line Config

show telnet

This command displays the current outbound telnet settings.

Syntax **show telnet**

Modes Privileged Exec and User Exec

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

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

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

telnet

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

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

Modes Privileged Exec and User Exec

telnetcon timeout

**Command
History**

Version 2.3 Modified: Changed to [ip telnet timeout](#).

telnetcon maxsessions

Command History

Version 2.3 Modified: Changed to [ip telnet maxsessions](#)

Serial Commands

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

- [lineconfig on page 91](#)
- [serial baudrate on page 91](#)
- [serial timeout on page 92](#)
- [show serial on page 92](#)

lineconfig

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

Syntax **lineconfig**

Mode Global Config

Usage Information Users executing this command enter the Line Config mode.

For details on modes, see [Chapter 3, Using the Command Line Interface, on page 39](#).

Example

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

Figure 18 lineconfig Command Example

Related Commands

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

serial baudrate

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

Syntax **serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}**

The **no serial baudrate** command sets the communication rate of the terminal interface to the 9600 default.

Default 9600

Mode Line Config

serial timeout

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

Syntax **serial timeout** *0-160*

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

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

Default 5

Mode Line Config

show serial

This command displays serial communication settings for the switch.

Syntax **show serial**

Mode Privileged Exec and User Exec

Example

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

Table 14 Fields of show serial Command Output

Field	Description
Serial Port Login Timeout (minutes)	Specifies the time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout
Baud Rate	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud (bps). The factory default is 9600
Character Size	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether hardware flow control is enabled or disabled. It is always disabled.
Stop Bits	The number of stop bits per character. The number of stop bits is always 1.
Parity	The parity method used on the serial port. The parity method is always None.

SNMP Management Commands

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

- [show snmpcommunity on page 95](#)
- [show snmptrap on page 95](#)
- [show trapflags on page 96](#)
- [snmp-server on page 97](#)
- [snmp-server community on page 97](#)
- [no snmp-server community on page 97](#)
- [snmp-server community ipaddr on page 98](#)
- [snmp-server community ipmask on page 98](#)
- [snmp-server community mode on page 98](#)
- [snmp-server community ro on page 99](#)
- [snmp-server community rw on page 99](#)
- [snmp-server enable traps bcaststorm on page 99](#)
- [snmp-server enable traps linkmode on page 100](#)
- [snmp-server enable traps multiusers on page 100](#)
- [snmp-server enable traps stpmode on page 101](#)
- [snmp-server enable trap violation on page 101](#)
- [snmp-server traps enable on page 101](#)
- [snmptrap on page 102](#)
- [snmptrap ipaddr on page 102](#)
- [snmptrap mode on page 102](#)
- [snmp trap link-status on page 103](#)
- [snmp trap link-status all on page 103](#)
- [snmptrap snmpversion on page 103](#)



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

In Global Config mode:

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

In Router OSPF Config mode:

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

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

show snmpcommunity

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

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

Syntax **show snmpcommunity**

Mode Privileged Exec

Table 15 Fields of show snmpcommunity Command Output

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

show snmptrap

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

Syntax **show snmptrap**

Mode Privileged Exec

Table 16 Fields of show snmptrap Command Report

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

show trapflags

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



Note: The DVMRP, OSPF, and PIM traps are not supported in the Layer 2 image.

Syntax `show trapflags`

Mode Privileged Exec

Table 17 Fields of show trapflags Command Report

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

snmp-server

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

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

Default None

Mode Global Config

snmp-server community

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



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

Syntax **snmp-server community** *name*

Default None

Mode Global Config

no snmp-server community

This command removes the specified community name from the SNMP community table.

Syntax **no snmp-server community** *name*

Mode Global Config

snmp-server community ipaddr

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

Syntax `snmp-server community ipaddr ipaddr name`

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

Default 0.0.0.0

Mode Global Config

snmp-server community ipmask

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

Syntax `snmp-server community ipmask ipmask name`

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

Default 0.0.0.0

Mode Global Config

snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case, the SNMP manager associated with this community cannot manage the switch until the

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

Syntax [no] **snmp-server community mode** *name*

Default Enable

Mode Global Config

snmp-server community ro

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

Syntax **snmp-server community ro** *name*

Mode Global Config

snmp-server community rw

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

Syntax **snmp-server community rw** *name*

Mode Global Config


snmp-server enable traps bcaststorm

This command enables the sending of Broadcast Storm traps.

Syntax [no] **snmp-server enable traps bcaststorm**

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

Default enabled

Mode	Global Config
Command History	Version 2.3 Introduced
	 Note: The CLI indicates successful execution of this command, and the show trapflags report shows successful execution of the command, but this trap is not currently supported.
Related Commands	storm-control broadcast Enable broadcast storm recovery mode. show storm-control Display switch configuration information.

snmp-server enable traps linkmode

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

Syntax **[no] snmp-server enable traps linkmode**

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

Default enabled

Mode Global Config

snmp-server enable traps multiusers

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

Syntax **[no] snmp-server enable traps multiusers**

The **no** version of this command disables Multiple User traps.

Default enabled

Mode Global Config

snmp-server enable traps stpmode

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

Syntax [no] **snmp-server enable traps stpmode**

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

Default enabled

Mode Global Config

snmp-server enable trap violation

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

Syntax [no] **snmp-server enable trap violation**

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

Default Disabled

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

Command History

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

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface	Identifies an interface and enters the Interface Config mode.

snmp-server traps enable

This command enables the Authentication traps.

Syntax [no] **snmp-server traps enable**

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

Default enabled

Mode Global Config

Command History

Version 2.3

Corrected from **snmp-server enable traps**

snmptrap

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

Syntax [no] **snmptrap** *name ipaddr*

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

Mode Global Config

snmptrap ipaddr

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



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

Syntax **snmptrap ipaddr** *name ipaddrold ipaddrnew*

Mode Global Config

snmptrap mode

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

Syntax [no] **snmptrap mode** *name ipaddr*

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

Mode Global Config

snmp trap link-status

This command enables link status traps by interface.

Syntax `[no] snmp trap link-status`

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



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

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

Command History

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

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
interface	Identifies an interface and enters the Interface Config mode.

snmp trap link-status all

This command enables link status traps for all interfaces.

Syntax `[no] snmp trap link-status all`

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



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

Mode Global Config

snmptrap snmpversion

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

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

Mode Global Config

System Configuration Commands

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

- [System Configuration Commands](#)
- [Virtual LAN \(VLAN\) Commands on page 120](#)
- [System Utility Commands on page 138](#)
- [Configuration Scripting on page 146](#)



Note: For Link Aggregation Group (LAG) (also called port channel) commands, see [Chapter 15, LAG/Port Channel Commands, on page 249](#).

User access commands are in [Chapter 8, User Account Commands, on page 157](#). A related chapter is [Security Commands on page 163](#).

Broadcast storm control commands are in the [Broadcast Storm Control Commands on page 199](#), in [Chapter 8, User Account Commands, on page 157](#).

System Configuration Commands

This section describes the following system configuration commands:

- [bridge aging-time on page 106](#)
- [configure on page 106](#)
- [enable on page 107](#)
- [interface on page 108](#)
- [interface range on page 108](#)
- [monitor session on page 112](#)
- [monitor session 1 mode on page 113](#)
- [no monitor on page 113](#)
- [no monitor session 1 on page 114](#)
- [show forwardingdb agetime on page 114](#)
- [show mac-address-table on page 114](#)

- [show mac-address-table multicast on page 115](#)
- [show mac-address-table stats on page 116](#)
- [show monitor session on page 116](#)
- [show port on page 117](#)
- [show port protocol on page 119](#)
- [shutdown \(Interface\) on page 119](#)
- [shutdown all on page 119](#)

MAC Database Commands

To configure and view information about the MAC databases, see the following commands in this section:

- [bridge aging-time on page 106](#)
- [show forwardingdb agetime on page 114](#)
- [show mac-address-table multicast on page 115](#)
- [show mac-address-table stats on page 116](#)

bridge aging-time

This command configures the forwarding database address aging timeout in seconds.

Syntax **bridge aging-time** *seconds*

The command **no bridge aging-time** sets the forwarding database address aging timeout to the default of 300 seconds.

Parameters	<i>seconds</i>	In place of <i>seconds</i> , enter a number between 10 and 1,000,000 to indicate the number of seconds before the timeout.
-------------------	----------------	--

Default 300

Mode Global Config

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

configure

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

Syntax	configure		
Command Modes	Privileged Exec		
Usage Information	Users executing this command enter the Global Config mode, which provides access to many commands within that mode. Also, this mode is a gateway to all other more protocol-specific modes except the VLAN mode. For details on modes, see Chapter 3, Using the Command Line Interface, on page 39 .		
Example	<pre>(S50) #configure (S50) (Config)#</pre>		
Related Commands	<table border="1"> <tr> <td>enable</td> <td>The enable command accesses the Privileged Exec mode.</td> </tr> </table>	enable	The enable command accesses the Privileged Exec mode.
enable	The enable command accesses the Privileged Exec mode.		

Figure 19 configure Command Example

enable

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



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

Syntax	enable
Defaults	none
Mode	User Exec
Usage Information	Users who execute this command enter the Privileged Exec mode, gaining access to the commands available in this mode, as well as being able to directly access the Global Config mode and the VLAN mode. After accessing the Global Config mode, users can access all modes to which the Global Config mode provides a gateway. To protect against unauthorized access, use the command enable passwd to configure a password for the command.
Example	<pre>(S50)>enable Password: (S50)#</pre>

Figure 20 enable Command Example

**Related
Commands**

enable passwd	Configure a password for the enable command.
configure	Use this command to access the Global Config mode from the Exec Privilege mode.

interface

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

Syntax **interface** *unit/slot/port*

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

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

Default None

Mode Global Config

**Related
Commands**

interface range	Groups a set of individual interfaces, a range of interfaces, or more than one range of interfaces, to which subsequent configuration commands can be applied (bulk configuration)
interface vlan	Creates a new VLAN and accesses the Interface VLAN mode for it, or selects an existing VLAN and accesses the Interface VLAN mode for it.

interface range

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

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

Parameters	ethernet <i>range,range,...</i>	Enter the keyword ethernet and one or more ports separated by hyphens and commas in this form: ethernet <i>unit/slot/port - port,unit/slot/port - port</i> . Spaces are not allowed around commas or hyphens. Example: ethernet 1/0/1-1/0/10,1/0/40-1/0/45
	port-channel <i>range,range,...</i>	Enter the keyword port-channel and one or more port channel numbers separated by commas or grouped in a range in this form: port-channel 0/1/1-0/1/4 Spaces are not allowed around commas or hyphens. You can enter up to six comma-separated ranges.
	vlan <i>range,range,</i> ...	Enter the keyword vlan and one or more VLAN numbers, from 1 to 3965, separated by commas or grouped in a range in this form: vlan 10,33-50 Spaces are not allowed around commas or hyphens. You can enter up to six comma-separated ranges.

Defaults This command has no default behavior or values.

Mode Global Config

Command History	Version 2.3	Introduced
------------------------	-------------	------------

Usage Information When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical). Important things to remember:

- Bulk configuration is created if at least one interface is valid.
- Automatically excludes non-existing interfaces from the bulk configuration and generates a warning message (Figure 22).
- The resulting interface range prompt includes interface types with slot/port information for valid interfaces, for example: (conf-if-range-et-1/0/10-1/0/11)#. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- If the interface range prompt has multiple port ranges, the smaller port range is excluded from the prompt (Figure 22).
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port (Figure 23).

Executing the **interface range** command puts you in the Interface Range mode, more specifically, in one of three versions of it—*Ethernet Range*, *Port Channel Range*, or *VLAN Range*. Here, you can execute commands that modify the selected set of interfaces. These commands have the same effect as they do when they are used within the Interface VLAN or Interface Config modes (see [interface on page 108](#), [LAG/Port Channel Commands on page 249](#), and [interface vlan on page 123](#)).

The command families available from the Ethernet Range prompt are displayed in the following CLI example (Figure 21 on page 110). The commands available from the VLAN

Range and Port Channel Range prompts within that mode are displayed in the Link Aggregation chapter (LAGs) in the *SFTOS Command Reference*.

Example

```
(s50-1) (conf-if-range-et-1/0/10-1/0/11)#?
addport                Add this port to a port-channel.
auto-negotiate         Enables/Disables automatic negotiation on a port.
classofservice         Configure Class of Service parameters.
cos-queue              Configure the Cos Queue Parameters.
deleteport            Delete this port from a port-channel.
description            Add Description to the interface
dot1x                  Configure Dot1x interface commands.
exit                   To exit from the mode.
gmrp                   Set GARP Multicast Registration Protocol parameters.
gvrp                   Set GARP VLAN Registration Protocol parameters.
igmp                   Enable/Disable IGMP Snooping on a selected interface
ip                     Configure IP parameters.
mac                    Configure MAC Access List group parameters.
mode                   Configure the double VLAN tunnel mode for this interface.
mtu                    Sets the default MTU size.
port                   Configure a physical port.
port-channel           Enable/Disable the port-channel's administrative mode.
port-security          Enable/Disable Port MAC Locking/Security for interface.
protocol               Configure the Protocol Based VLAN parameters.
service-policy         Configure DiffServ Service.
--More-- or (q)uit
set                    Configure switch options and settings.
shutdown              Enable/Disable a port.
snmp                   Configure SNMP options.
snmp-server            Enable/Disable SNMP violation traps interface.
spanning-tree         Set the spanning tree operational mode.
speed                  Sets the speed and duplex setting for the interface.
traffic-shape          Configure the maximum transmission bandwidth limit.
vlan                   Configure VLAN parameters.

(s50-1) (conf-if-range-et-1/0/10-1/0/11)#mode ?
dvlan-tunnel           Configure double VLAN tunneling for a specific port.
dot1q-tunnel           Configure double VLAN tunneling for a specific port.

(s50-1) (conf-if-range-et-1/0/10-1/0/11)#mode dvlan-tunnel ?
<cr>                  Press Enter to execute the command.

(s50-1) (conf-if-range-et-1/0/10-1/0/11)#mode dvlan-tunnel
(s50-1) (conf-if-range-et-1/0/10-1/0/11)#vlan ?
acceptframe            Configure how to handle tagged/untagged frames
                      received.
ingressfilter          Enable/Disable application of Ingress Filtering Rules.
participation          Configure how ports participate in a specific VLAN.
priority               Configure the priority for untagged frames.
pvid                   Configure the VLAN id for a specific port.
tagging                Configure tagging for a specific VLAN port.
untagging              Configure untagging for a specific VLAN port.
```

Figure 21 Commands Available in Ethernet Range Mode

SFTOS, in contrast to FTOS, does not allow spaces around commas or hyphens in the range statement. The following example shows an incorrect range statement, followed by the associated error message.

Example

```
Forcel0(config)#interface range vlan 10 - 20
% Warning: Non-existing ports (not configured) are ignored by
interface-range
(conf-if-range-vlan 10-20)#
```

Figure 22 Bulk Configuration Warning Message

[Figure 23](#) is an example of a correctly formatted single range bulk configuration.

Example

```
Forcel0(config)#interface range ethernet 5/0/1-5/0/23
Forcel0(config-if-range)#no shutdown
Forcel0(config-if-range)#
```

Figure 23 Single Range Bulk Configuration

[Figure 24](#) shows how to use commas to add different interface types to the range enabling all Gigabit Ethernet interfaces in the range 5/1 to 5/23 and both 10-Gigabit Ethernet interfaces 1/0/49 and 1/0/50.

Example

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

Figure 24 Multiple Range Bulk Configuration for Gigabit Ethernet

Use the [show running-config](#) command to view the VLAN and port channel interfaces. VLAN or port channel interfaces that are not displayed in the [show running-config](#) command cannot be used with the bulk configuration feature of the **interface range** command. Note that you can only modify, not create, virtual interfaces (ethernet, port channel, VLAN) using the **interface range** command.



Note: If a range has VLAN, physical, and port channel interfaces, only commands related to physical interfaces can be bulk-configured. To configure commands specific to VLAN or port channel, only those respective interfaces should be configured in a particular range.

Related Commands

interface	Accesses the Interface Config mode for a designated logical or physical interface.
interface vlan	Creates a new VLAN and accesses the Interface VLAN mode for it, or selects an existing VLAN and accesses the Interface VLAN mode for it.
port-channel	

monitor session

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

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

Parameters	destination interface <i>unit/slot/port</i>	Specify the probe port (target port). The probe port can be a VLAN member only if you first add the port to a VLAN and then configure it as a probe port.
	source interface <i>unit/slot/port</i>	Specify the source interface (mirrored port). The port can be a part of any VLAN.
	mode	Enable/disable the port mirroring session. See monitor session 1 mode on page 113 .

To remove the destination port, use **no monitor session 1 destination interface**.

To remove a source port, use **no monitor session 1 source interface *unit/slot/port***.

In other words, removing the source interface requires specifying the port to be removed, but removing the destination port does not require specifying the destination port, since there can be only one destination port.

Default None

Mode Global Config

Usage Information Note the restrictions described above on using mirrored and probe ports in VLANs. Furthermore, if either port is in a VLAN, then the other port must also be in the same VLAN.

Remove an existing source or destination port before replacing it with another. For more on configuring port monitoring (port mirroring), see the Port Mirroring chapter of the *SFTOS Configuration Guide*.

Related Commands	monitor session 1 mode	Sets the monitor session (port monitoring) mode to enabled.
	no monitor	Removes the destination port and all source ports from the mirroring configuration.
	show monitor session	Shows the mirroring configuration.

monitor session 1 mode

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

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

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

Syntax `[no] monitor session 1 mode`

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

Default disabled

Mode Global Config

**Related
Commands**

monitor session	Adds a mirrored port (source port) or mirroring port (destination port) to a session identified with the session ID of 1.
no monitor	Removes the destination port and all source ports from the mirroring configuration.
show monitor session	Shows the mirroring configuration.

no monitor

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

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

Default enabled

Syntax `no monitor`

Mode Global Config

no monitor session 1

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

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

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

Syntax	no monitor session 1
Default	enabled
Mode	Global Config

show forwardingdb agetime

This command displays the timeout for address aging.

Syntax	show forwardingdb agetime
Mode	Privileged Exec

Example

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

Figure 25 Example of show forwardingdb agetime Command Output

Command History

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

show mac-address-table

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

Syntax	show mac-address-table { gmrp igmpsnooping multicast stats }
	gmrp —Display GMRP entries in the MFDB table.

igmpsnooping—Display IGMP Snooping entries in the MFDB table.

multicast—Display Multicast Forwarding Database Table information.

stats—Display MFDB statistics.

Mode Privileged Exec

Field Descriptions Total Entries—This displays the total number of entries that can possibly be in the Multicast Forwarding Database table.

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

Current Entries—This displays the current number of entries in the Multicast Forwarding Database table.

Related Commands

show mac-address-table multicast	Displays Multicast Forwarding Database (MFDB) information
show mac-address-table stats	Displays Multicast Forwarding Database (MFDB) statistics
show mac-address-table gmrp	Displays GARP Multicast Registration Protocol (GMRP) entries in the MFDB table
show mac-address-table igmpsnooping	Displays IGMP Snooping entries in the MFDB table
show mac-addr-table	Displays forwarding database entries

show mac-address-table multicast

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

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

For 1-3965, you have the option of entering a valid VLAN ID.

Mode Privileged Exec

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

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

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

Description—The text description of this multicast table entry.

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

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

**Related
Commands**

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

show mac-address-table stats

This command displays Multicast Forwarding Database (MFDB) statistics.

Syntax **show mac-address-table stats**

Mode Privileged Exec

Report Fields:

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

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

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

Example

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

Figure 26 Command Example: show mac-address-table stats

**Related
Commands**

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

show monitor session

This command displays the port monitoring information for the system.

Syntax **show monitor session 1**

Mode Privileged Exec

Example

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

Figure 27 Command Example: show monitor session 1

Field Descriptions

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

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

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

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

Related Commands

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

show port

This command displays port information for a selected port or for all ports. The Port Summary panel of the Web User Interface displays the same information.

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

Mode Privileged Exec

Command History

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

Example

```

Forcel0 S2410 #show port all
Interface   Type      Admin   Physical   Physical   Link   Link   LACP   Flow
-----   -
0/1         PC Mbr    Enable  10G Full   10G Full   Down  Enable Enable Disable
0/2         PC Mbr    Enable  10G Full   10G Full   Down  Enable Enable Disable
0/3         PC Mbr    Enable  10G Full   10G Full   Down  Enable Enable Disable
0/4         PC Mbr    Enable  10G Full   10G Full   Down  Enable Enable Disable
0/5         PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/6         PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/7         PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/8         PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/9         PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/10        PC Mbr    Enable  10G Full   10G Full   Down  Enable Enable Disable
0/11        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/12        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/13        PC Mbr    Disable 10G Full   10G Full   Down  Enable Enable Disable
0/14        PC Mbr    Enable  10G Full   10G Full   Down  Enable Enable Disable
0/15        PC Mbr    Enable  10G Full   10G Full   Down  Enable Enable Disable
0/16        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/17        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/18        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/19        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/20        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/21        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/22        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/23        PC Mbr    Enable  10G Full   10G Full   Up     Enable Enable Disable
0/24        PC Mbr    Disable 10G Full   10G Full   Down  Enable Enable Disable
1/1         LAG       Enable  N/A       N/A       Up     Enable N/A     Enable
1/2         LAG       Enable  N/A       N/A       Up     Enable N/A     Enable
Forcel0 S2410 #

```

Figure 28 show port all Command Output Example

Interface—Valid unit, slot and port number separated by forward slashes.. This field only displays in the **show port all** report.



Note: Port IDs 1/1 and 1/2 in [Figure 28](#) are LAGs.

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

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

PC Mbr—Indicates a member of a LAG (port channel).

Probe—Indicates a probe port.

Admin Mode—The port administration state. The port must be enabled in order for it to be allowed into the network. It is either enabled or disabled. The default is enabled.

Physical Mode—The desired port speed and duplex mode. In the S2410, all ports are set to auto-negotiate speed and duplex mode.

Physical Status—Indicates the port speed and duplex mode.

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

Link Trap—Indicates whether or not to send a trap when link status changes. The default is enabled.

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

Flow Mode—Displays whether flow control is enabled or disabled.

show port protocol

This command displays the protocol-based VLAN information for either the entire system, or for the indicated group.

Syntax `show port protocol groupid`

Mode Privileged Exec

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

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

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

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

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

shutdown (Interface)

This command disables a port.

The **no** version of this command enables a port.

Syntax `[no] shutdown`

Default enabled

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

Command History	Version 2.3	Added Interface Range mode.
	interface range	Defines an interface range and accesses the Interface Range mode
Related Commands	interface	Identifies an interface and enters the Interface Config mode.

shutdown all

This command disables all ports.

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

Syntax [no] shutdown all

Default enabled

Mode Global Config

Virtual LAN (VLAN) Commands

In SFTOS 2.4.1, the **interface vlan** command is the starting point for VLAN configuration. Executing the command creates a new VLAN and invokes the Interface VLAN mode, where all VLAN configuration commands reside for the specified VLAN. You execute this **interface vlan** command (see [interface vlan on page 123](#)) from the Global Config mode.

Table 18 Commands in the Interface VLAN Mode

Commands	Command/Command Family Description	Location of Command Syntax Description
description	Add a description to the VLAN.	This chapter
encapsulation (VLAN)	Configure interface link layer encapsulation type.	This chapter
exit	Leave the mode.	
help	Display help for various special keys.	
igmp	Configure IGMP Snooping parameters for the VLAN.	IGMP Snooping Commands on page 235
ip	Configure IP parameters.	
makestatic	Change the VLAN type from Dynamic to Static.	This chapter
mtu (VLAN)	Set the default MTU size.	This chapter
name (VLAN)	Configure an optional VLAN name.	This chapter
protocol	Configure the protocols associated with particular group IDs.	This chapter
tagged/untagged	Configure tagging for a specific VLAN port.	This chapter

Virtual LAN (VLAN) commands in this section are:

- [clear vlan on page 121](#)
- [description on page 122](#)
- [encapsulation \(VLAN\) on page 123](#)
- [interface vlan on page 123](#)
- [makestatic on page 124](#)
- [mtu \(VLAN\) on page 125](#)
- [name \(VLAN\) on page 125](#)
- [network mgmt_vlan on page 126](#)

- [participation \(VLAN\) on page 126](#)
- [priority \(VLAN\) on page 126](#)
- [protocol group on page 127](#)
- [protocol vlan group on page 127](#)
- [protocol vlan group all on page 128](#)
- [pvid \(VLAN\) on page 128](#)
- [show vlan on page 129](#)
- [show vlan port on page 130](#)
- [tagged on page 131](#)
- [untagged on page 132](#)
- [vlan on page 132](#)
- [vlan acceptframe on page 133](#)
- [vlan database on page 133](#)
- [vlan ingressfilter on page 133](#)
- [vlan participation \(interface\) on page 133](#)
- [vlan participation all on page 134](#)
- [vlan port acceptframe on page 134](#)
- [vlan port ingressfilter all on page 134](#)
- [vlan port pvid all on page 134](#)
- [vlan port tagging all on page 135](#)
- [vlan protocol group on page 136](#)
- [vlan protocol group add protocol on page 136](#)
- [vlan protocol group remove on page 136](#)
- [vlan pvid on page 137](#)
- [vlan tagging on page 137](#)



Note: For information on commands related to the management VLAN, see [General System Management and Information Commands on page 55](#) (most specifically, [interface managementethernet on page 58](#)) in the Management chapter.

For general instructions on configuring the management VLAN, see the Management chapter in the *SFTOS Configuration Guide*.

For other VLAN information in the *SFTOS Configuration Guide*, see the Creating VLANS section of the Getting Started chapter, the chapters on the Web UI, STP, IEEE 802.1Q VLANs, VLAN-Stack commands, GARP and GVRP, IGMP Snooping.

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Syntax **clear vlan**

Default disabled

Mode	Privileged Exec	
Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports

description

Enter a description for the selected interface (port or VLAN).

Syntax	[no] description <i>description</i>
	The <i>description</i> allows spaces if you surround the statement with single or double quotes.
Default	none
Mode	Interface VLAN, Interface Config
Command History	Version 2.3 Introduced
Usage Information	The following example shows the use of both single quotes and double quotes in entering a description for a port. The example also shows the resulting descriptions presented in show interfaces description commands.

Example

```
S50 #conf
S50 (Config)#interface 1/0/1
S50 (Interface 1/0/1)#description "1/0/1 is access port"
S50 (Interface 1/0/1)#exit
S50 (Config)#interface 1/0/30
S50 (Interface 1/0/30)#description 'management port in vlan 30'
S50 (Interface 1/0/30)#exit
S50 (Config)#exit
S50 #show interfaces description 1/0/1
Interface.....1/0/1
IfIndex.....1
Description....1/0/1 is access port
MAC Address....00:01:E8:D5:BA:C0
Bit Offset Val..1

S50 #show interfaces description 1/0/30
Interface.....1/0/30
IfIndex.....30
Description....management port in vlan 30
MAC Address....00:01:E8:D5:BA:C0
Bit Offset Val..30

S50 #
```

Figure 29 show interfaces description Command Example

Related Commands	interface vlan	Creates a VLAN, assigns it an ID and then enters the Interface VLAN mode
-------------------------	--------------------------------	--

show interfaces	Displays information, including the description, about a selected interface.
show running-config	Display/capture the current setting of different protocol packages supported on the switch.

encapsulation (VLAN)

This command configures the link layer encapsulation type for the packet within the VLAN. Acceptable encapsulation types are Ethernet and SNAP.

Syntax	encapsulation { ethernet snap }		
Default	ethernet		
Mode	Interface VLAN Restrictions—Routed frames are always Ethernet-encapsulated when a frame is routed to a VLAN.		
Command History	<table border="1"> <tr> <td>Version 2.3</td> <td>Introduced</td> </tr> </table>	Version 2.3	Introduced
Version 2.3	Introduced		
Related Commands	<table border="1"> <tr> <td>interface vlan</td> <td>Creates a VLAN, assigns it an ID and then enters the Interface VLAN mode</td> </tr> </table>	interface vlan	Creates a VLAN, assigns it an ID and then enters the Interface VLAN mode
interface vlan	Creates a VLAN, assigns it an ID and then enters the Interface VLAN mode		

interface vlan

This command creates a new VLAN if the identified VLAN ID does not already exist, or else the command selects an existing VLAN. Then, in either case, the command invokes the Interface VLAN mode, in which you have access to VLAN configuration commands for the specified VLAN.

Syntax	interface vlan <i>vlanid</i>		
	The <i>vlanid</i> is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 2-3965. The no version of this command deletes an existing VLAN.		
Default	None		
Mode	Global Config		
Command History	<table border="1"> <tr> <td>Version 2.3</td> <td>Introduced. Replaces vlan database and vlan commands.</td> </tr> </table>	Version 2.3	Introduced. Replaces vlan database and vlan commands.
Version 2.3	Introduced. Replaces vlan database and vlan commands.		

Usage Information

After using this command to access the Interface VLAN mode (the prompt for the Interface VLAN mode is `(conf-if-vl-<vlan-id>#)`), you can configure the selected VLAN.

You can also make configuration changes to a VLAN in the Interface Range mode (see [interface range on page 108](#)) and the Interface Config mode (see [interface on page 108](#)). For details on modes, see [Chapter 3, Using the Command Line Interface, on page 39](#).

Example

```

Forcel0 #config
Forcel0 (Config)#interface vlan 5
Forcel0 (Conf-if-vl-5)#?

description          Add Description to the interface
encapsulation        Configure interface link layer encapsulation type.
exit                 To exit from the mode.
help                 Display help for various special keys.
igmp                 Configure IGMP Snooping parameters for the Vlan
ip                   Configure IP parameters.
mtu                  Sets the default MTU size.
protocol              Configure the Protocols associated with particular
                    Group Ids.
makestatic            Change the VLAN type from 'Dynamic' to 'Static'.
name                 Configure an optional VLAN Name.
participation         Configure how ports participate in a specific VLAN.
priority              Configure the priority for untagged frames.
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.

Forcel0 (Conf-if-vl-5)#exit
Forcel0 (Config)#exit
Forcel0 #show vlan brief
VLAN ID  VLAN Name          MAC Aging      IP Address
-----  -
1         Default                 300            unassigned
5                                 300            unassigned

Forcel0#
    
```

Figure 30 Using the interface vlan Command

Related Commands

interface	Accesses the Interface Config mode for a designated logical or physical interface.
interface range	Groups a set of individual interfaces, a range of interfaces, or more than one range of interfaces, to which subsequent configuration commands can be applied (bulk configuration)
show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
show port	Displays port information for a selected port or for all ports

makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-3965.

Syntax **makestatic 2-3965**

Mode	Interface VLAN	
Command History	Version 2.3	Changed from vlan makestatic to makestatic and moved to Interface VLAN mode.
Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports

mtu (VLAN)

This command sets the MTU (Maximum Transmission Unit) of the selected VLAN.

Syntax	[no] mtu <i>576-1500</i>	
Default	1500	
Mode	Interface VLAN	
Command History	Version 2.3	Introduced
Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports

name (VLAN)

This command changes the name of a VLAN.

Syntax **[no] name** *newname*

The *newname* is an alphanumeric string of up to 32 characters.

The **no** version of this command sets the name of a VLAN to a blank string.

Default The name for VLAN ID 1 is always Default. The name for other VLANs is defaulted to a blank string.

Mode Interface VLAN

Command History

Version 2.3	Modified: Changed from vlan name to name and mode changed from VLAN database to Interface VLAN. Removed ID range variable.
-------------	--

Related Commands

show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
show port	Displays port information for a selected port or for all ports

network mgmt_vlan

Command History

Version 2.3	Deprecated: The functionality is available in the vlan participation command.
-------------	--

Related Commands

interface managementethernet	Invokes ManagementEthernet mode (the (Config-if-ma)# prompt), at which the user can set the network parameters of the switch, including using the vlan participation command.
vlan participation (management)	Assigns the management VLAN.

participation (VLAN)

Configure how ports participate in a specific VLAN.

Mode Interface VLAN

Command History

Version 2.3	Introduced but deprecated in favor of the tagged command
-------------	---

Related Commands

tagged	Sets tagging to enabled for a specific interface in the selected VLAN.
------------------------	--

priority (VLAN)

Configure the priority for untagged frames.

Mode Interface VLAN

Command History

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

Related Commands

tagged	Sets tagging to enabled for a specific interface in the selected VLAN.
------------------------	--

protocol group

This command attaches a group ID to the selected VLAN. A group can only be associated with one VLAN at a time. However, the VLAN association can be changed. The referenced VLAN should be created prior to the creation of the protocol-based VLAN, except when GVRP is expected to create the VLAN.

Syntax `[no] protocol group groupid`

The **no** version of this command removes the group ID from this VLAN.

Default None

Mode Interface VLAN

Command History

Version 2.3	Modified: Removed <i>vlanid</i> parameter and changed mode from VLAN database to Interface VLAN.
-------------	--

Related Commands

interface vlan	Configure a VLAN and enter Interface VLAN mode.
show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
show port	Displays port information for a selected port or for all ports

protocol vlan group

This command adds the physical *unit/slot/port* interface to the protocol-based VLAN identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

The **no** version of this command removes the interface from this protocol-based VLAN group that is identified by this *groupid*.

Syntax `[no] protocol vlan group groupid`

Default None

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

Command History	Version 2.3	Added Interface Range mode.
	interface range	Defines an interface range and accesses the Interface Range mode
Related Commands		

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by *groupid*. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

The **no** version of this command removes all interfaces from this protocol-based VLAN group that is identified by this *groupid*.

Syntax	[no] protocol vlan group all <i>groupid</i>
Default	None
Mode	Global Config

pvid (VLAN)

Configure the VLAN ID for a specific port.

Mode	Interface VLAN	
Command History	Version 2.3	Introduced but deprecated in favor of the tagged command
Related Commands	untagged	Sets tagging to disabled for a specific port (or range of ports) in the selected VLAN.

show vlan

This command displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs. The ID is a valid VLAN identification number.

Syntax `show vlan [brief | id vlanid | name | port]`

Parameters	brief	(OPTIONAL) Enter the keyword brief to display summary information for all configured VLANs.
	id <i>vlanid</i>	(OPTIONAL) Enter the keyword id followed, in place of <i>vlanid</i> , by the desired VLAN number to display detailed information for the selected VLAN. Range: 1 to 3965
	name	(OPTIONAL) Enter the keyword name to display the names of configured VLANs.

Mode Privileged Exec and User Exec

Command History
Version 2.3 Modified: Changed parameters to include **show vlan brief**.

Usage Information For the **show vlan** command, without parameters, the output is shown in [Figure 31](#).

Example

```

Forcel0#show vlan
Codes: * - Default VLAN, G - GVRP VLANs, E - Ethernet interface

Vlan Id  Status      Q  Ports
-----
* 1      Inactive    U  E  1/0/1 ,1/0/2 ,1/0/3 ,1/0/4 ,1/0/5 ,1/0/6 ,1/0/7
    1/0/8 ,1/0/9 ,1/0/10,1/0/11,1/0/12,1/0/13,1/0/14
    1/0/15,1/0/16,1/0/17,1/0/18,1/0/19,1/0/20,1/0/21
    1/0/22,1/0/23,1/0/24,1/0/25,1/0/26,1/0/27,1/0/28
    1/0/29,1/0/30,1/0/31,1/0/32,1/0/33,1/0/34,1/0/35
    1/0/36,1/0/37,1/0/38,1/0/39,1/0/40,1/0/41,1/0/42
    1/0/43,1/0/44,1/0/45,1/0/46,1/0/47,1/0/48,1/0/49
    1/0/50,2/0/1 ,2/0/2 ,2/0/3 ,2/0/4 ,2/0/5 ,2/0/6
    2/0/7 ,2/0/8 ,2/0/9 ,2/0/10,2/0/11,2/0/12,2/0/13
    2/0/14,2/0/15,2/0/16,2/0/17,2/0/18,2/0/19,2/0/20
    2/0/21,2/0/22,2/0/23,2/0/24,2/0/25,2/0/26,2/0/27
    2/0/28,2/0/29,2/0/30,2/0/31,2/0/32,2/0/33,2/0/34
    2/0/35,2/0/36,2/0/37,2/0/38,2/0/39,2/0/40,2/0/41
    2/0/42,2/0/43,2/0/44,2/0/45,2/0/46,2/0/47,2/0/48
    2/0/49,2/0/50,3/0/1 ,3/0/2 ,3/0/3 ,3/0/4 ,3/0/5
    3/0/6 ,3/0/7 ,3/0/8 ,3/0/9 ,3/0/10,3/0/11,3/0/12
    3/0/13,3/0/14,3/0/15,3/0/16,3/0/17,3/0/18,3/0/19
    3/0/20,3/0/21,3/0/22,3/0/23,3/0/24,3/0/25,3/0/26

--More-- or (q)uit
--!output deleted!--

```

Figure 31 Output of the show vlan Command

Description of the fields in the **show vlan** report:

Vlan Id: VLAN ID

Status: Active or Inactive. A VLAN is active only if the VLAN contains interfaces and those interfaces are operationally up.

Q: "T" indicates that the port is tagged; "U" indicates untagged.

Ports: "E" for Ethernet, followed by the port numbers (unit/slot/port) in the VLAN

The output of the **show vlan brief** command is shown in the following example:

Example

```

Forcel0#show vlan brief
VLAN      Name      MAC Aging      IP Address
-----
1         abc       1800           unassigned
2         egf       1800           unassigned
3         sss       1800           unassigned
5                  1800           unassigned
12                 1800           unassigned
13                 1800           unassigned
    
```

Figure 32 Output of the show vlan brief Command

Description of the fields in the **show vlan brief** report:

VLAN: VLAN ID

Name: Assigned VLAN name

MAC Aging: Displayed in seconds

IP Address: IP Address assigned to the VLAN

Usage Information

For the **show vlan id *vlan-id*** command, the output is shown in the following example:

Example

```

Forcel0#show vlan id 1
Codes: * - Default VLAN, G - GVRP VLANs
      NUM      Status      Q Ports
*    1        Inactive      U Gi 0/8,11
    
```

Figure 33 Output of the show vlan id Command

Description of the fields in the **show vlan id** report:

NUM: VLAN ID

Status: A VLAN is active only if the VLAN contains interfaces and those interfaces are operationally up.

Q: (T) tagged or (U) untagged information

Ports: Speed - whether it is 10G, 1G or fast Ethernet interface and port number (unit/slot/port)

show vlan port

Display 802.1Q port parameters.

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

Parameters	<i>unit/slot/port</i>	Enter interface in unit/slot/port format for retrieving information about the associated interface.
	all	Enter all for retrieving information about all interfaces.

Mode Privileged Exec

Command History
Version 2.1 Introduced

Example

```

Forcel0-S50 #show vlan port 1/0/1
      Port      Acceptable  Ingress      Default
Interface VLAN ID Frame Types Filtering      GVRP      Priority
-----
1/0/1      1      Admit All    Enable      Disable      0

Protected Port ..... False

Forcel0-S50 #show vlan port all
      Port      Acceptable  Ingress      Default
Interface VLAN ID Frame Types Filtering      GVRP      Priority
-----
1/0/1      1      Admit All    Enable      Disable      0
1/0/2      1      Admit All    Enable      Disable      0
1/0/3      1      Admit All    Enable      Disable      0
1/0/4      1      Admit All    Enable      Disable      0
1/0/5      1      Admit All    Enable      Disable      0
1/0/6      1      Admit All    Enable      Disable      0
1/0/7      1      Admit All    Enable      Disable      0
1/0/8      1      Admit All    Enable      Disable      0
1/0/9      1      Admit All    Enable      Disable      0
1/0/10     1      Admit All    Enable      Disable      0
1/0/11     1      Admit All    Enable      Disable      0

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

```

Figure 34 Output of the show vlan port Command

tagged

This command sets tagging to enabled for a specific port (or range of ports) in the selected VLAN. If tagging is enabled, traffic is transmitted as tagged frames.

Syntax **tagged** *unit/slot/port*

The *unit/slot/port* is a valid interface belonging to the VLAN.

To remove tagging from the interface, use the **no tagged** command (not **untagged**). If tagging is disabled, traffic is transmitted as untagged frames.

Mode Interface VLAN

Command History
Version 2.3 Introduced

Usage Information The **tagged** command includes the functionality of the **participation include** command and the **acceptframe vlanOnly** command. For details, see the VLAN chapter in the *SFTOS Configuration Guide*.

Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports
	interface vlan	Creates a VLAN or selects an already-created VLAN.

untagged

This command adds a Layer 2 interface to the selected VLAN as an untagged interface.

Syntax `[no] untagged unit/slot/port`

The *unit/slot/port* is a valid interface belonging to the VLAN.

To remove an untagged interface from a VLAN, use the **no untagged unit/slot/port** command.

Mode Interface VLAN

Command History	Version 2.3	Introduced
------------------------	-------------	------------

Usage Information The **untagged** command includes the functionality of these commands: **participation include**, **pvid**, and **acceptframe untagged**. For details, see the VLAN chapter in the *SFTOS Configuration Guide*.

Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports
	tagged	Sets tagging to enabled for a specified interface in the selected VLAN.

vlan

Command History	Version 2.3	Modified: Replaced by interface vlan .
------------------------	-------------	--

vlan acceptframe

This command sets the frame acceptance mode per interface.

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Deprecated
Related Commands	tagged	Adds the designated interface to the selected VLAN as a tagged interface.
	untagged	Adds the designated interface to the selected VLAN as an untagged interface.

vlan database

Command History	Version 2.3	Modified: Replaced by interface vlan .
------------------------	-------------	--

vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Command History	Version 2.3	Deprecated
Related Commands	tagged	Adds the designated interface to the selected VLAN as a tagged interface.
	untagged	Adds the designated interface to the selected VLAN as an untagged interface.

vlan participation (interface)

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

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

vlan participation all

Command History

Version 2.3	Deprecated
-------------	------------

Related Commands

vlan participation (management)	In the Interface ManagementEthernet mode, this command assigns the management VLAN of the switch.
---	---

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number .

Mode Global Config

Command History

Version 2.3	Deprecated
-------------	------------

Related Commands

tagged	Configure a tagged interface in the selected VLAN.
untagged	Configure an untagged interface in the selected VLAN.

vlan port acceptframe

This command sets the frame acceptance mode for all interfaces.

Mode Global Config

Command History

Version 2.3	Deprecated
-------------	------------

vlan port ingressfilter all

This command enables ingress filtering for all ports.

Mode Global Config

Command History

Version 2.3	Deprecated
-------------	------------

vlan port pvid all

This command changes the VLAN ID for all interfaces.

Mode	Global Config	
Command History	Version 2.3	Deprecated
Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports

vlan port tagging all

This command sets the tagging behavior for all interfaces in a VLAN to enabled.

Command History	Version 2.3	Deprecated
Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports
	tagged	Add a tagged port to the selected VLAN.

vlan port untagging all

This command sets the tagging behavior for all interfaces in a VLAN to disabled so that traffic is transmitted as untagged frames.

Mode	Global Config	
Command History	Version 2.3	Deprecated
Related Commands	show vlan	Displays information about VLANs, either detailed information for a specific VLAN or summary information for all configured VLANs.
	show port	Displays port information for a selected port or for all ports.
	untagged	Adds a Layer 2 interface to the selected VLAN as an untagged interface.

vlan protocol group

This command adds a protocol-based VLAN group to the system. The *groupname* is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Syntax `vlan protocol group groupname`

Mode Global Config

vlan protocol group add protocol

This command adds the *protocol* to the protocol-based VLAN identified by *groupid*. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command will fail and the protocol will not be added to the group. The possible values for protocol are ip, arp, and ipx.

The **no** version of this command removes the *protocol* from this protocol-based VLAN group that is identified by this *groupid*. The possible values for protocol are **ip**, **arp**, and **ipx**.

Syntax `[no] vlan protocol group add protocol groupid protocol`

Default None

Mode Global Config

vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this *groupid*.

Syntax `vlan protocol group remove groupid`

Mode Global Config

vlan pvid

This command changes the VLAN ID per interface.

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Deprecated
Related Commands	tagged	Adds the designated interface to the selected VLAN as a tagged interface.
	untagged	Adds the designated interface to the selected VLAN as an untagged interface.

vlan tagging

This command sets tagging to enabled for the selected interface in a specified VLAN. If tagging is enabled, traffic is transmitted as tagged frames.

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Deprecated
Related Commands	tagged	Sets tagging to enabled for a specified interface in the selected VLAN.
	untagged	Adds a Layer 2 interface to the selected VLAN as an untagged interface.

vlan untagging

This command sets tagging to disabled for the selected interface in a specified VLAN.

Mode	Interface Config	
Command History	Version 2.3	Deprecated
Related Commands	untagged	Adds a Layer 2 interface to the selected VLAN as an untagged interface.

System Utility Commands

This section describes system utilities. The commands are divided into two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

System utility commands in this section are:

- [clear config on page 138](#)
- [clear counters on page 138](#)
- [clear igmpsnooping on page 139](#)
- [clear port-channel on page 139](#)
- [clear traplog on page 139](#)
- [copy on page 139](#)
- [copy \(clibanner\) on page 141](#)
- [enable passwd on page 142](#)
- [logout on page 143](#)
- [ping on page 144](#)
- [reload on page 144](#)
- [show terminal length on page 144](#)
- [terminal length on page 145](#)
- [traceroute on page 145](#)
- [write on page 146](#)

clear config

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

Syntax **clear config**

Mode Privileged Exec

clear counters

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

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

Mode Privileged Exec

clear port-channel

This command clears all port-channels (LAGs).

Syntax **clear port-channel**

Mode Privileged Exec

clear traplog

This command clears the trap log.

Syntax **clear traplog**

Mode Privileged Exec

clear igmpsnooping

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

Syntax **clear igmpsnooping**

Mode Privileged Exec

copy

This command has options that enable you to upload or download files to or from the switch. Local URLs can be specified using TFTP or Xmodem.

The following files can be specified as the source file for uploading from the switch:

- Event log (also called the error log or the persistent log) (**nvrām:errorlog**)
- Buffered message log (also called the System log) (**nvrām:log**)
- startup configuration (**nvrām:startup-config**)
- trap log (**nvrām:traplog**)
- See also [copy \(clibanner\)](#).

Specify a URL for the destination in this form:

```
copy nvrām:clibanner tftp://tftp_server_ip_address/path/filename
copy nvrām:errorlog tftp://tftp_server_ip_address/path/filename
copy nvrām:log tftp://tftp_server_ip_address/path/filename
copy nvrām:traplog tftp://tftp_server_ip_address/path/filename
copy nvrām:script scriptname tftp://tftp_server_ip_address/path/filename
copy nvrām:startup-config tftp://tftp_server_ip_address/path/filename
```

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

- HTTP secure-server certificates (**sslpem-root**, **sslpem-server**, **sslpem-dhweak**, or **sslpem-dhstrong**)
- SSH key files (**sshkey-rsa**, **sshkey-rsa2**, or **sshkey-dsa**)
- SFTOS system software (**system:image**)
- startup configuration (**startup-config**)

Download the startup configuration or code image by specifying the TFTP source as a URL and the destination as either **nvrām:startup-config** or **system:image**, respectively.

The command can also be used to save the running configuration to NVRAM by specifying the source as **system:running-config** and the destination as **nvrām:startup-config**.

The following commands download to the switch (source specified first):

```
copy tftp://tftp_server_ip_address/path/filename nvrām:clibanner
copy tftp://tftp_server_ip_address/path/filename nvrām:script
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-root
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-server
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-dhweak
copy tftp://tftp_server_ip_address/path/filename nvrām:sslpem-dhstrong
copy tftp://tftp_server_ip_address/path/filename nvrām:sshkey-rsa1
copy tftp://tftp_server_ip_address/path/filename nvrām:sshkey-rsa2
copy tftp://tftp_server_ip_address/path/filename nvrām:sshkey-dsa
copy tftp://tftp_server_ip_address/path/filename nvrām:startup-config
copy tftp://tftp_server_ip_address/path/filename system:image
```



Note: You can use the command **copy tftp //tftp_server_ip_address/path/filename nvrām:startup-config** to copy either a binary file or a text file to the startup-config file. The result is a text file.

The following command copies from the switch system memory to flash memory:

copy system:running-config nvram:startup-config



Note: This command creates a text-based startup-config file.

Parameters	<i>tfoot_server_ip_address</i>	Enter the URL of the TFTP server in IPv4 address format: <i>xxx.xxx.xxx.xxx</i>
	<i>path/filename</i>	Enter the path on the TFTP server and the filename. If the file resides in the root directory, then you can simply enter the filename. The path and filename can be no more than 31 characters each. The file size cannot be larger than 2K.
Default	None	
Mode	Privileged Exec	
Command History	Version 2.3 Modified: Modified functionality of copy system:running-config nvram:startup-config and copy tftp //tfoot_server_ip_address/path/filename nvram:startup-config .	
Related Commands	copy (clibanner)	Downloads the CLI banner text file to the switch.
	write	Saves the running configuration to NVRAM, duplicating the functionality of copy system:running-config nvram:startup-config

Example

```

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

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

File transfer operation completed successfully.

```

Figure 35 Using the copy command to Upload the Event Log

copy (clibanner)

This version of the **copy** command, with the “clibanner” option, downloads the CLI banner text file to the switch. Local URLs can be specified using `tftp` or `xmodem`. The CLI banner is configurable text that you can have displayed when the CLI user logs in to the switch. The file

cannot be created on the switch. Instead, create the banner file using a text editor, put it on your TFTP server, and then download it to the switch.

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

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

copy nvram:clibanner tftp://tftp_server_ip_address/filepath

The **no clibanner** command removes the CLI banner.

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

Default none

Mode Privileged Exec

Example

```
copy tftp://192.168.77.52/banner.txt nvram:clibanner
Mode..... TFTP
Set TFTP Server IP..... 192.168.77.52
TFTP Path..... ./
TFTP Filename..... banner.txt
Data Type..... Cli Banner

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

CLI Banner file transfer operation completed successfully!

(Forcel0 S50) #exit
Forcel0 S50) >logout

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

Figure 36 Using the copy command to Download the CLI Banner

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

enable passwd

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

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

logout

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



Note: Save configuration changes before logging out.

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

quit

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



Note: Save configuration changes before logging out.

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

ping

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

Syntax **ping** *ipaddr*

Mode Privileged Exec and User Exec

reload

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

Syntax **reload**

Mode Privileged Exec

Usage Information For a sample of the output from the **reload** command, see the section “Upgrading the Software Image” in the Getting Started chapter of the book *SFTOS Command Reference Guide*.

show terminal length

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

Syntax **show terminal length**

Mode Privileged Exec and User Exec

Command History	Version 2.3	Introduced
	<hr/>	
Related Commands	terminal length	Sets the number of lines displayed on the terminal without pausing.

terminal length

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

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

traceroute

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

Syntax **traceroute** *ipaddr* [*port*]

ipaddr should be a valid IP address.

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

Mode Privileged Exec

write

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

Syntax	write memory		
Mode	Privileged Exec		
Related Commands	<hr/> <table><tr><td>copy</td><td>Uploads and downloads to/from the switch.</td></tr></table> <hr/>	copy	Uploads and downloads to/from the switch.
copy	Uploads and downloads to/from the switch.		

Configuration Scripting

Configuration scripting enables you to generate text-formatted script files representing the current configuration. These configuration script files can be uploaded to a PC and edited, downloaded to the system and applied to the system. Configuration scripts can be applied to one or more switches with no/minor modifications.

Use the **show running-config** command to capture the running configuration into a script. Use the **copy** command (See “[copy](#)” on page 139.) to transfer the configuration script to/from the switch.



Note: The file extension must be “.scr”.

A maximum of ten scripts are allowed on the switch.

The combined size of all script files on the switch shall not exceed 500 KB.

Configuration script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.

The commands in this section are:

- [script apply on page 147](#)
- [script delete on page 147](#)
- [script list on page 147](#)
- [script show on page 148](#)
- [script validate on page 148](#)

script apply

This command applies the commands in the configuration script to the switch. The apply command backs up the running configuration and then starts applying the commands in the script file. Application of the commands stops at the first failure of a command. The *scriptname* parameter is the name of the script to be applied.

Syntax **script apply** *scriptname*

Mode Privileged Exec

script delete

This command deletes a specified script where the *scriptname* parameter is the name of the script to be deleted. The **all** option deletes all the scripts present on the switch.

Syntax **script delete** {*scriptname* | **all**}

Parameters	<i>scriptname</i>	File name of configuration script with extension
	all	Deletes all configuration script files from the switch

Mode Privileged Exec

script list

This command lists all scripts present on the switch as well as the total number of files present.

Syntax **script list**

Mode Privileged Exec

Report Elements Configuration Script Name
Size (Bytes)

script show

This command displays the contents of a script file. The parameter *scriptname* is the name of the script file.

Syntax `script show scriptname`

Mode Privileged Exec

The format of display is: Line <no>: <Line contents>

script validate

This command validates a configuration script file by parsing each line in the script file where *scriptname* is the name of the script to be validated. The validation will stop at the first failure of a command.

Syntax `script validate scriptname`

Mode Privileged Exec

This chapter provides a detailed explanation of the following Syslog commands:

- [logging buffered on page 149](#)
- [logging buffered wrap on page 150](#)
- [logging cli-command on page 150](#)
- [logging console on page 151](#)
- [logging host on page 151](#)
- [logging host reconfigure on page 152](#)
- [logging host remove on page 152](#)
- [logging persistent on page 152](#)
- [logging port on page 152](#)
- [logging syslog on page 153](#)
- [show logging on page 153](#)
- [show logging buffered on page 154](#)
- [show logging hosts on page 155](#)
- [show logging traplogs on page 156](#)

The commands are of two types:

- Configuration commands configure features and options of the device. For every configuration command there is a show command that displays the configuration setting.
- Show commands display settings, statistics, and other information.

logging buffered

This command enables logging of the System Log to RAM and any other enabled destination, including the console and any enabled syslog server.

Syntax **logging buffered** [*severitylevel*]

The *severitylevel* value is specified through one of the following keywords or the keyword's representative integer, as shown here: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Use **no logging buffered** to disable logging to the in-memory log.

Default disabled; critical

Mode Global Config

Related Commands	logging buffered wrap	Enables wrapping of in-memory logging when full capacity is reached.
	logging cli-command	Enables logging to the System Log of all Command Line Interface (CLI) commands issued on the system.
	logging console	Enables logging of System log messages to the console.
	logging host	Configures mirroring of System log messages to a syslog server.
	show logging buffered	Displays buffered logging (the System log).

logging buffered wrap

This command enables wrapping of in-memory logging when full capacity is reached. Otherwise when full capacity is reached, logging stops.

Syntax **logging buffered wrap**

Use **no logging buffered wrap** to disable wrapping of in-memory logging and to configure logging to stop when full capacity is reached.

Default wrap

Mode Privileged Exec

logging cli-command

This command enables logging to the System Log of all Command Line Interface (CLI) commands issued on the system.

Syntax **[no] logging cli-command**

Default enabled

Mode Privileged Exec

logging console

This command enables logging of System log messages to the console.

Syntax **logging console** [*severitylevel*]

The *severitylevel* value is specified through one of the following keywords or the keyword's representative integer, as shown here: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7). Note that the severity level set here does not change the severity level set for the System log messages saved in RAM.

Use **no logging console** to disable logging to the console.

Default disabled; severity = critical

Mode Global Config

logging host

This command configures mirroring of System log messages to a syslog server. Up to eight server hosts can be configured. Also, use this command to modify the port or logging severity level to a configured host identified by its IP address.

Syntax **logging host** *ipaddress* [*port* [*severitylevel*]]

The *severitylevel* value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7). Note that the severity level set here does not change the severity level set for the System log messages saved in RAM.

Default Port = 514; Level = critical

Mode Global Config

**Related
Commands**

[logging buffered](#)

Enables logging of the System Log to RAM and any other enabled destination, including the console and any enabled syslog server.

[show logging hosts](#)

logging host reconfigure

This command enables you to revise the IP address of a configured syslog host.

Syntax **logging host reconfigure** *host-id hostaddress*

Use [show logging hosts](#) to learn association of *host-id* with *hostaddress*.

Mode Global Config

Command History	Version 2.3	Introduced
------------------------	-------------	------------

logging host remove

This command removes the identified host.

Syntax **logging host remove** *host-id*

Use [show logging hosts](#) to learn association of *host-id* with *hostaddress*.

Mode Global Config

logging persistent

Command History	Version 2.3	Removed
------------------------	-------------	---------

logging port

Command History	Version 2.3	Removed
------------------------	-------------	---------

logging syslog

This command enables logging to any configured syslog server.

Syntax **logging syslog**

Use **no logging syslog** to disable syslog logging.

Default disabled; local0

Mode Global Config

show logging

This command displays a combination of the system log and event log (buffered log).

Syntax **show logging**

Mode Privileged Exec

Example

```
Force10 #show logging

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

Syslog Logging                 : disabled

Log Messages Received         : 50
Log Messages Dropped          : 0
Log Messages Relayed          : 0
Log Messages Ignored          : 0

Event Log
-----
```

File	Line	TaskID	Code	d	h	m	s
EVENT> bootos.c	434	0FFFFFFE0	AAAAAAAA	0	0	0	10
ERROR> unitmgr.c	3325	0E14B970	00000000	0	0	11	16
EVENT> bootos.c	434	0FFFFFFE0	AAAAAAAA	0	0	0	9
ERROR> unitmgr.c	3325	0E14B970	00000000	4	2	53	36
EVENT> bootos.c	434	0FFFFFFE0	AAAAAAAA	0	0	0	9
ERROR> unitmgr.c	3325	0E41C9B8	00000000	0	0	7	16
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	12
ERROR> unitmgr.c	3325	0E8382D0	00000000	3	0	21	32
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	13
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	10
EVENT> bootos.c	430	0FFFFFFE0	AAAAAAAA	0	0	0	13

```
Force10 #
```

Figure 37 Sample Output from the show logging Command

Fields in the report include:

Logging Client Local Port—The port on the collector/relay to which syslog messages are sent

CLI Command Logging—The mode for logging CLI commands, whether enabled or disabled

Console Logging—The mode for console logging, whether enabled or disabled

Console Logging Severity Filter—The minimum event severity to display to the console

Buffered Logging—The mode for buffered logging, whether enabled or disabled

Syslog Logging—The mode for logging to configured syslog hosts, whether enabled or disabled. If set to disabled, logging stops to all syslog hosts.

Log Messages Received—The number of messages received by the log process. This includes messages that are dropped or ignored.

Log Messages Dropped—The number of messages that could not be processed

Log Messages Relayed

Log Messages Ignored

Event Log—Table consisting of these columns: File, Line, TaskID, Code, and “d h m s”

File—The file in which the event originated.

Line—The line number of the event.

Task Id—The task ID of the event.

Code—The event code.

“d h m s”—The time this event occurred in days, hours, minutes, and seconds since system boot..



Note: Event log information is retained across a switch reset.

show logging buffered

This command displays buffered logging (the System log).

Syntax **show logging buffered**

Mode Privileged Exec

Fields in the report include:

Buffered (In-Memory) Logging—The current state of the in-memory log

Buffered Logging Wrapping Behavior—The behavior of the in-memory log when faced with a log-full situation. “On” when wrapping is enabled, “Off” when not.

Buffered Log Count—The count of valid entries in the buffered log

The System log messages follow the summary statistics.

Related Commands	logging buffered	Enables logging of the System Log to RAM and any other enabled destination, including the console and any enabled syslog server.
	logging cli-command	Displays CLI activity in the log.

Example

```

Forcel0 #show logging buffered
Buffered (In-Memory) Logging      : enabled
Buffered Logging Wrapping Behavior : On
Buffered Log Count                : 122085

<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121958 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121959 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121960 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121961 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121962 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121963 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121964 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121965 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.
<6> JAN 04 10:23:54 0.0.0.0-1 UNKN[237531112]: filter_cfg.c(1148) 121966 %%
filterIntfChangeCallback: Received an interface event callback while not in
EXECUTE state.

--More-- or (q)uit

```

Figure 38 Sample Output from the show logging Command

show logging hosts

This command displays configured logging hosts.

Syntax `show logging hosts unit`

The *unit* variable is the host index

Mode Privileged Exec

Fields in the report include:

Index—An integer from 1 to 8, used for removing the associated syslog host

IP Address—IP Address of the configured syslog host

Severity—The minimum severity to log to the specified address

Port—Server Port Number. This is the port on the local host from which syslog messages are sent.

Status—The state of logging to configured syslog hosts. If the status is Active, logging occurs; if Disable, no logging occurs.

show logging traplogs

This command displays the SNMP trap summary (number of traps since last reset and last view) and trap details.

Syntax **show logging traplogs**

Mode Privileged Exec

Command History

Version 2.3	Modified: Replaces the show msglog command with the use of the keyword traplogs , displaying the message log maintained by the switch, including system trace information.
-------------	--

Fields in the report include:

Number of Traps since last reset—The number of traps that have occurred since the last reset of this device.

Number of Traps since log last displayed—The number of traps that have occurred since the traps were last displayed. Getting the traps by any method (terminal interface display, Web display, upload file from switch etc.) will result in this counter being cleared to 0.

Log—The sequence number of this trap.

System Up Time—The relative time since the last reboot of the switch at which this trap occurred.

Trap—The relevant information of this trap.

The log messages appear after the summary statistics. The table consists of three columns — Log (sequential number), System Up Time, and Trap.



Note: Trap log information is not retained across a switch reset.

Note: Traps are replicated in the System log, denoted by the “TRAPMGR” Component name and “traputil.c” as the file name.

Commands in this chapter manage user accounts. The commands are comprised of two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

The user account commands are:

- [clear pass on page 157](#)
- [disconnect on page 158](#)
- [show loginsession on page 158](#)
- [show users on page 158](#)
- [username passwd on page 159](#)
- [users snmpv3 accessmode on page 160](#)
- [users snmpv3 authentication on page 160](#)
- [users snmpv3 encryption on page 160](#)



Note: For related commands, see the chapter [Security Commands on page 163](#).

clear pass

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

Syntax **clear pass**

Mode Privileged Exec

disconnect

This command closes the designated remote session or all sessions.

Syntax **disconnect** {*sessionID* | **all**}

Mode Privileged Exec

show loginsession

This command displays current telnet and serial port connections to the switch. It also displays SSH sessions.

Syntax **show loginsession**

Mode Privileged Exec

ID Login Session ID

Parameters User Name—The name the user will use to login using the serial port or Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. The Read/Write user 'admin' is the only factory default.

Connection From—IP address of the telnet client machine or EIA-232 for the serial port connection.

Idle Time—Time this session has been idle.

Session Time—Total time this session has been connected.

Session Type—Source of connection—serial port, Telnet, etc.

show users

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges.

Syntax **show users**

Mode Privileged Exec

Parameters User Name—The name the user will use to login using the serial port, Telnet or Web. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to eight characters, and is not case sensitive. The Read/Write user 'admin' is the only factory default.

User Access Mode—Shows whether the operator is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the 'admin' user has Read/Write access. There can only be one Read/Write user and up to five Read Only users.

SNMPv3 Access Mode—This field displays the SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.

SNMPv3 Authentication—This field displays the authentication protocol to be used for the specified login user.

SNMPv3 Encryption—This field displays the encryption protocol to be used for the specified login user.

username passwd

This command adds a new user (account) if space permits, along with the user's password. This command replaces the **users name** and **users passwd** commands, which have been removed from SFTOS.

Syntax **username** *user* **passwd** *password*

To remove a user, use the **no username** *user* command.

To delete or change a password, remove and reenter the user with the new password.



Note: The 'admin' user account cannot be deleted.

Parameters	<i>user</i>	Enter a string to represent the new user's name. The name can be up to eight characters in length. The name can be comprised of alphanumeric characters, as well as the dash ('-') and underscore ('_').
	password <i>password</i>	Enter the keyword password , followed by a new password, which cannot be more than eight alphanumeric characters in length. Note: If a user is authorized for authentication, or encryption is enabled, the password must be at least eight alphanumeric characters in length.

Default no password

Mode Global Config

Usage Information The username and password are not case-sensitive.

Six user names can be defined.

users snmpv3 accessmode

This command specifies the SNMP v3 access privileges for the specified login user. The valid accessmode values are **readonly** or **readwrite**. The *username* is the login user name for which the specified access mode applies. The default is **readwrite** for 'admin' user; **readonly** for all other users.

The **no** version of this command sets the snmpv3 access privileges for the specified login user as **readwrite** for the 'admin' user; **readonly** for all other users. The *username* is the login user name for which the specified access mode will apply.

Default	admin -- readwrite; other -- readonly
Syntax	[no] users snmpv3 accessmode <i>username</i> [readonly readwrite]
Mode	Global Config

users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are **none**, **md5** or **sha**. If md5 or sha are specified, the user login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *username* is the login user name associated with the authentication protocol.

The **no** version of this command sets the authentication protocol to be used for the specified login user to **none**. The *username* is the login user name for which the specified authentication protocol will be used.

Default	no authentication
Syntax	users snmpv3 authentication <i>username</i> [none md5 sha] users snmpv3 authentication <i>username</i>
Mode	Global Config

users snmpv3 encryption

This command specifies the encryption protocol to be used for the specified login user. The valid encryption protocols are des or **none**.

If **des** is specified, the required key may be specified on the command line. The **key** may be up to 16 characters long. If the **des** protocol is specified but a key is not provided, the user will be prompted for the key. When using the des protocol, the user login password is also used as the snmpv3 encryption password and therefore must be at least eight characters in length.

If **none** is specified, a key must not be provided. The *username* is the login user name associated with the specified encryption.

The **no** version of this command sets the encryption protocol to **none**. The *username* is the login user name for which the specified encryption protocol will be used.

Default	no encryption
Syntax	[no] users snmpv3 encryption <i>username none des [key]</i>
Mode	Global Config

This chapter provides a detailed explanation of the security commands available in the SFTOS software, presented in the following sections:

- [Port Security Commands](#)
- [Port-Based Network Access Control \(IEEE 802.1X\) on page 168](#)
- [RADIUS Commands on page 180](#)
- [TACACS+ Commands on page 187](#)
- [Secure Shell \(SSH\) Commands on page 192](#)
- [Hypertext Transfer Protocol \(HTTP\) Commands on page 195](#)
- [Broadcast Storm Control Commands on page 199](#)



Note: Related chapters include:

- [User Account Commands on page 157](#)
- [ACL Commands on page 287](#)

Port Security Commands

This section contains the following commands:

- [port-security on page 164](#)
- [port-security max-dynamic on page 164](#)
- [port-security max-static on page 165](#)
- [port-security mac-address on page 165](#)
- [port-security mac-address move on page 166](#)
- [show port-security on page 166](#)
- [show port-security on page 166](#)
- [show port-security dynamic on page 167](#)
- [show port-security static on page 168](#)
- [show port-security violation on page 168](#)

Implementation Notes

- 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.

port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config).

The **no** version of this command disables port locking at the system level (Global Config) or port level (Interface Config).

Syntax	[no] port-security				
Default	Disabled				
Modes	Global Config and Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.				
Command History	<hr/> <table><tr><td>Version 2.3</td><td>Added Interface VLAN and Interface Range modes.</td></tr></table> <hr/>	Version 2.3	Added Interface VLAN and Interface Range modes.		
Version 2.3	Added Interface VLAN and Interface Range modes.				
Related Commands	<table><tr><td>interface</td><td>Identifies an interface and enters the Interface Config mode.</td></tr><tr><td>interface range</td><td>Defines an interface range and accesses the Interface Range mode</td></tr></table> <hr/>	interface	Identifies an interface and enters the Interface Config mode.	interface range	Defines an interface range and accesses the Interface Range mode
interface	Identifies an interface and enters the Interface Config mode.				
interface range	Defines an interface range and accesses the Interface Range mode				

port-security max-dynamic

This command sets the maximum of dynamically locked MAC addresses allowed on a specific port.

The **no** version of this command resets the maximum of dynamically locked MAC addresses allowed on a specific port to its default value.

Syntax	port-security max-dynamic <i>maxvalue</i> no port-security max-dynamic
Default	600
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	Version 2.3 Added Interface Range mode.
Related Commands	interface range Defines an interface range and accesses the Interface Range mode

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a specific port.

The **no** version of this command resets the maximum of statically locked MAC addresses allowed on a specific port to its default value.

Syntax	port-security max-static <i>maxvalue</i> no port-security max-static
Default	20
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	Version 2.3 Added Interface Range mode
Related Commands	interface range Defines an interface range and accesses the Interface Range mode

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses. The *vid* is the VLAN ID.

The **no** version of this command removes a MAC address from the list of statically locked MAC addresses.

Syntax **port-security mac-address** *mac-address vid*

no port-security mac-address *mac-address vid*

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.		
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Version 2.3</td> <td>Added Interface Range mode.</td> </tr> </table>	Version 2.3	Added Interface Range mode.
Version 2.3	Added Interface Range mode.		
Related Commands	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">interface range</td> <td>Defines an interface range and accesses the Interface Range mode</td> </tr> </table>	interface range	Defines an interface range and accesses the Interface Range mode
interface range	Defines an interface range and accesses the Interface Range mode		

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

Syntax	port-security mac-address move		
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.		
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Version 2.3</td> <td>Added Interface Range mode.</td> </tr> </table>	Version 2.3	Added Interface Range mode.
Version 2.3	Added Interface Range mode.		
Related Commands	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">interface range</td> <td>Defines an interface range and accesses the Interface Range mode</td> </tr> </table>	interface range	Defines an interface range and accesses the Interface Range mode
interface range	Defines an interface range and accesses the Interface Range mode		

show port-security

This command displays the port-security settings for a particular interface or for the entire system.

Syntax	show port-security [<i>unit/slot/port</i> all]
Mode	Privileged Exec
	When no parameter is entered, the one report field is:
	Port Security Administration Mode—Port-locking mode for the entire system
	When either the <i>unit/slot/port</i> or all parameter is entered, the report fields are:
	Intf — Port number (<i>unit/slot/port</i>)
	Interface Admin Mode — Port-locking mode for the Interface
	Dynamic Limit—Maximum dynamically allocated MAC Addresses
	Static Limit—Maximum statically allocated MAC Addresses
	Violation Trap Mode—Whether violation traps are enabled

Example

```

Forcel0 #show port-security all
  Intf      Admin   Dynamic   Static   Violation
  ---      ---     ---       ---       ---
  1/0/1     Disabled 600       20       Disabled
  1/0/2     Disabled 600       20       Disabled
  1/0/3     Disabled 600       20       Disabled
  1/0/4     Disabled 600       20       Disabled
  1/0/5     Disabled 600       20       Disabled
  1/0/6     Disabled 600       20       Disabled
  1/0/7     Disabled 600       20       Disabled
  1/0/8     Disabled 600       20       Disabled
  1/0/9     Disabled 600       20       Disabled
  1/0/10    Disabled 600       20       Disabled
  1/0/11    Disabled 600       20       Disabled
  1/0/12    Disabled 600       20       Disabled
  1/0/13    Disabled 600       20       Disabled
  1/0/14    Disabled 600       20       Disabled
  1/0/15    Disabled 600       20       Disabled
  1/0/16    Disabled 600       20       Disabled
  1/0/17    Disabled 600       20       Disabled
  1/0/18    Disabled 600       20       Disabled
--More-- or (q)uit
--!output deleted!--
Forcel0#

```

Figure 39 Example of show port-security all Command Output**Related
Commands**

show port-security dynamic	Displays the dynamically locked MAC addresses for port
show port-security static	Displays the statically locked MAC addresses for port
show port-security violation	Displays the source MAC address of the last packet that was discarded on a locked port

show port-security dynamic

This command displays the dynamically locked MAC addresses for port.

Syntax `show port-security dynamic unit/slot/port`

Mode Privileged Exec

The one report field is:

MAC Address — MAC address of the dynamically locked MAC

show port-security static

This command displays the statically locked MAC addresses for port.

Syntax **show port-security static** *unit/slot/port*

Mode Privileged Exec

The one report field is:

MAC Address—MAC Address of statically locked MAC

show port-security violation

This command displays the source MAC address of the last packet that was discarded on a locked port.

Syntax **show port-security violation** *unit/slot/port*

Mode Privileged Exec

The one report field is:

MAC Address—MAC Address of discarded packet on locked port

Port-Based Network Access Control (IEEE 802.1X)

This section contains the following commands:

- [authentication login on page 169](#)
- [clear dot1x statistics on page 170](#)
- [clear radius statistics on page 170](#)
- [dot1x defaultlogin on page 170](#)
- [dot1x initialize on page 171](#)
- [dot1x login on page 171](#)
- [dot1x max-req on page 171](#)
- [dot1x port-control on page 172](#)
- [dot1x port-control all on page 172](#)
- [dot1x re-authenticate on page 173](#)
- [dot1x re-authentication on page 173](#)
- [dot1x system-auth-control on page 174](#)

- [dot1x timeout on page 174](#)
- [dot1x user on page 175](#)
- [show authentication on page 175](#)
- [show authentication users on page 176](#)
- [show dot1x on page 176](#)
- [show dot1x users on page 179](#)
- [show users authentication on page 179](#)
- [users defaultlogin on page 180](#)
- [users login on page 180](#)

authentication login

This command creates an authentication login list. To authenticate a user, the authentication methods in the user's login will be attempted in the order specified by the list until an authentication attempt succeeds or fails.



Note: The default login list included with the default configuration can not be changed.

Syntax `authentication login listname [method1 [method2 [method3]]]`

`no authentication login listname`

The *listname* is up to 15 alphanumeric characters and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method "local" is set as the first method by default.

When the optional parameters *method1*, and, optionally, *method2* and *method3* are used, an ordered list of the methods specified in those parameters is set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the list. The maximum number of authentication login methods is three. The possible method values are **local**, **radius**, **tacacs**, and **reject**:

- The **local** keyword indicates that the user's locally stored ID and password are used for authentication.
- The **radius** keyword indicates that the user's ID and password will be authenticated using a RADIUS server.
- The **tacacs** keyword indicates that the user's ID and password will be authenticated using a TACACS+ server.
- The **reject** keyword indicates the user is never authenticated.

The **no** version of this command deletes the specified authentication login list. The attempt to delete fails if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the non configured user for any component

The login list is the default login list included with the default configuration and was not created using ‘authentication login’. The default login list cannot be deleted.

Mode Global Config

**Related
Commands**

[radius server host](#) Configure the RADIUS authentication and accounting server.

[tacacs-server host](#) Specify a TACACS+ server host.

[show authentication](#)

clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Syntax **clear dot1x statistics {unit/slot/port | all}**

Mode Privileged Exec

clear radius statistics

This command is used to clear all RADIUS statistics.

Syntax **clear radius statistics**

Mode Privileged Exec

dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Syntax **dot1x defaultlogin** *listname*

Mode Global Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Syntax **dot1x initialize** *unit/slot/port*

Mode Global Config

Command History

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

dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The user parameter must be a configured user and the listname parameter must be a configured authentication login list.

Syntax **dot1x login** *user listname*

Mode Global Config

dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Syntax **dot1x max-req** *count*

The *count* value must be in the range 1 - 10.

The **no** version of this command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Default	2
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	Version 2.3 Interface Range mode added
Related Commands	interface range Defines an interface range and accesses the Interface Range mode

dot1x port-control

This command sets the authentication mode to be used on the specified port. The control mode may be one of the following.

Force-unauthorized—The authenticator PAE unconditionally sets the controlled port to unauthorized.

Force-authorized—The authenticator PAE unconditionally sets the controlled port to authorized.

Auto—The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Syntax **dot1x port-control {force-unauthorized | force-authorized | auto}**

Use **no dot1x port-control** to set the authentication mode to be used on the specified port to **auto**.

Default **auto**

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

Command History	Version 2.3 Interface Range mode added
Related Commands	interface range Defines an interface range and accesses the Interface Range mode

dot1x port-control all

This command sets the authentication mode to be used on all ports. The control mode may be one of the following.

Force-unauthorized—The authenticator PAE unconditionally sets the controlled port to unauthorized.

Force-authorized—The authenticator PAE unconditionally sets the controlled port to authorized.

Auto—The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server.

Syntax **dot1x port-control all** { **force-unauthorized** | **force-authorized** | **auto** }

no dot1x port-control all sets the authentication mode to be used on all ports to **auto**.

Default **auto**

Mode Global Config

dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Syntax **dot1x re-authenticate** *unit/slot/port*

Mode Global Config

Command History

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

dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

The **no** version of this command disables re-authentication of the supplicant for the specified port.

Syntax **dot1x re-authentication**

Default disabled

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

Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

dot1x system-auth-control

This command is used to enable the dot1x authentication support on the switch. By default, the authentication support is disabled. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

The **no** version of this command is used to disable the dot1x authentication support on the switch.

Syntax **dot1x system-auth-control**

Default disabled

Mode Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the keyword used and the value (in seconds) passed, various timeout configurable parameters are set.

Syntax **dot1x timeout** **{reauth-period seconds} | {quiet-period seconds} | {tx-period seconds} | {supp-timeout seconds} | {server-timeout seconds}**

The **no** version of this command sets the value, in seconds, of the specified timer to the its default value:

no dot1x timeout {reauth-period | quiet-period | tx-period | supp-timeout | server-timeout}

Parameters reauth-period—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

quiet-period—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.

tx-period—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.

supp-timeout—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.

server-timeout—Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default reauth-period: 3600 seconds

quiet-period: 60 seconds

tx-period: 30 seconds

supp-timeout: 30 seconds

server-timeout: 30 seconds

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

Command History	Version 2.3	Interface Range mode added
	show dot1x	Display data on the dot1x configuration, for a specified port or all ports,
Related Commands		

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *user* parameter must be a configured user.

The **no** version of this command removes the user from the list of users with access to the specified port or all ports.

Syntax **dot1x user** *user* {*unit/slot/port* | **all**}

Mode Global Config

Related Commands	show dot1x users	Display 802.1x port security user information for locally configured users.
-------------------------	----------------------------------	---

show authentication

This command displays the ordered authentication methods for all authentication login lists.

Syntax	show authentication		
Mode	Privileged Exec		
	Authentication Login List—This displays the authentication login listname.		
	Method 1—This displays the first method in the specified authentication login list, if any.		
	Method 2—This displays the second method in the specified authentication login list, if any.		
	Method 3—This displays the third method in the specified authentication login list, if any.		
Related Commands	<hr/> <table><tr><td>authentication login</td><td>Define authentication login lists.</td></tr></table> <hr/>	authentication login	Define authentication login lists.
authentication login	Define authentication login lists.		

show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Syntax	show authentication users <i>listname</i>
Mode	Privileged Exec
	User—This field displays the user assigned to the specified authentication login list.
	Component—This field displays the component (User or 802.1x) for which the authentication login list is assigned.

show dot1x

This command displays a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the keywords used.

Syntax	show dot1x [{summary { <i>unit/slot/port</i> all } {detail <i>unit/slot/port</i>} {statistics <i>unit/slot/port</i>}]
Mode	Privileged Exec
	If none of the optional parameters are used, the global dot1x configuration summary is displayed.
	Administrative mode—Indicates whether authentication control on the switch is enabled or disabled.

If the optional parameter **summary** { *unit/slot/port* | **all** } is used, the dot1x configuration for the specified port or all ports are displayed.

Port—The interface whose configuration is displayed.

Control Mode—The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto

Operating Control Mode—The control mode under which this port is operating. Possible values are authorized | unauthorized

Reauthentication Enabled—Indicates whether re-authentication is enabled on this port

Key Transmission Enabled—Indicates if the key is transmitted to the supplicant for the specified port

If the optional parameter **detail** *unit/slot/port* is used, the detailed dot1x configuration for the specified port are displayed.

Port—The interface whose configuration is displayed

Protocol Version—The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.

PAE Capabilities—The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.

Authenticator PAE State—Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.

Backend Authentication State—Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.

Quiet Period—The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.

Transmit Period—The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

Supplicant Timeout—The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.

Server Timeout—The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.

Maximum Requests—The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.

Reauthentication Period—The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.

Reauthentication Enabled—Indicates if reauthentication is enabled on this port. Possible values are "True" or "False".

Key Transmission Enabled—Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.

Control Direction—Indicates the control direction for the specified port or ports. Possible values are both or in.

Example

```

Forcel0 #show dot1x detail 0/1

Port..... 1/0/1
Protocol Version..... 1
PAE Capabilities..... Authenticator
Authenticator PAE State..... Initialize
Backend Authentication State..... Initialize
Quiet Period..... 60
Transmit Period..... 30
Supplicant Timeout..... 30
Server Timeout (secs)..... 30
Maximum Requests..... 2
Reauthentication Period..... 3600
Reauthentication Enabled..... FALSE
Key Transmission Enabled..... FALSE
Control Direction..... both

```

Figure 40 Example of Output from the show dot1x detail Command

If the optional parameter **statistics unit/slot/port** is used, the dot1x statistics for the specified port are displayed.

Port—The interface whose statistics are displayed.

EAPOL Frames Received—The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted—The number of EAPOL frames of any type that have been transmitted by this authenticator.

EAPOL Start Frames Received—The number of EAPOL start frames that have been received by this authenticator.

EAPOL Logoff Frames Received—The number of EAPOL logoff frames that have been received by this authenticator.

Last EAPOL Frame Version—The protocol version number carried in the most recently received EAPOL frame.

Last EAPOL Frame Source—The source MAC address carried in the most recently received EAPOL frame.

EAP Response/Id Frames Received—The number of EAP response/identity frames that have been received by this authenticator.

EAP Response Frames Received—The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.

EAP Request/Id Frames Transmitted—The number of EAP request/identity frames that have been transmitted by this authenticator.

EAP Request Frames Transmitted—The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

Invalid EAPOL Frames Received—The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

EAP Length Error Frames Received—The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x users

This command displays 802.1x port security user information for locally configured users.

Syntax **show dot1x users** *unit/slot/port*

Mode Privileged Exec

Example

```
Force10 #show dot1x users 0/1
Users
-----
admin
```

Figure 41 Example of Output from the show dot1x users Command

User—Users configured locally to have access to the specified port.

**Related
Commands**

[dot1x user](#) Add the specified user to the list of users with access to the specified port or all ports.

show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Syntax **show users authentication**

Mode Privileged Exec

Example

```
Force10 #show users authentication
Authentication Login Lists
User          System Login    802.1x
-----
admin        defaultList     defaultList
default      tacConfig       defaultList
```

Figure 42 Example Output from the show users authentication Command

User—This field lists every user that has an authentication login list assigned.

System Login—This field displays the authentication login list assigned to the user for system login.

802.1x Port Security—This field displays the authentication login list assigned to the user for 802.1x port security.

users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Syntax `users defaultlogin listname`

Mode Global Config

users login

This command assigns the specified authentication login list to the specified user for system login. The *user* must be a configured *user* and the *listname* must be a configured login list.

If the user is assigned a login list that requires remote authentication, all user access (from all CLI, Web, and Telnet sessions) will be blocked until authentication is complete.

Note that the login list associated with the 'admin' user cannot be changed to prevent accidental lockout from the switch.

Syntax `users login user listname`

Mode Global Config

RADIUS Commands

This section contains the following commands for the Remote Authentication Dial-In User Service (RADIUS), one method for validating administration access to the switch:

- [radius accounting mode on page 181](#)
- [radius server host on page 181](#)
- [radius server key on page 182](#)
- [radius server msgauth on page 183](#)
- [radius server primary on page 183](#)
- [radius server retransmit on page 183](#)
- [radius server timeout on page 184](#)
- [show radius on page 184](#)
- [show radius accounting statistics on page 185](#)
- [show radius statistics \(authentication\) on page 186](#)

radius accounting mode

This command is used to enable the RADIUS accounting function.

The **no** version of this command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Syntax **radius accounting mode**

Default disabled

Mode Global Config

radius server host

Configure the RADIUS authentication and accounting server connections.

Syntax **radius server host {auth | acct} ipaddr [port]**

no radius server host {auth | acct} ipaddr

Parameters	auth	Use this keyword if you want to configure a connection to a RADIUS authentication server. See Usage, below.
	acct	Use this keyword if you want to configure a connection to a RADIUS accounting server. See Usage, below.
	<i>ip-addr</i>	Enter the IP address, in dotted decimal format, of the server host.
	<i>port</i>	(Optional) Configure the UDP port number to use to connect to the configured RADIUS server. See Usage, below.

Usage If the **auth** keyword is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the **no** form of the command.

If the optional *port* parameter is used with the **auth** keyword, the command will configure the UDP port number to use to connect to the configured RADIUS authentication server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The port number must lie between 1 - 65535, with 1812 being the default value.

If the **acct** keyword is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the **no** form of the command before this command succeeds. If the optional *port* parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server, then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

The **no** version of this command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the **auth** keyword is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the **acct** keyword is used, the previously configured RADIUS accounting server is removed from the configuration. The *ipaddr* parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

Mode Global Config

**Related
Commands**

authentication login	Define an authentication login list.
show radius	Display RADIUS servers.
users defaultlogin	Assign the authentication login list to use for non-configured users when attempting to log in to the system.

radius server key

Configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server.

Syntax **radius server key {auth | acct} ipaddr**

Depending on whether the **auth** or **acct** keyword is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

Mode Global Config

radius server msgauth

This command enables the message authenticator attribute for a specified server.

Syntax **radius server msgauth** *ipaddr*

Mode Global Config

radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Syntax **radius server primary** *ipaddr*

Mode Global Config

radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

The **no** version of this command sets the maximum number of times a request packet is re-transmitted, when no response is received from the RADIUS server, to the default value, i.e. 10.

Syntax **radius server retransmit** *retries*
no radius server retransmit

Default 10

Mode Global Config

radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Syntax **radius server timeout** *seconds*

The **no radius server timeout** command sets the timeout value to the default value, after which a request must be retransmitted to the RADIUS server if no response is received.

Default 6

Mode Global Config

show radius

This command is used to display the various RADIUS configuration items for the switch, as well as the configured RADIUS servers.

Syntax **show radius** [**servers**]

Mode Privileged Exec

If the optional keyword **servers** is not included, the following RADIUS configuration items will be displayed:

Primary Server IP Address—Indicates the configured server currently in use for authentication

Number of configured servers—The configured IP address of the authentication server

Max number of retransmits—The configured value of the maximum number of times a request packet is retransmitted

Timeout Duration—The configured timeout value, in seconds, for request re-transmissions

Accounting Mode—Yes or No

If the optional keyword **servers** is included, the following information regarding configured RADIUS servers is displayed.

IP Address—IP Address of the configured RADIUS server

Port—The port in use by this server

Type—Primary or secondary

Secret Configured—Yes / No

show radius accounting statistics

This command is used to display the configured RADIUS accounting mode, accounting server, and the statistics for the configured accounting server.

Syntax `show radius accounting [statistics IP address]`

Mode Privileged Exec

If the optional keyword **statistics IP address** is not included, then only the accounting mode and the RADIUS accounting server details are displayed, as listed here:

Example

```
(S50-TAC-5) #show radius accounting
RADIUS Accounting Mode..... Disable
IP Address..... 1.1.1.1
Port..... 1813
Secret Configured..... NoForce10#
```

Figure 43 show radius accounting Command Example

Table 19 show radius accounting Command Example Fields

Field	Description
RADIUS Accounting Mode	Enabled or disabled
IP Address	The configured IP address of the RADIUS accounting server
Port	The port in use by the RADIUS accounting server
Secret Configured	Yes or No

If the optional keyword **statistics IP address** is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Example

```
(S50-TAC-5) #show radius accounting accounting statistics 1.1.1.1
RADIUS Accounting Server IP Address..... 1.1.1.1
Round Trip Time..... 0.00
Requests..... 0
Retransmissions..... 0
Responses..... 0
Malformed Responses..... 0
Bad Authenticators..... 0
Pending Requests..... 0
Timeouts..... 0
Unknown Types..... 0
Packets Dropped..... 0
```

Figure 44 show radius accounting statistics IP address Command Example

Table 20 show radius accounting Command Example Fields

Field	Description
RADIUS Accounting Server IP Address	IP Address of the configured RADIUS accounting server
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

show radius statistics (authentication)

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Syntax `show radius statistics [IP address]`

Mode Privileged Exec

If the IP address is not specified, then only the Invalid Server Address field is displayed. Otherwise all the following listed fields are displayed:

Invalid Server Addresses—The number of RADIUS Access-Response packets received from unknown addresses.

Server IP Address—IP address of the server.

Round Trip Time—The time interval, in hundredths of a second, between the most recent Access-Reply | Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

Access Requests—The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

Access Retransmission—The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

Access Accepts—The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.

Access Rejects—The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.

Access Challenges—The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.

Malformed Access Responses—The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.

Bad Authenticators—The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.

Pending Requests—The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.

Timeouts—The number of authentication timeouts to this server.

Unknown Types—The number of RADIUS packets of unknown types, which were received from this server on the authentication port.

Packets Dropped—The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

TACACS+ Commands

SFTOS supports Terminal Access Controller Access Control System (TACACS+) as another method for administrator login authentication. This section contains these commands:

- [tacacs-server host on page 188](#)
- [tacacs-server key on page 188](#)
- [tacacs-server timeout on page 189](#)
- [key on page 189](#)
- [port on page 190](#)
- [priority on page 190](#)
- [single-connection on page 191](#)
- [show tacacs on page 191](#)
- [timeout on page 191](#)

tacacs-server host

Configure a TACACS+ server and enter into TACACS+ Configuration mode.

Syntax `tacacs-server host ip-address`

To remove a TACACS+ server host, use the **no tacacs-server host** {*hostname* | *ip-address*} command.

Parameters	<i>ip-address</i>	Enter the IP address, in dotted decimal format, of the TACACS+ server host.
Default	Not configured	
Mode	CONFIGURATION	
Usage Information	In CONFIGURATION mode, you can set several global values for all TACACS+ servers, as listed below. Successful use of the tacacs-server host command to identify a particular host puts you into the TACACS configuration mode for that particular host. In that mode, you can override global and default settings of those parameters. In that TACACS configuration mode, you can also use the following commands for the particular TACACS host: key, port, priority, single-connection, and timeout	
Related Commands	authentication login	Specify the login authentication method.
	tacacs-server key	Configure a TACACS+ key for the TACACS server.
	tacacs-server timeout	Specify a global timeout value for all TACACS+ hosts.
	single-connection	Configure the client to maintain a single open connection with the TACACS server.
	port	Specify a server port number for a particular TACACS host.
	timeout	Specify the timeout value for a particular TACACS host.
	key	Specify the authentication and encryption key for all communications between the client and the particular TACACS server.
	priority	Specify the priority value for a particular TACACS server.
	show tacacs	Display settings for all or a particular TACACS server.

tacacs-server key

Configure a key for communication between a TACACS+ server and client.

Syntax `tacacs-server key key`

To delete a key, use the **no tacacs-server key *key***

Parameters	<i>key</i>	Enter a text string, up to 127 characters long, as the clear text password. Leading spaces are ignored.
Default	Not configured.	
Command Modes	CONFIGURATION	
Usage Information	The key configured with this command must match the key configured on the TACACS+ daemon.	
Related Commands	tacacs-server host	Identify a TACACS server.
	key	Specify the authentication and encryption key for all communications between the client and a particular TACACS server.

tacacs-server timeout

Specify a global timeout value for all TACACS+ hosts.

Syntax **tacacs-server timeout** *timeout*

To restore the default, enter **no tacacs-server timeout**.

Parameters	<i>timeout</i>	Range: 1 to 30 seconds
Default	5 seconds	
Mode	Global Config	
Related Commands	tacacs-server host	Identify a TACACS server.
	timeout	Specify the timeout value for a particular TACACS server.

key

Specify the authentication and encryption key for all communications between the client and the particular TACACS server. This key must match the key configured on the server.

Syntax **key** *key-string*

Parameters	<i>key-string</i>	Range: 1 to 128 characters
-------------------	-------------------	----------------------------

port

Default If unspecified, the key-string defaults to the global value.

Command Mode TACACS Configuration

Related Commands	tacacs-server host	Identify a TACACS server.
	tacacs-server key	Specify the authentication and encryption key at a global level for communications between the client and TACACS servers.

port

Specify a server port number for a particular TACACS host.

Syntax **port** *port-number*

Parameters	<i>port-number</i>	Range: zero (0) to 65535
-------------------	--------------------	--------------------------

Default If unspecified, the port number defaults to 49.

Command Mode TACACS Configuration

tacacs-server host	Identify a TACACS server.
------------------------------------	---------------------------

priority

Use the priority command to determine the order in which the servers will be used, with 0 being the highest priority.

Syntax **priority** *priority*

Parameters	<i>priority</i>	Range: zero (0) to 65535
-------------------	-----------------	--------------------------

Default If unspecified, the priority defaults to 0.

Command Mode TACACS Configuration

Related Commands	tacacs-server host	Identify a TACACS server.
-------------------------	------------------------------------	---------------------------

single-connection

Configure the client to maintain a single open connection with the TACACS server.

Syntax **[no] single-connection**

Default Use multiple connections. In other words, the client will use a separate connection for each authentication session.

Command Mode TACACS Configuration

Related Commands	tacacs-server host	Identify a TACACS server.
-------------------------	------------------------------------	---------------------------

show tacacs

Display configuration and status for a particular TACACS server.

Syntax **show tacacs** [*ip-address*]

Parameters	<i>ip-address</i>	IP address of the server host, in dotted decimal format.
-------------------	-------------------	--

Command Mode Privileged Exec

Related Commands	tacacs-server host	Identify a TACACS server.
-------------------------	------------------------------------	---------------------------

timeout

Specify the timeout value for a particular TACACS host.

Syntax **timeout** *timeout*

Parameters	<i>timeout</i>	Range: 1 to 30 seconds
-------------------	----------------	------------------------

Default If no timeout value is specified, the global value is used.

Command Mode TACACS Configuration

Related Commands	tacacs-server host	Identify a TACACS server.
	tacacs-server timeout	Specify the authentication and encryption key for all communications between the client and the particular TACACS server.

Secure Shell (SSH) Commands

The commands in this section are:

- [ip ssh maxsessions on page 192](#)
- [ip ssh protocol on page 193](#)
- [ip ssh server enable on page 193](#)
- [ip ssh timeout on page 194](#)
- [show ip ssh on page 194](#)
- [sshcon maxsessions on page 195](#)
- [sshcon timeout on page 195](#)

This section provides a detailed explanation of the SSH commands. The commands are of two functional types:

- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display switch settings, statistics and other information.

ip ssh maxsessions

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

Syntax `ip ssh maxsessions 0-5`

The command **no ip ssh maxsessions** sets the maximum number of SSH connection sessions that can be established to the default value.

Default 5

Mode Global Config

Command History	Version 2.3	Changed from sshcon maxsessions and moved from Privileged Exec mode to Global Config mode.
------------------------	-------------	---

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Syntax	ip ssh protocol [1] [2]
Default	1 and 2
Mode	Global Config
Command History	Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode.

ip ssh server enable

Enable SSH.

The **no** version of this command disables SSH..



Note: This command requires keys/certificates to be generated offline before the service will start. See *s50-secure-management.pdf* at (log-in required):
<https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx>

Syntax	ip ssh server enable
	no ip ssh server enable
Default	disabled
Mode	Global Config
Command History	Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode.
Related Commands	ip telnet server enable Enable/disable Telnet services.
	ip http secure-server enable Enable/disable HTTPS services.

ip ssh timeout

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

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

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

Syntax `ip ssh timeout 1-160`

The time is a decimal value from 1 to 160.

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

Default 5 (minutes)

Mode Global Config

Command History

Version 2.3	Changed from sshcon timeout and moved from Privileged Exec mode to Global Config.
-------------	--

Related Commands

show ip ssh	This command displays the SSH settings.
-----------------------------	---

show ip ssh

This command displays the SSH settings.

Syntax `show ip ssh`

Mode Privileged Exec

Report fields:

Administrative Mode—This field indicates whether the administrative mode of SSH is enabled or disabled.

Protocol Levels—The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.

Connections—This field specifies the current SSH connections.

SSH Sessions Currently Active

Max SSH Sessions Allowed

SSH Timeout—SSH login timeout configured by **ip ssh timeout** command

sshcon maxsessions

Command History	Version 2.3	Replaced by ip ssh maxsessions .
------------------------	-------------	--

sshcon timeout

Command History	Version 2.3	Replaced by ip ssh timeout .
------------------------	-------------	--

Hypertext Transfer Protocol (HTTP) Commands

The commands in this section are:

- [ip http javamode enable on page 196](#)
- [ip http secure-port on page 196](#)
- [ip http secure-protocol on page 196](#)
- [ip http secure-server enable on page 197](#)
- [ip http server enable on page 197](#)
- [show ip http on page 198](#)

This section provides a detailed explanation of the HTTP commands. The commands are divided into the following groups:

- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display switch settings, statistics and other information.

ip http javamode enable

Enable Java mode for the Web interface to SFTOS.

Syntax	ip http javamode enable
	Use no ip http javamode enable to disable Java mode.
Default	disabled
Mode	Global Config
Command History	<hr/> Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode. <hr/>

ip http secure-port

This command is used to set the SSLT port.

Syntax	ip http secure-port <i>portid</i>
	The no ip http secure-port command resets the SSLT port to the default value.
	The <i>portid</i> value can be from 1 to 65535.
Default	443
Mode	Global Config
Command History	<hr/> Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode. <hr/>

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Syntax	ip http secure-protocol [SSL3] [TLS1]
Default	SSL3 and TLS1
Mode	Global Config
Command History	<hr/> Version 2.3 Modified: Moved from Privileged Exec mode to Global Config mode. <hr/>

ip http secure-server enable

This command is used to enable the secure socket layer for secure HTTP.

The **no** version of this command is used to disable the secure socket layer for secure HTTP.



Note: This command requires keys/certificates to be generated offline before the service will start. See *s50-secure-management.pdf* at (log-in required): <https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx>

Syntax	[no] ip http secure-server enable	
Default	disabled	
Mode	Global Config	
Command History	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode and added enable to the command.

ip http server enable

This command enables access to the switch through the Web User Interface (Web UI) of SFTOS. When access is enabled, the user can log in to the switch from the Web UI.

Syntax	[no] ip http server enable	
	Use no ip http server enable to disable access to the switch through the Web UI. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web UI takes effect immediately. All interfaces are affected.	
Default	enabled	
Mode	Global Config	
Command History	Version 2.3	Modified: Moved from Privileged Exec mode to Global Config mode and added enable to the command.
Related Commands	ip address (management)	Configures the IP address of the management interface.
	ip http secure-server enable	Enable the secure socket layer for secure HTTP.
	show ip http	Displays the HTTP settings for the switch.

show ip http

This command displays the HTTP settings for the switch.

Syntax `show ip http`

Mode Privileged Exec

The report fields are:

HTTP Mode (Unsecure) — This field indicates whether basic HTTP is enabled or disabled on the switch.

HTTP Mode (Secure) — This field indicates whether the administrative mode of secure HTTP (HTTPS) is enabled or disabled on the switch.

Java Mode — This field indicates whether Java mode is enabled or disabled on the switch.

Secure Port—This field specifies the port configured for SSLT.

Secure Protocol Level—The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.

Example

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

Figure 45 Example of show ip http Command Output

Broadcast Storm Control Commands

This section contains the following commands:

- [show storm-control](#)
- [storm-control broadcast on page 200](#)
- [storm-control flowcontrol on page 200](#)



Note: This feature works on the 10G ports of the S2410, but because of S2410 hardware limitations, broadcast storm recovery counters are not incremented.

show storm-control

This command displays switch configuration information.

Syntax `show storm-control [unit/slot/port | all]`

Mode Privileged Exec

Broadcast Storm Recovery Mode—May be enabled or disabled. The factory default is disabled.

802.3x Flow Control Mode—May be enabled or disabled. The factory default is disabled.

Example

```
Force10-S50 #show storm-control
802.3x Flow Control Mode..... Disable

Force10-S50 #show storm-control 1/0/1

  Intf      Bcast   Bcast   Mcast   Mcast   Ucast   Ucast
  Mode     Level  Mode    Level  Mode    Level
-----
1/0/1  Disable   5      Disable   5      Disable   5

Force10-S50 #show storm-control all ?
<cr>                               Press enter to execute the command.

Force10-S50 #show storm-control all

  Intf      Bcast   Bcast   Mcast   Mcast   Ucast   Ucast
  Mode     Level  Mode    Level  Mode    Level
-----
1/0/1  Disable   5      Disable   5      Disable   5
1/0/2  Disable   5      Disable   5      Disable   5
1/0/3  Disable   5      Disable   5      Disable   5
1/0/4  Disable   5      Disable   5      Disable   5
1/0/5  Disable   5      Disable   5      Disable   5
1/0/6  Disable   5      Disable   5      Disable   5
1/0/7  Disable   5      Disable   5      Disable   5
1/0/8  Disable   5      Disable   5      Disable   5
1/0/9  Disable   5      Disable   5      Disable   5
!-----output truncated-----!
```

Figure 46 Command Example: show storm-control

Related Commands	storm-control broadcast	Configure storm control.
	show interface ethernet	The report generated by the show interface ethernet command contains broadcast storm statistics.
	snmp-server enable traps bcaststorm	Enable the sending of Broadcast Storm traps.

storm-control broadcast

This command enables broadcast storm recovery mode. If the mode is enabled, broadcast storm recovery with high and low thresholds is implemented.

The threshold implementation follows a percentage pattern. If the broadcast traffic on any Ethernet port exceeds the high threshold percentage (as represented in [Table 21](#)) of the link speed, the switch discards the broadcast traffic until the traffic returns to the low threshold percentage or less. The full implementation is depicted in the table below.

Table 21 Broadcast Storm Recovery Thresholds

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

Syntax `[no] storm-control broadcast`

Default disabled

Mode Global Config

Related Commands	show storm-control	Shows the storm control configuration
	show interface ethernet	Shows broadcast storm statistics

storm-control flowcontrol

This command enables 802.3x flow control for the switch.

Syntax `[no] storm-control flowcontrol`

The **no** version of this command disables 802.3x flow control for the switch.



Note: This command only applies to full-duplex mode ports.

Note: 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

Default disabled

Mode Global Config

These commands configure the Dynamic Host Configuration Protocol (DHCP) Server parameters and address pools.

The following commands are covered in this chapter:

- [bootfile on page 204](#)
- [clear ip dhcp binding on page 204](#)
- [clear ip dhcp server statistics on page 204](#)
- [clear ip dhcp conflict on page 205](#)
- [client-identifier on page 205](#)
- [client-name on page 205](#)
- [default-router on page 206](#)
- [dns-server on page 206](#)
- [domain-name on page 206](#)
- [hardware-address on page 207](#)
- [host on page 207](#)
- [ip dhcp bootp automatic on page 208](#)
- [ip dhcp conflict logging on page 208](#)
- [ip dhcp excluded-address on page 208](#)
- [ip dhcp ping packets on page 209](#)
- [ip dhcp pool on page 209](#)
- [lease on page 209](#)
- [network on page 210](#)
- [netbios-name-server on page 210](#)
- [netbios-node-type on page 210](#)
- [next-server on page 211](#)
- [option on page 211](#)
- [service dhcp on page 212](#)
- [show ip dhcp binding on page 212](#)
- [show ip dhcp global configuration on page 213](#)
- [show ip dhcp pool configuration on page 213](#)
- [show ip dhcp server statistics on page 214](#)
- [show ip dhcp conflict on page 214](#)

bootfile

The command specifies the name of the default boot image for a DHCP client. The filename specifies the boot image file.

The **no** version of this command deletes the boot image name.

Syntax **bootfile** *filename*

no bootfile

Default none

Mode DHCP Pool Config

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If “*” is specified, the bindings corresponding to all the addresses are deleted. address is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Syntax **clear ip dhcp binding** {*address* | *}

Default none

Mode Privileged Exec

clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Syntax **clear ip dhcp server statistics**

Mode Privileged Exec

clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (*) character is used as the address parameter.

Syntax **clear ip dhcp conflict** {*address* | *}

Default none

Mode Privileged Exec

client-identifier

This command specifies the unique identifier for a DHCP client. The unique identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. Refer to the "Address Resolution Protocol Parameters" section of RFC 1700, Assigned Numbers for a list of media type codes.

The **no** version of this command deletes the client identifier.

Syntax [**no**] **client-identifier** *uniqueidentifier*

Default None

Mode DHCP Pool Config

client-name

This command specifies the name for a DHCP client. The name is a string consisting of standard ASCII characters.

The **no** version of this command removes the client name.

Syntax **client-name** *name*
no client-name

Default None

Mode DHCP Pool Config

default-router

This command specifies the default router list for a DHCP client. { *address1*, *address2*...*address8* } are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

The **no** version of this command removes the default router list.

Syntax **default-router** *address1* [*address2*....*address8*]
 no default-router

Default None

Mode DHCP Pool Config

dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

The **no** version of this command removes the DNS Server list.

Syntax **dns-server** *address1* [*address2*....*address8*]
 no dns-server

Default none

Mode DHCP Pool Config

domain-name

This command specifies the domain name for a DHCP client. The domain specifies the domain name string of the client.

The **no** version of this command removes the domain name.

Syntax **domain-name** *domain*

Default none

Mode DHCP Pool Config

hardware-address

This command specifies the hardware address of a DHCP client.

The **hardware-address** is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format.

The *type* indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

The **no** version of this command removes the hardware address of the DHCP client.

Syntax [no] **hardware-address** *hardware-address* [*type*]

Default ethernet

Mode DHCP Pool Config

host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

The *prefix-length* is an integer from 0 to 32.

The **no** version of this command removes the IP address of the DHCP client.

Syntax **host** *address* [**mask** | *prefix-length*]

no host

Default none

Mode DHCP Pool Config

ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

The **no** version of this command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Syntax **ip dhcp bootp automatic**

Default disable

Mode Global Config

ip dhcp conflict logging

This command enables conflict logging on DHCP server.

The **no** version of this command disables conflict logging on DHCP server.

Syntax **ip dhcp conflict logging**

Default enabled

Mode Global Config

ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Syntax **ip dhcp excluded-address** *lowaddress* [*highaddress*]

The **no** version of this command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default none

Mode Global Config

ip dhcp ping packets

This command is used to specify the number in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. Setting the number of ping packets to 0 is the same as 'no ip dhcp ping packets' and will prevent the server from pinging pool addresses.

Syntax **ip dhcp ping packets** *0,2-10*

Use **no ip dhcp ping packets** to prevent the server from pinging pool addresses and will set the number of packets to 0.

Default 2

Mode Global Config

ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP Pool Config mode.

Syntax **ip dhcp pool** *name*

The **no** version of this command removes the DHCP address pool. The name should be a previously configured pool name.

Default none

Mode Global Config Mode

lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If *infinite* is specified, lease is set for 60 days. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 1439. *Minutes* is an integer from 0 to 86399.

The **no** version of this command restores the default value of the lease time for DHCP Server.

Syntax **lease** {[*days* [*hours*] [*minutes*]] | [**infinite**]}

Default 1 (day)

Mode DHCP Pool Config

network

This command is used to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

The **no** version of this command removes the subnet number and mask.

Syntax **network** *networknumber* [**mask** | **prefixlength**]

no network

Default none

Mode DHCP Pool Config

netbios-name-server

This command configures Windows Internet Naming Service (WINS) name servers that are available to DHCP clients. WINS name servers map NetBIOS names to IP addresses on TCP/IP networks.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (*address1* is the most preferred server, *address2* is the next most preferred server, and so on).

Syntax [**no**] **netbios-name-server** *address* [*address2...address8*]

Default none

Mode DHCP Pool Config

netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. The *type* variable specifies the NetBIOS node type. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed

- h-node—Hybrid (recommended)

The **no** version of this command removes the NetBIOS node type.

Syntax **netbios-node-type** *type*

Default none

Mode DHCP Pool Config

next-server

This command configures the next server in the boot process of a DHCP client.

Address is the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

The **no** version of this command removes the boot server list.

Syntax **next-server** *address*

no next-server

Default If the **next-server** command is not used to configure a boot server list, the DHCP Server uses inbound interface helper addresses as boot servers.

Mode DHCP Pool Config

option

The command configures DHCP Server options. *Code* specifies the DHCP option code. Ascii string specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. **Hex string** specifies hexadecimal data. in hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.

Example: **a3:4f:22:0c** / **a3 4f 22 0c** / **a34f.220c.9fed** The *address* specifies an IP address.

The **no** version of this command removes the options.

Syntax **option** *code* {**ascii string** | **hex string1** [*string2...string8*] | **ip address1** [*address2...address8*] }

no option code

Default none

Mode DHCP Pool Config

service dhcp

This command enables the DHCP server and relay agent features on the router.

The **no** version of this command disables the DHCP server and relay agent features.

Syntax **service dhcp**

Default disabled

Mode Global Config

show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Syntax **show ip dhcp binding** [*address*]

Mode Privileged Exec and User Exec

IP address—The IP address of the client.

Hardware Address—The MAC Address or the client identifier.

Lease expiration—The lease expiration time of the IP Address assigned to the client.

Type—The manner in which IP Address was assigned to the client.

show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Syntax **show ip dhcp global configuration**

Mode Privileged Exec and User Exec

Service DHCP—The field to display the status of dhcp protocol.

Number of Ping Packets—The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.

Excluded Address—The ranges of IP addresses that a DHCP server should not assign to DHCP clients.

show ip dhcp pool configuration

This command displays pool configuration. If **all** is specified, configuration for all the pools is displayed.

Syntax **show ip dhcp pool configuration** {*name* | **all**}

Mode Privileged Exec and User Exec

Pool Name—The name of the configured pool.

Pool Type—The pool type.

Lease Time—The lease expiration time of the IP Address assigned to the client.

DNS Servers—The list of DNS servers available to the DHCP client

Default Routers—The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Network—The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Client Name—The name of a DHCP client.

Client Identifier—The unique identifier of a DHCP client.

Hardware Address—The hardware address of a DHCP client.

Hardware Address Type—The protocol of the hardware platform.

Host—The IP address and the mask for a manual binding to a DHCP client.

show ip dhcp server statistics

This command displays DHCP server statistics.

Syntax **show ip dhcp server statistics**

Mode Privileged Exec and User Exec

Address Pool—The number of configured address pools in the DHCP server.

Automatic Bindings—The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.

Manual Bindings—The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.

Expired Bindings—The number of expired leases.

Malformed Bindings—The number of truncated or corrupted messages that were received by the DHCP server.

Messages Received

DHCPREQUEST—The number of DHCPREQUEST messages that were received by the server.

DHCPDECLINE—The number of DHCPDECLINE messages that were received by the server.

DHCPRELEASE—The number of DHCPRELEASE messages that were received by the server.

DHCPINFORM—The number of DHCPINFORM messages that were received by the server.

Messages Sent

DHCPOFFER— The number of DHCPOFFER messages that were sent by the server.

DHCPACK—The number of DHCPACK messages that were sent by the server.

DHCPNACK—The number of DHCPNACK messages that were sent by the server.

show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Syntax **show ip dhcp conflict** [*ip-address*]

Mode Privileged Exec and User Exec

IP address—The IP address of the host as recorded on the DHCP server.

Detection Method—The manner in which the IP address of the hosts were found on the DHCP Server

Detection time—The time when the conflict was found.

This section provides a detailed explanation of the Simple Network Time Protocol (SNTP) commands. The commands are comprised of two functional groups:

- Configuration Commands configure features and options of the switch.
- Show commands display settings, statistics, and other information. For every configuration command there is a show command that displays the configuration setting.

This chapter describes the following commands:

- [sntp broadcast client poll-interval](#)
- [sntp client mode on page 216](#)
- [sntp client port on page 216](#)
- [sntp unicast client poll-interval on page 217](#)
- [sntp unicast client poll-timeout on page 217](#)
- [sntp unicast client poll-retry on page 217](#)
- [sntp server on page 218](#)
- [show sntp on page 218](#)
- [show sntp client on page 219](#)
- [show sntp server on page 220](#)

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 16.

Syntax `sntp broadcast client poll-interval poll-interval`

Use the **no sntp broadcast client poll-interval** version of this command to reset the poll interval for SNTP broadcast client back to its default value.

Default 6

Mode Global Config

sntp client mode

This command enables the Simple Network Time Protocol (SNTP) client, and optionally sets the mode to either broadcast or unicast.

Syntax	sntp client mode [broadcast unicast]	
	Use the no sntp client mode command to disable SNTP client mode.	
Parameters	broadcast	SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet-wide scope.
	unicast	SNTP operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
Default	Disabled (No SNTP requests are sent from the client, nor are any received SNTP messages processed.)	
Mode	Global Config	

sntp client port

This command sets the SNTP client port ID to a value from 1–65535.

Syntax	sntp client port <i>portid</i> [<i>poll-interval</i>]	
Parameters	<i>portid</i>	Specify the local UDP port to listen for responses/broadcasts. The allowed range is (1 to 65535). Default value is 123.
	<i>poll-interval</i>	Optionally, set the poll interval for the client in seconds, as a power of two, in the range from 6 to 10. Default value is 6. This setting is true for both unicast and broadcast poll requests. Broadcasts received prior to the expiry of this interval are discarded.
	Use the no sntp client port command to reset the SNTP client port to its default values.	
Default	123	
Usage	You can also set the poll interval for a unicast client with the sntp unicast client poll-interval command.	
Mode	Global Config	

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where *poll-interval* can be a value from 6 to 16.

Syntax **sntp unicast client poll-interval** *poll-interval*

Use the **no sntp unicast client poll-interval** command to reset the poll interval for SNTP unicast clients to its default.

Usage You can also set the poll interval for an SNTP client with the **sntp client port** command.

Default 6

Mode Global Config

sntp unicast client poll-timeout

This command sets the number of seconds to wait for an SNTP response when the client is configured in unicast mode.

Syntax **sntp unicast client poll-timeout** *poll-timeout*

The *poll-timeout* range is 1 to 30 seconds.

Use the **no sntp unicast client poll-timeout** command to reset the poll timeout for SNTP unicast clients to its default value.

Default 5 seconds

Mode Global Config

sntp unicast client poll-retry

This command sets the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode.

Syntax **sntp unicast client poll-retry** *poll-retry*

The *poll-retry* for SNTP unicast clients is an integer from 0 to 10 retries.

Use the **no sntp unicast client poll-retry** version of this command to reset the poll retry for SNTP unicast clients to its default value.

Default	1 retry
Mode	Global Config

sntp server

This command configures an SNTP server connection (with a maximum of three).

Syntax **sntp server** *ipaddress* [*priority* [*version* [*portid*]]]

Parameters	<i>ipaddress</i>	Specify either the IPv4 address of the server or a DNS hostname. If DNS, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
	<i>priority</i>	Optionally, specify the priority of this server entry in determining the sequence of servers to which SNTP requests will be sent. The client continues sending requests to different servers until a successful response is received or all servers are exhausted. A server entry with a priority of 1 is queried before a server with a priority of 2, and then a server with a priority of 3. If more than one server has the same priority then the requesting order follows the lexicographical ordering of the entries in this table. Allowed range is 1 to 3. Default value is 1.
	<i>version</i>	If <i>priority</i> is specified, optionally identify the NTP version running on the server. Allowed range is (1 to 4). Default value is 4.
	<i>portid</i>	The the port ID a value of 1–65535.

Use the **no sntp server remove** *ipaddress* command to delete the server from the list of SNTP servers.

Mode Global Config

show sntp

This command is used to display SNTP settings and status.

Syntax **show sntp**

Mode Privileged Exec

Example

```

Forcel0# show sntp
Last Update Time:                AUG 20 09:04:15 2006
Last Unicast Attempt Time:       AUG 20 09:04:15 2006
Last Attempt Status:             Success

Broadcast Count:                 0

Forcel0#

```

Figure 47 show sntp Command Example

Field Descriptions	Last Update Time—Time of last clock update
	Last Attempt Time—Time of last transmit query (in unicast mode).
	Last Attempt Status—Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
	Broadcast Count—Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
	Multicast Count—Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot

show sntp client

This command is used to display SNTP client settings.

Syntax **show sntp client**

Mode Privileged Exec

Example

```
Force10# show sntp client
Client Supported Modes:          unicast broadcast
SNTP Version:                   4
Port:                           123
Client Mode:                     disabled
Force10#
```

Figure 48 show sntp client Command Example

Field Descriptions	Client Supported Modes—Supported SNTP Modes (broadcast and/or unicast)
	SNTP Version—The highest SNTP version the client supports
	Port—SNTP Client Port
	Client Mode—Configured SNTP Client Mode
	Poll Interval—If enabled, the poll interval value for SNTP clients in seconds as a power of two
	Poll Timeout—If enabled, the poll timeout value in seconds for SNTP clients
	Poll Retry—If enabled, the poll retry value for SNTP clients

show sntp server

This command is used to display SNTP server settings and configured servers.

Syntax **show sntp server**

Mode Privileged Exec

Example

```

Forcel0# show sntp server

Server IP Address:
Server Type:                unknown
Server Stratum:             0
Server Reference Id:
Server Mode:                 Reserved
Server Maximum Entries:     3
Server Current Entries:     0

No SNTP Servers exist.

Forcel0#

```

Figure 49 show sntp server Command Example

Field Descriptions

Server IP Address—IP address of configured SNTP server

Server Type—Address type of server

Server Stratum—Claimed stratum of the server for the last received valid packet

Server Reference ID—Reference clock identifier of the server for the last received valid packet

Server Mode—SNTP server mode

Server Max Entries—Total number of SNTP Servers allowed

Server Current Entries—Total number of SNTP configured

For each configured server:

IP Address—IP Address of configured SNTP Server

Address Type—Address Type of configured SNTP server

Priority—IP priority type of the configured server

Version—SNTP version number of the server. The protocol version used to query the server in unicast mode

Port—Server port number

Last Attempt Time—Last server attempt time for the specified server

Last Attempt Status—Last server attempt status for the server

Total Unicast Requests—Number of requests to the server

Failed Unicast Requests—Number of failed requests from server

VLAN-Stack commands, also called *Double VLAN tagging*, *QinQ*, and *VLAN tunneling*. With this feature, you can “stack” VLANs into one tunnel and switch them through the network. The commands in this chapter, in order, are:

- [dvlan-tunnel ethertype on page 221](#)
- [mode dot1q-tunnel on page 222](#)
- [mode dvlan-tunnel on page 222](#)
- [show dot1q-tunnel on page 223](#)
- [show dvlan-tunnel on page 224](#)

dvlan-tunnel ethertype

This command configures the etherType for all VLAN-Stack interfaces on the system.

Syntax `dvlan-tunnel ethertype {802.1Q | vman | custom 0-65535}`

The etherType may have the values of **802.1Q**, **vman**, or **custom**. For **custom**, the value of the etherType must be set to a number from 0 to 65535.

The **no** version of this command sets the etherType for the specified interface to the default.

Default **vman**

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

Command History

Version 2.3	Interface Range mode added
-------------	----------------------------

Web User Interface

Double VLAN Tunneling (The Double VLAN Tunneling panel is the SFTOS Web Interface panel with similar functionality. Access it in the node tree through **System >> Port >> Double VLAN Tunneling**.)

Related Commands

interface range	Defines an interface range and accesses the Interface Range mode
show dot1q-tunnel	Displays the configured etherType and other information about Double VLAN Tunneling for a specified interface or for all interfaces.
show dvlan-tunnel	same as above

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled. This command performs the same function as **mode dvlan-tunnel**.

The **no** version of this command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Syntax	mode dot1q-tunnel
Default	disabled
Mode	Interface Config
Web User Interface	Double VLAN Tunneling
Usage Information	By default, all ports become core ports. To configure a particular port as an access port, enable DVLAN tagging in Interface Config mode for that port with this command.
Related Commands	show dot1q-tunnel Displays information about Double VLAN Tunneling for a specified interface or for all interfaces.
	show dvlan-tunnel same as above.

mode dvlan-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled. This command performs the same function as **mode dot1q-tunnel**.

The **no** version of this command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Syntax	mode dvlan-tunnel
Default	disabled
Mode	Interface Config
Web User Interface	Double VLAN Tunneling
Usage Information	By default, all ports become core ports. To configure a particular port as an access port, enable DVLAN tagging in Interface Config mode for that port with this command.

Related Commands	show dot1q-tunnel	Displays information about Double VLAN Tunneling for a specified interface or for all interfaces.
	show dvlan-tunnel	same as above

show dot1q-tunnel

This command displays whether an interface is enabled for Double VLAN Tunneling, along with the system-configured etherType and detailed information about Double VLAN Tunneling for the specified interface, or a list of interfaces and their tunneling status. This command performs the same function as **show dvlan-tunnel**.

Syntax	show dot1q-tunnel [interface { <i>unit/slot/port</i> all }]	
Parameters	interface { <i>unit/slot/port</i> all }	Enter the interface keyword followed by either a specific address in the form of <i>unit/slot/port</i> or enter the word all . Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.
Mode	Privileged Exec and User Exec	
Web User Interface	Double VLAN Tunneling Summary (This S50 Web Interface panel has similar functionality. Access it in the node tree through System >> Port >> Double VLAN Tunneling.)	
Usage Information	The following screen capture shows the use of the three ways of using the command—without the interface keyword and with the keyword followed by a port number or all .	

Example

```
(S2410) >show dot1q-tunnel ?
<cr>                               Press Enter to execute the command.
interface                             Enter interface.

(S2410) >show dot1q-tunnel
Interfaces Enabled for DVLAN Tunneling..... None

(S50-8) >show dot1q-tunnel interface 1/0/1
Interface Mode      EtherType
-----
1/0/1      Disable 802.1Q

(S50-8) >show dot1q-tunnel interface all
Interface Mode      EtherType
-----
1/0/1      Disable 802.1Q
1/0/2      Disable 802.1Q
1/0/3      Disable 802.1Q
1/0/4      Disable 802.1Q
1/0/5      Disable 802.1Q
1/0/6      Disable 802.1Q
1/0/7      Disable 802.1Q
1/0/8      Disable 802.1Q
1/0/9      Disable 802.1Q
1/0/10     Disable 802.1Q
! [truncated]!
```

Related Commands	dvlan-tunnel etherType	Configures the etherType for all vlan-stack (Double VLAN tagging) interfaces on the system.
	mode dot1q-tunnel	Enable Double VLAN Tunneling on the specified interface.
	mode dvlan-tunnel	same as above

show dvlan-tunnel

This command displays whether an interface is enabled for Double VLAN Tunneling, along with the system-configured etherType and detailed information about Double VLAN Tunneling for the specified interface, or a list of interfaces and their tunneling status. This command performs the same function as **show dot1q-tunnel**.

Syntax	show dvlan-tunnel [interface { <i>unit/slot/port</i> all }]	
Parameters	interface { <i>unit/slot/port</i> all }	Enter the interface keyword followed by either a specific address in the form of <i>unit/slot/port</i> or enter the word all . Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.
Mode	Privileged Exec and User Exec	
Web User Interface	Double VLAN Tunneling Summary (This S50 Web Interface panel has similar functionality. Access it in the node tree through System >> Port >> Double VLAN Tunneling.)	
Related Commands	dvlan-tunnel etherType	Configures the etherType for all vlan-stack (Double VLAN tagging) interfaces on the system.
	mode dot1q-tunnel	Enable Double VLAN Tunneling on the specified interface.
	mode dvlan-tunnel	same as above

This chapter provides a detailed explanation of the General Attribute Registration Protocol (GARP) commands, including GVRP and GMRP commands. The commands are divided into two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

The sections in this chapter are:

- [GARP Commands on page 225](#)
- [GARP VLAN Registration Protocol \(GVRP\) Commands on page 228](#)
- [GARP Multicast Registration Protocol \(GMRP\) Commands on page 231](#)

GARP Commands

The commands in this sections are:

- [set garp timer join on page 225](#)
- [set garp timer leave on page 226](#)
- [set garp timer leaveall on page 227](#)
- [show garp on page 227](#)

set garp timer join

This command sets the GVRP join time per port and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group.

This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). the value 20 centiseconds is 0.2 seconds.

Syntax **set garp timer join** 10-100

no set garp timer join

The **no** version of this command sets the GVRP join time per port and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

Default 20 centiseconds

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

Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode


set garp timer leave

This command sets the GVRP leave time per port. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service.time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds.

Syntax **set garp timer leave** 20-600

Use **no set garp timer leave** to set the GVRP leave time per port to 60 centiseconds (0.6 seconds).

Default 60

 **Note:** This command has an effect only when GVRP is enabled.

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

Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated per port. A *Leave All PDU* indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds.

Syntax `set garp timer leaveall 200-6000`

Use **no set garp timer leaveall** to set how frequently *Leave All PDUs* are generated per port to 1000 centiseconds (10 seconds).



Note: This command has an effect only when GVRP is enabled.

Default 1000

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

Command History	Version 2.3	Interface Range mode added
	interface range	Defines an interface range and accesses the Interface Range mode
Related Commands		

show garp

This command displays Generic Attributes Registration Protocol (GARP) information.

Syntax `show garp`

Mode Privileged Exec and User Exec

GMRP Admin Mode—This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.

GVRP Admin Mode—This displays the administrative mode of GARP VLAN Registration Protocol (GVRP) for the system

GARP VLAN Registration Protocol (GVRP) Commands

This section provides a detailed explanation of the GVRP commands:

- [gvrp adminmode enable on page 228](#)
- [gvrp interfacemode enable on page 228\]](#)
- [gvrp interfacemode enable all on page 229](#)
- [set gvrp adminmode on page 229](#)
- [set gvrp interfacemode on page 229](#)
- [set gvrp interfacemode all on page 229](#)
- [show gvrp configuration on page 229](#)

gvrp adminmode enable

This command enables GVRP globally.

Syntax **gvrp adminmode enable**

Use **no gvrp adminmode enable** to disable GVRP.

Default disabled

Mode Global Config

Command History	Version 2.3	Changed from set gvrp interfacemode ; revised syntax.
------------------------	-------------	--

gvrp interfacemode enable

This command enables GVRP (GARP VLAN Registration Protocol) for a specific port.

Syntax **gvrp interfacemode enable**

Use **no gvrp interfacemode enable** to disable GVRP (GARP VLAN Registration Protocol) for a specific port. If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Default disabled

Mode Interface Config

Command History	Version 2.3	Changed from set gvrp interfacemode
------------------------	-------------	--

gvrp interfacemode enable all

This command enables GVRP (GARP VLAN Registration Protocol) for all ports.

Syntax **set gvrp interfacemode enable all**

Use **no set gvrp interfacemode enable all** to disable GVRP for all ports. If GVRP is disabled, Join Time, Leave Time, and Leave All Time have no effect.

Default disabled

Mode Global Config

Command History	Version 2.3	Changed from set gvrp interfacemode all
------------------------	-------------	--

set gvrp adminmode

Command History	Version 2.3	Changed to gvrp adminmode enable
------------------------	-------------	---

set gvrp interfacemode

This command enables GVRP (GARP VLAN Registration Protocol) for a specific port.

Mode Interface Config

Command History	Version 2.3	Changed to gvrp interfacemode enable
------------------------	-------------	---

set gvrp interfacemode all

Command History	Version 2.3	Changed to gvrp interfacemode enable all
------------------------	-------------	---

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

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

Mode Privileged Exec and User Exec

Example

```
(Forcel0_S50) #show gvrp configuration 0/1
Interface      Join      Leave      LeaveAll      Port
                Timer      Timer      Timer          GVRP Mode
                (centisecs) (centisecs) (centisecs)
-----
0/1            20         60         1000          Disabled

Forcel0-S50 #show gvrp configuration all
Interface      Join      Leave      LeaveAll      Port
                Timer      Timer      Timer          GVRP Mode
                (centisecs) (centisecs) (centisecs)
-----
0/1            20         60         1000          Disabled
0/2            20         60         1000          Disabled
0/3            20         60         1000          Disabled
0/4            20         60         1000          Disabled
0/5            20         60         1000          Disabled
0/6            20         60         1000          Disabled
0/7            20         60         1000          Disabled
0/8            20         60         1000          Disabled
0/9            20         60         1000          Disabled
0/10           20         60         1000          Disabled
!-----output truncated-----!
```

Figure 50 show gvrp configuration Command Output Example

Interface Valid unit, slot and port number separated by forward slashes.

Join Timer—Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Leave Timer—Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

LeaveAll Timer—This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Port GMRP Mode—Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

Port GVRP Mode—Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

GARP Multicast Registration Protocol (GMRP) Commands

This section provides details on GMRP commands. The commands in this sections are:

- [gmrp adminmode on page 231](#)
- [set gmrp adminmode on page 232](#)
- [gmrp interfacemode enable all on page 232](#)
- [set gmrp interfacemode all on page 233](#)
- [show gmrp configuration on page 233](#)
- [show mac-address-table gmrp on page 234](#)

GARP Multicast Registration Protocol (GMRP)

- GMRP propagates group membership throughout a network.
- GMRP allows end stations and SFTOS Switching devices to issue and revoke declarations relating to group membership.
- (De)registration updates the Multicast Forwarding Database—multicast packets only forwarded through ports with a GMRP registration.
- GMRP is disabled by default—user must enable GMRP for the switch and then for individual ports.
- GMRP is part of the SFTOS Switching package and:
 - Interacts with the Spanning Tree Protocol, GARP, and the Multicast Forwarding Database
 - Requires Independent VLAN Learning
- There is an instance of GMRP for each VLAN.
- MAC addresses are qualified by the 2-byte VLAN ID.
- SFTOS GMRP complies with:
 - IEEE 802.1D Clause 10
 - GMRP port configuration and status table from RFC 2674
- SFTOS limitations:
 - Default filtering behavior is not supported.
 - Static entries are not coordinated.

gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system. The default value is disable.

Syntax **gmrp adminmode enable**

Use **no gmrp adminmode enable** to disable GARP Multicast Registration Protocol (GMRP) on the system.

Mode	Global Config
Command History	Version 2.3 Changed from set gmrp adminmode . Modified syntax and moved to Global Config mode from Privileged Exec mode.

set gmrp adminmode

Command History	Version 2.3 Changed to gmrp adminmode .
------------------------	---

gmrp interfacemode enable all

This command enables GARP Multicast Registration Protocol on all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Syntax	gmrp interfacemode enable all
	Use no gmrp interfacemode enable all to disable GARP Multicast Registration Protocol on all interfaces.
Default	disabled
Mode	Global Config
Command History	Version 2.3 Changed from set gmrp interfacemode all ; revised syntax.

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default disabled

Syntax **set gmrp interfacemode**

Use **no set gmrp interfacemode** to disable GARP Multicast Registration Protocol on a selected interface. If an interface that has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Mode Interface Config

set gmrp interfacemode all

Command History

Version 2.3	Changed to gmrp interfacemode all .
-------------	--

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

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

Mode Privileged Exec and User Exec

Interface—This displays the *unit/slot/port* of the interface that is described in this row of the table.

Join Timer—Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Leave Timer—Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

LeaveAll Timer—This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).

Port GMRP Mode—Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

Port GVRP Mode—Indicates the GVRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

show mac-address-table gmrp

This command displays the GARP Multicast Registration Protocol (GMRP) entries in the Multicast Forwarding Database (MFDB) table.

Syntax **show mac-address-table gmrp**

Mode Privileged Exec

Mac Address—A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In a system the MAC address will be displayed as 8 bytes.

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

Description—The text description of this multicast table entry.

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



Note: The current S2410 hardware does not support IGMP Snooping, so the commands in this chapter appear in the CLI but do not function.

This chapter provides a detailed explanation of the following IGMP Snooping commands:

- [igmp enable \(interface\) on page 236](#)
- [igmp enable \(global\) on page 236](#)
- [igmp fast-leave \(interface\) on page 237](#)
- [igmp groupmembership-interval \(interface\) on page 237](#)
- [igmp interfacemode enable all on page 238](#)
- [igmp maxresponse on page 238](#)
- [igmp mcrtextpiretime \(interface\) on page 239](#)
- [igmp mrouter \(interface\) on page 240](#)
- [igmp mrouter interface enable on page 240](#)
- [set igmp \(interface\) on page 241](#)
- [set igmp \(system\) on page 241](#)
- [set igmp fast-leave on page 241](#)
- [set igmp groupmembership-interval \(global\) on page 241](#)
- [set igmp groupmembership-interval \(interface\) on page 242](#)
- [set igmp interface on page 242](#)
- [set igmp interfacemode all on page 242](#)
- [set igmp maxresponse \(global\) on page 243](#)
- [set igmp maxresponse \(interface\) on page 243](#)
- [set igmp mcrtextpiretime \(global\) on page 244](#)
- [set igmp mcrtextpiretime \(interface\) on page 244](#)
- [set igmp mrouter on page 245](#)
- [show igmpsnooping on page 245](#)
- [show igmpsnooping fast-leave on page 246](#)
- [show igmpsnooping mrouter interface on page 246](#)
- [show mac-address-table igmpsnooping on page 247](#)


igmp enable (interface)

This command enables IGMP Snooping on a selected interface. If an interface that has IGMP Snooping enabled is enabled for routing or is enlisted as a member of a LAG (port channel), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or LAG membership is removed from that interface.

Syntax	[no] igmp enable
Default	disabled
Mode	Interface Config; Interface VLAN
Command History	Version 2.3 Revised from set igmp . Added Interface VLAN mode.
Related Commands	igmp enable (global) This command enables IGMP Snooping on the system. show igmpsnooping Displays IGMP Snooping status.

igmp enable (global)

This command enables IGMP Snooping on the system. The default value is disabled.

	<p>Note: The IGMP application supports the following:</p> <ul style="list-style-type: none"> • Global configuration or per interface configuration. Per-VLAN configuration is unsupported in the IGMP Snooping application. • Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error. • Maintenance of the forwarding table entries based on the MAC address versus the IP address. • Flooding of unregistered multicast data packets to all ports in the VLAN.
---	--

Syntax	[no] igmp enable
Default	disabled
Mode	Global Config
Command History	Version 2.3 Changed from set igmp (system)
Related Commands	igmp enable (interface) This command enables IGMP Snooping on a selected interface. show igmpsnooping Displays IGMP Snooping status.

igmp fast-leave (interface)

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

Fast-leave admin mode should be enabled only on VLANs where only one host is connected to each Layer 2 LAN port, to prevent the inadvertent dropping of the other hosts that were connected to the same Layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP v. 2 hosts.

Syntax	[no] igmp fast-leave					
	The no version of this command disables IGMP Snooping fast-leave admin mode on a selected interface.					
Default	disable					
Mode	Interface Config; Interface VLAN					
Command History	<hr/> Version 2.3 Revised from set igmp fast-leave . <hr/>					
Related Commands	<hr/> <table> <tr> <td>igmp enable (global)</td> <td>Enables IGMP Snooping on the system.</td> </tr> <tr> <td>show igmpsnooping</td> <td>Displays IGMP Snooping status information.</td> </tr> </table> <hr/>		igmp enable (global)	Enables IGMP Snooping on the system.	show igmpsnooping	Displays IGMP Snooping status information.
igmp enable (global)	Enables IGMP Snooping on the system.					
show igmpsnooping	Displays IGMP Snooping status information.					

igmp groupmembership-interval (interface)

This command sets the IGMP Group Membership Interval time on a particular interface. The group membership interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.

Syntax **igmp groupmembership-interval 2-3600**

The variable must be greater than the IGMPv3 maximum response time value. The range is 2 to 3600 seconds.

The **no igmp groupmembership-interval** command sets the IGMP v3 group membership interval time on the interface to the default value.

Default 260 seconds

Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#; Interface VLAN.	
Command History	Version 2.3	Modified: Revised from set igmp groupmembership-interval . Added Interface Range mode.
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	set igmp groupmembership-interval (global)	Sets the IGMP Group Membership Interval time globally.
	interface range	Defines an interface range and accesses the Interface Range mode
	interface	Identifies an interface and enters the Interface Config mode.
	igmp maxresponse	Sets the IGMP Maximum Response time on a selected interface.
	show igmpsnooping	Displays IGMP Snooping status information.

igmp interfacemode enable all

This command enables IGMP Snooping on all interfaces. If an interface that has IGMP Snooping enabled is enlisted as a member of a LAG (port channel), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will be subsequently re-enabled if LAG membership is removed from that interface.

Syntax	[no] igmp interfacemode enable all	
	The no version of this command disables IGMP Snooping on all interfaces.	
Default	disabled	
Mode	Global Config	
Command History	Version 2.3	Changed from set igmp interfacemode all
Related Commands	igmp enable (interface)	This command enables IGMP Snooping on a selected interface.
	show igmpsnooping	Displays IGMP Snooping status.

igmp maxresponse

This command sets the IGMP maximum response time on a selected port or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface.

Syntax	igmp maxresponse <i>1-3599</i>	
	The variable must be less than the IGMP query interval time value. The range is 1 to 3599 seconds.	
	The no igmp maxresponse command sets the IGMP Maximum Response time on the interface to the default value.	
Default	10 seconds	
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#; Interface VLAN.	
Command History	Version 2.3	Modified: Revised from set igmp maxresponse . Added Interface Range mode and Interface VLAN mode.
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	interface	Identifies an interface and enters the Interface Config mode.
	interface vlan	Identifies a VLAN and enters the Interface VLAN mode.
	set igmp maxresponse (global)	Sets the IGMP maximum response time globally.
	show igmpsnooping	Displays IGMP Snooping status information.

igmp mcrtexpiretime (interface)

This command sets the Multicast router present expiration time on a particular interface.

Syntax	[no] igmp mcrtexpiretime <i>0-3600</i>	
	The variable is the amount of time in seconds that a switch will wait for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.	
	The no igmp mcrtexpiretime command sets the Multicast Router Present Expiration time on the interface to 0. A value of 0 indicates an infinite timeout, i.e. no expiration.	
Default	0	
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#; Interface VLAN.	
Command History	Version 2.3	Modified: Revised from set igmp mcrtexpiretime . Added Interface Range mode and Interface VLAN mode.

Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	set igmp mcrctexpiretime (global)	sets the Multicast router present expiration time for all routers.
	interface range	Defines an interface range and accesses the Interface Range mode
	show igmpsnooping	Displays IGMP Snooping status information.
	show igmpsnooping	Displays IGMP Snooping status information.

igmp mrouter (interface)

This command configures the VLAN ID (*vlanId*) that has the multicast router mode enabled.

Syntax `[no] igmp mrouter vlanId`

The **no** version of this command disables multicast router mode for a particular VLAN ID (*vlanId*).

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

Command History	Version 2.3	Modified: Revised from set igmp mrouter . Added Interface Range mode.
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	interface	Identifies an interface and enters the Interface Config mode.

igmp mrouter interface enable

This command configures a selected interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Syntax `[no] igmp mrouter interface enable`

The **no** version of this command disables the status of the interface as a statically configured multicast router interface.

Default disable

Mode Interface Config

Command History	Version 2.3	Revised from set igmp mrouter interface .
------------------------	-------------	--

Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
-------------------------	---	--

set igmp (interface)

Command History	Version 2.3	Revised to igmp (interface) .
------------------------	-------------	--------------------------------------

Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
-------------------------	---	--

set igmp (system)

Command History	Version 2.3	Changed to igmp enable (global)
------------------------	-------------	---

Related Commands	igmp enable (global)	Enables IGMP Snooping on the system.
	igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp fast-leave

Command History	Version 2.3	Revised to igmp fast-leave .
------------------------	-------------	-------------------------------------

Related Commands	igmp fast-leave (interface)	Enables or disables IGMP Snooping fast-leave admin mode on a selected interface.
	igmp enable (global)	Enables IGMP Snooping on the system.

set igmp groupmembership-interval (global)

This command sets the IGMP Group Membership Interval time globally. The group membership interval time is the amount of time in seconds that a switch will wait for a report from a particular group before deleting the interface from the entry.

Syntax `set igmp groupmembership-interval 2-3600`

set igmp groupmembership-interval (interface)

The variable must be greater than the IGMPv3 maximum response time value. The range is 2 to 3600 seconds.

The **no igmp groupmembership-interval** command sets the IGMP v3 group membership interval time globally to the default value.

Default 260 seconds

Mode Global Config

Related Commands

igmp groupmembership-interval (interface)	Sets the IGMP Group Membership Interval time on a particular interface.
igmp enable (interface)	Enables IGMP Snooping on a selected interface.
igmp enable (global)	Enables IGMP Snooping on the system.

set igmp groupmembership-interval (interface)

Command History

Version 2.3	Revised to igmp groupmembership-interval (interface level).
-------------	--

Related Commands

igmp groupmembership-interval (interface)	Sets the IGMP Group Membership Interval time on a particular interface.
igmp enable (interface)	Enables IGMP Snooping on a selected interface.
igmp enable (global)	Enables IGMP Snooping on the system.

set igmp interface

Command History

Version 2.3	Revised to igmp mrouter interface enable .
-------------	---

Related Commands

igmp mrouter interface enable	Enables IGMP Snooping on a selected interface.
igmp enable (global)	Enables IGMP Snooping.

set igmp interfacemode all

Command History

Version 2.3	Changed to igmp interfacemode enable all
-------------	--

Related Commands	igmp interfacemode enable all	Sets the IGMP Group Membership Interval time on a particular interface.
	igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp maxresponse (global)

This command sets the IGMP maximum response time on the system.

Syntax `[no] set igmp maxresponse 1-3599`

The variable is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 3599 seconds.

The **no set igmp maxresponse** command sets the IGMP Maximum Response time on the system to 10 seconds.

Default 10

Mode Global Config

Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	show igmpsnooping	Displays IGMP Snooping status information.

set igmp maxresponse (interface)

Command History	Version 2.3	Revised to igmp maxresponse .
------------------------	-------------	--------------------------------------

Related Commands	igmp maxresponse	Sets the IGMP Maximum Response time on a particular interface.
	igmp enable (interface)	Enables IGMP Snooping on a selected interface.

set igmp mcrtexpiretime (global)

This command sets the Multicast router present expiration time for all routers.

Syntax [no] **set igmp mcrtexpiretime** 0-3600

The variable is the amount of time in seconds that a switch will wait for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite timeout, i.e. no expiration.

The **no igmp mcrtexpiretime** command sets the Multicast Router Present Expiration time on the interface to 0. A value of 0 indicates an infinite timeout, i.e. no expiration.

Default 0

Mode Global Config

Related Commands

igmp enable (interface)	Enables IGMP Snooping on a selected interface.
igmp mcrtexpiretime (interface)	Sets the Multicast router present expiration time on a selected interface.
show igmpsnooping	Displays IGMP Snooping status information.

set igmp mcrtexpiretime (interface)

Command History

Version 2.3	Revised to igmp mcrtexpiretime .
-------------	---

Related Commands

igmp enable (interface)	Enables IGMP Snooping on a selected interface.
igmp mcrtexpiretime (interface)	Sets the Multicast router present expiration time on a selected interface.
set igmp mcrtexpiretime (global)	Sets the Multicast router present expiration time globally.
show igmpsnooping	Displays IGMP Snooping status information.

set igmp mrouter

Command History	Version 2.3	Revised to igmp mrouter .
Related Commands	igmp enable (interface)	Enables IGMP Snooping on a selected interface.
	igmp mrouter (interface)	Configures a selected interface as a multicast router interface.

show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

Syntax **show igmpsnooping** [*unit/slot/port* | 1-3965]

Parameters	<i>unit/slot/port</i>	OPTIONAL Display ports on which Multicast Routers are detected. Enter interface in <i>unit/slot/port</i> format.
	1-3965	OPTIONAL Display VLANS for the specified interface on which Multicast Routers are detected.

Mode Privileged Exec

Command History	Version 2.3	Modified: 1-3965 option added (VLAN ID).
------------------------	-------------	--

Report Fields When **no parameter** is specified, the response contains the following fields:

Admin Mode—Enabled or Disabled

Interfaces Enabled for IGMP Snooping—This is the list of interfaces on which IGMP Snooping is enabled.

Multicast Control Frame Count—This displays the number of multicast control frames that are processed by the CPU.

Vlans enabled for IGMP snooping

When the **optional argument** *unit/slot/port* is used, the response is as follows:

IGMP Snooping Admin Mode—This indicates whether or not IGMP Snooping is active on the interface.

Fast Leave Mode—Disable or Enabled

Group Membership Interval—This is the amount of time a switch will wait for a report for a particular group on a particular interface before it sends a query on that interface. This value may be configured

Max Response Time—This displays the amount of time the switch will wait after sending a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.

Multicast Router Present Expiration Time—If a query is not received on an interface within this amount of time, the interface is removed from the list of interfaces with multicast routers attached. This value may be configured.

When the **optional argument 1-3965** is used, the response is the same as for *unit/slot/port*, except that one more report field is added:

Vlan ID—This echoes the number of the VLAN specified in the parameter.

show igmpsnooping fast-leave

Command History

Version 2.3	Deprecated: Use show igmpsnooping to display whether or not IGMP Snooping is enabled on the designated interface.
-------------	---

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Syntax **show igmpsnooping mrouter interface** { *unit/slot/port* | **vlan 1-3965** }

Parameters	<i>unit/slot/port</i>	Display ports on which Multicast Routers are detected. Enter interface in <i>unit/slot/port</i> format.
	vlan 1-3965	Display VLANS for the specified interface on which Multicast Routers are detected.

Mode Privileged Exec

Report Fields *unit/slot/port*—The port on which multicast router information is being displayed.

Multicast Router Attached—This indicates whether or not multicast router is statically enabled on the interface.

VLAN ID—The list of VLANs of which the interface is a member.

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Syntax **show mac-address-table igmpsnooping**

Mode Privileged Exec

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

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

Description—The text description of this multicast table entry.

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

**Related
Commands**

show mac-address-table	Depending on selected display parameters, displays various Multicast Forwarding Database (MFDB) information.
show mac-addr-table	Displays forwarding database entries

show mac-address-table igmpsnooping

Chapter 15 LAG/Port Channel Commands

This section provides syntax details of the Link Aggregation Group (LAG) commands (802.3ad), also called port channel, port trunking, and other terms. The commands in this chapter are:

- [addport](#)
- [deleteport \(interface config\) on page 250](#)
- [deleteport \(global config\) on page 251](#)
- [port-channel on page 251](#)
- [port-channel enable all \(global\) on page 251](#)
- [port-channel enable \(interface\) on page 252](#)
- [port-channel linktrap on page 252](#)
- [port-channel name on page 253](#)
- [port-channel staticcapability on page 253](#)
- [port lacpmode on page 253](#)
- [port lacpmode enable all on page 254](#)
- [port lacptimeout \(global\) on page 254](#)
- [port lacptimeout \(interface\) on page 255](#)
- [show port-channel brief on page 255](#)
- [show port-channel on page 256](#)
- [show port-channel summary on page 257](#)
- [shutdown on page 257](#)

addport

In Interface Config mode for a selected port, this command adds the port to the designated LAG (port channel).



Note: The **addport** command is also available in Interface Config mode for a selected LAG, but the command is non-functional in that context.

In Ethernet Range mode (Interface Range mode for the selected range of physical ports), this command adds the selected ports to the designated LAG.

Syntax **addport** *unit/slot/port*

Specify the LAG ID in its logical slot/port format (e.g., 1/4).

Mode Interface Config; Interface Range (specifically Ethernet Range, which is indicated by the (conf-if-range-et-[interfaces])# prompt, such as (conf-if-range-et-1/0/10-1/0/11)#).

Command History	Version 2.3	Added Interface Range mode
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	deleteport (interface config)	Deletes the selected port from the designated LAG or, in Interface Range mode, the selected range of ports.
	show port-channel	Display the configured LAG names and their IDs. The interface number is specified in logical slot/port format, which displays one (1) as the slot number; the port number is a sequential integer, based on existing LAG numbers when the new LAG is created. Before adding ports to the newly defined LAG, use this command to determine the logical ID that identifies the LAG to use when associating a port with it.

deleteport (interface config)

This command deletes the selected port from the LAG (port channel) or, in Interface Range mode, the selected range of ports.

Syntax **deleteport** *unit/slot/port*

Mode Interface Config; Interface Range (specifically Ethernet Range, which is indicated by the (conf-if-range-et-[interfaces])# prompt, such as (conf-if-range-et-1/0/10-1/0/11)#).

Command History	Version 2.3	Interface Range mode added
Related Commands	show port-channel	Display the configured LAG names and their IDs. The interface number is specified in logical slot/port format, which displays one (1) as the slot number; the port number is a sequential integer, based on existing LAG numbers when the new LAG is created. Before adding ports to the newly defined LAG, use this command to determine the logical ID that identifies the LAG to use when associating a port with it.

deleteport (global config)

This command deletes all configured ports from the LAG (port channel).

Syntax `deleteport {unit/slot/port} all`

Mode Global Config

Related Commands

show port-channel	Display the configured LAG names and their IDs. The interface number is specified in logical slot/port format, which displays one (1) as the slot number; the port number is a sequential integer, based on existing LAG numbers when the new LAG is created. Before adding ports to the newly defined LAG, use this command to determine the logical ID that identifies the LAG to use when associating a port with it.
-----------------------------------	---

port-channel

This command creates a new LAG (port channel) and generates a logical *unit/slot/port* for it.

Syntax `[no] port-channel name`

The *name* field is an alphanumeric string that allows the dash '-' character.

Use **no port-channel** *unit/slot/port* (slot/port format) to delete the designated LAG.

Mode Global Config

Related Commands

port-channel name	Rename a designated LAG, or enter one name for all configured LAGs.
show port-channel	Display the configured LAG names and their IDs. The interface number is specified in logical slot/port format, which displays one (1) as the slot number; the port number is a sequential integer, based on existing LAG numbers when the new LAG is created. Before adding ports to the newly defined LAG, use this command to determine the logical ID that identifies the LAG to use when associating a port with it.
addport	Add a port to a LAG. Ports added to a LAG must be physical ports, not other LAGs.

port-channel enable all (global)

This command enables the administrative mode for all LAGs (port channels).

The **no** version of this command disables all LAGs.

Syntax	[no] port-channel enable all
Mode	Global Config
Command History	<hr/> Version 2.3 Replaced adminmode with enable . <hr/>

port-channel enable (interface)

This command enables the selected port channel (LAG).

The **no** version of this command disables the selected LAG.

Syntax	[no] port-channel enable
Mode	Interface Config; Interface Range (Port Channel Range), which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-po-1/1-1/2)#
Usage	The [no] shutdown command provides the same functionality within both the Interface Config and Port Channel Range modes for the selected LAG(s).
Command History	<hr/> Version 2.3 Replaced adminmode with enable . <hr/>
Related Commands	<hr/> interface Accesses the Interface Config mode for the selected LAG. <hr/> shutdown Enables or disables the selected LAG. <hr/>

port-channel linktrap

This command enables link trap notifications for the LAG (port channel).

The **no** version of this command disables link trap notifications for the LAG.

Syntax **[no] port-channel linktrap {unit/slot/port | all}**

Parameters	<i>unit/slot/ port</i>	Enter the logical ID of a configured LAG (slot/port format, such as 1/4).
	all	Enter all to select all configured LAGs.
Default	enabled	
Mode	Global Config	

port-channel name

This command renames a LAG (port channel) or all LAGs.

Syntax	port-channel name { <i>unit/slot/port</i> all } <i>name</i>	
Parameters	<i>unit/slot/ port</i>	Enter the logical ID of a configured LAG (slot/port format, such as 1/4).
	all	Enter all to select all configured LAGs.
	<i>name</i>	Enter an alphanumeric string up to 15 characters. This name replaces the user-entered name that was associated with the selected LAG when it was created. Or, if all was entered instead of the LAG ID, the entered name replaces the names of all configured LAGs.
Mode	Global Config	
Related Commands	addport	Add a port to a LAG. Ports added to a LAG must be physical ports, not other LAGs.
	port-channel	Create or delete a LAG.
	show port-channel	Display the configured LAG names and their IDs. The interface number is specified in logical slot/port format, which displays one (1) as the slot number; the port number is a sequential integer, based on existing LAG numbers when the new LAG is created. Before adding ports to the newly defined LAG, use this command to determine the logical ID to identify the LAG when associating a port with it.

port-channel staticcapability

Enable/Disable static capability for all LAGs (port channels).

Syntax	[no] port-channel staticcapability
Default	disabled

Mode Global Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port. The **no** version of this command disables Link Aggregation Control Protocol (LACP) on a port.

Syntax **[no] port lacpmode**

Default disabled

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

Command History	Version 2.4	Deprecated. Use [no] port-channel staticcapability .
	Version 2.3	Added Interface VLAN and Interface Range modes.

Related Commands	port-channel staticcapability	Enables static LAGs (port channels) on the device.
-------------------------	---	--

port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports. The **no** version of this command disables Link Aggregation Control Protocol (LACP) on all ports.

Syntax **[no] port lacpmode enable all**

Mode Global Config

Command History	Version 2.4	Deprecated. Use [no] port-channel staticcapability .
	Version 2.3	Revised from [no] port lacpmode all .

Related Commands	port-channel staticcapability	Enables static LAGs (port channels) on the device.
-------------------------	---	--

port lacptimeout (global)

This command sets the Link Aggregation Control Protocol (LACP) timeout on all ports.

The **no** version of this command removes the Link Aggregation Control Protocol (LACP) timeout on all ports.

Syntax	[no] port lacptimeout {short all long all}	
Parameters	short all	Enter short all to select the short timeout setting (3 seconds) for all ports.
	long all	Enter long all to select the long timeout setting (90 seconds) for all ports.
Mode	Global Config	
Related Commands	port lacptimeout (interface)	Set the LACP timeout on the selected port(s).

port lacptimeout (interface)

This command sets the Link Aggregation Control Protocol (LACP) timeout on the selected port.

The **no** version of this command removes the Link Aggregation Control Protocol (LACP) timeout on the selected port.

Syntax	[no] port lacptimeout {short long}	
Parameters	short	Enter short to select the short timeout setting (3 seconds) for the selected ports.
	long	Enter long to select the long timeout setting (90 seconds) for the selected ports.
Mode	Interface Config; Interface Range	
Command History	Version 2.3	Added Interface Range mode.
Related Commands	interface	Accesses the Interface Config mode for the selected interface.
	interface range	Defines an interface range and accesses the Interface Range mode
	port lacptimeout (global)	Set the Link Aggregation Control Protocol (LACP) timeout on ports.

show port-channel brief

This command displays the static capability of all port channels (LAGs) on the device as well as a summary of individual port channels.

Syntax **show port-channel brief**

Mode Privileged Exec and User Exec

Example

```
Force10 S2410 #show port-channel brief
Static Capability: Disabled
Logical Interface Port-Channel Name Link State Mbr Ports Active Ports
-----
1/1 lag1 Up 0/16, 0/17, 0/18, 0/19, 0/20, 0/21, 0/22, 0/23, 0/8, 0/9, 0/5, 0/12
1/2 lag2 Up 0/10, 0/11 0/10, 0/11
```

Figure 51 Example of show port-channel brief Command Output

Static Capability—This field displays whether or not the device has static capability enabled.

For each LAG, the following information is displayed:

Logical Interface—The field displays the logical ID of the LAG.

Port-Channel Name—This field displays the user-assigned name of the LAG.

Link State—This field indicates whether the link is up or down.

Mbr Ports—This field lists the ports that are members of this LAG, in *slot/port* notation.

Active Ports—This field lists the ports that are actively participating in this LAG.

The example in [Figure 51](#) shows two LAGs, with system-assigned IDs of 1/1 and 1/2.

show port-channel

This command displays an overview of all port channels (LAGs) on the switch.

Syntax **show port-channel {LAG_ID | all}**

Mode Privileged Exec

LAG_ID—Valid unit, slot and port number separated by forward slashes.

Lag Name—The name of this port channel (LAG). You may enter any string of up to 15 alphanumeric characters.

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

Admin Mode—May be enabled or disabled. The factory default is enabled.

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

STP Mode—The Spanning Tree Protocol Administrative Mode associated with the port or port channel (LAG). The possible values are:

Disable - Spanning tree is disabled for this port.

Enable - Spanning tree is enabled for this port.

Mbr Ports—A listing of the ports that are members of this port channel (LAG), in *unit/slot/port* notation. There can be a maximum of eight ports assigned to a given port channel (LAG).

Port Speed—Speed of the port channel port.

Type—This field displays the status designating whether a particular port channel (LAG) is statically or dynamically maintained.

Static - The port channel is statically maintained.

Dynamic - The port channel is dynamically maintained.

Active Ports—This field lists the ports that are actively participating in the port channel (LAG).

show port-channel summary

Display the static capability of all LAGs on the device as well as a summary of individual LAGs.

Syntax **show port-channel**

Mode Privileged Exec

Static Capability—whether the device has static capability enabled.

port channel/LAG Summary:

Lag Name—The name of the lag.

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

Mbr Ports—A listing of the ports that are members of this lag, in slot.port notation.

Active Ports—A listing of ports that are actively participating in the LAG.

shutdown

This command disables the selected LAG (port channel).

The **no** version of this command enables the selected LAG.

Syntax [no] shutdown

Default disabled

Mode Interface Config; Interface Range (Port Channel Range), which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-po-1/1-1/2)#.

**Related
Commands**

interface	Defines an interface range and accesses the Interface Range mode
interface range	Identifies an interface and enters the Interface Config mode.
port-channel enable all (global)	Enables [disables] all LAGs.
shutdown (Interface)	Enables [disables] the selected port.

Spanning Tree (STP) Commands

This chapter provides a detailed explanation of the Spanning Tree commands. The commands are divided into two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.



Note: The SFTOS software platform STP default mode is IEEE 802.1s, but the legacy IEEE 802.1D mode is available. To change to the legacy IEEE 802.1D mode, set the STP operational mode to disabled, then enable the IEEE 802.1D mode. With the IEEE 802.1D mode operationally enabled, the rapid configuration and multiple instances features are not available. If the rapid configuration and multiple instances capabilities are required, use the IEEE 802.1s mode which is compatible with the legacy IEEE 802.1D standard.

The chapter describes the following commands:

- [show spanning-tree on page 260](#)
- [show spanning-tree interface on page 261](#)
- [show spanning-tree mst detailed on page 262](#)
- [show spanning-tree mst port detailed on page 262](#)
- [show spanning-tree mst port summary on page 264](#)
- [show spanning-tree mst summary on page 264](#)
- [show spanning-tree summary on page 265](#)
- [show spanning-tree vlan on page 265](#)
- [spanning-tree on page 265](#)
- [spanning-tree bpdumigrationcheck on page 266](#)
- [spanning-tree configuration name on page 266](#)
- [spanning-tree configuration revision on page 266](#)
- [spanning-tree edgeport on page 267](#)
- [spanning-tree forceversion on page 267](#)
- [spanning-tree forward-time on page 268](#)
- [spanning-tree hello-time on page 268](#)

- [spanning-tree max-age on page 269](#)
- [spanning-tree max-hops on page 269](#)
- [spanning-tree mst on page 269](#)
- [no spanning-tree mst on page 270](#)
- [spanning-tree mst instance on page 271](#)
- [spanning-tree mst priority on page 271](#)
- [spanning-tree mst vlan on page 272](#)
- [spanning-tree port mode enable on page 272](#)
- [spanning-tree port mode enable all on page 273](#)

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree, when the optional parameter “brief” is not included in the command. The following details are displayed.

Syntax `show spanning-tree brief`

Mode Privileged Exec and User Exec

Bridge Priority—Specifies the bridge priority for the spanning tree.

Bridge Identifier—The bridge identifier for the selected instance.

Time Since Topology Change—The time in seconds since the topology last changed.

Topology Change Count—Number of times the topology has changed.

Topology Change in progress—Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.

Designated Root—The bridge identifier of the root bridge. It is derived from the bridge priority and the base MAC address of the bridge.

Root Path Cost—Value of the Root Path Cost parameter for the common and internal spanning tree.

Root Port Identifier—Port to access the Designated Root.

Bridge Max Age—Specifies the bridge maximum age for the spanning tree.

Bridge Forwarding Delay—Specifies the time spent in “Listening and Learning” mode before forwarding packets. Bridge Forwarding Delay must be greater or equal to “(Bridge Max Age/2) + 1”. The time range is from 4 seconds to 30 seconds. The default value is 15.

Hello Time—Configured value of the parameter for common spanning tree.

Bridge Hold Time—Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

CST Regional Root—Bridge Identifier of the common spanning tree regional root. It is derived using the bridge priority and the base MAC address of the bridge.

Regional Root Path Cost—Path cost to the common spanning tree Regional Root.

Associated FIDs—List of forwarding database identifiers currently associated with this instance.

Associated VLANs—List of VLAN IDs currently associated with this instance.

When the “brief” optional parameter is included, this command displays spanning tree settings for the bridge. In this case, the following details are displayed.

Bridge Priority—Specifies the bridge priority for the spanning tree.

Bridge Identifier—The bridge identifier for the selected instance.

Bridge Max Age—Specifies the bridge maximum age for the spanning tree.

Hello Time—Configured value of the parameter for the common spanning tree.

Bridge Forwarding Delay—Specifies the time spent in “Listening and Learning” mode before forwarding packets. Bridge Forwarding Delay must be greater or equal to “(Bridge Max Age/2) + 1”. The time range is from 4 seconds to 30 seconds. The default value is 15.

Bridge Hold Time—Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *unit/slot/port* is the desired switch port. The following details are displayed on execution of the command.

Syntax **show spanning-tree interface** *unit/slot/port*

Mode Privileged Exec and User Exec

Port mode—Enabled or disabled.

Port Up Time Since Counters Last Cleared—Time since port was reset, displayed in days, hours, minutes, and seconds.

Hello Time—Configured value of the parameter for common spanning tree.

STP BPDUs Transmitted—Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received—Spanning Tree Protocol Bridge Protocol Data Units received.

RST BPDUs Transmitted—Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RST BPDUs Received—Rapid Spanning Tree Protocol Bridge Protocol Data Units received.

MSTP BPDUs Transmitted—Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received—Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

show spanning-tree mst detailed

This command displays settings and parameters for the specified multiple spanning tree instance. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

Syntax **show spanning-tree mst detailed** *mstid*

Mode Privileged Exec and User Exec

MST Instance ID—The ID of the MST being created.

MST Bridge Priority—The bridge priority for the MST instance selected.

Time Since Topology Change—The time since the topology changed.

Topology Change Count—Number of times the topology has changed for this multiple spanning tree instance.

Topology Change in Progress—Value of the Topology Change parameter for the multiple spanning tree instance.

Designated Root—Identifier of the Regional Root for this multiple spanning tree instance.

Root Path Cost—Path Cost to the Designated Root for this multiple spanning tree instance.

Root Port Identifier—Port to access the Designated Root for this multiple spanning tree instance.

Associated FIDs—List of forwarding database identifiers associated with this instance.

Associated VLANs—List of VLAN IDs associated with this instance.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The *unit/slot/port* is the desired switch port.

Syntax **show spanning-tree mst port detailed** *mstid unit/slot/port*

Mode Privileged Exec and User Exec

MST Instance ID—The ID of the MST instance.

Port Identifier—The port identifier for the specified port within the spanning tree.

Port Priority—The priority for a particular port within the selected MST instance.

Port Forwarding State—Current spanning tree state of this port

Port Role—Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree.

Port Path Cost—Configured value of the Internal Port Path Cost parameter

Designated Root—The Identifier of the designated root for this port.

Designated Port Cost—Path Cost offered to the LAN by the Designated Port

Designated Bridge—Bridge Identifier of the bridge with the Designated Port.

Designated Port Identifier—Port on the Designated Bridge that offers the lowest cost to the LAN.

If 0 (defined as the default CIST ID) is passed as the *mstid*, then this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *unit/slot/port* is the desired switch port. In this case, the following are displayed.

Port Identifier—The port identifier for this port within the CST.

Port Priority—The priority of the port within the CST.

Port Forwarding State—The forwarding state of the port within the CST.

Port Role—The role of the specified interface within the CST.

Port Path Cost—The configured path cost for the specified interface.

Designated Root—Identifier of the designated root for this port within the CST.

Designated Port Cost—Path Cost offered to the LAN by the Designated Port.

Designated Bridge—The bridge containing the designated port

Designated Port Identifier—Port on the Designated Bridge that offers the lowest cost to the LAN

Topology Change Acknowledgement—Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.

Hello Time—The hello time in use for this port.

Edge Port—The configured value indicating if this port is an edge port.

Edge Port Status—The derived value of the edge port status. True if operating as an edge port; false otherwise.

Point To Point MAC Status—Derived value indicating if this port is part of a point to point link.

CST Regional Root—The regional root identifier in use for this port.

CST Port Cost—The configured path cost for this port.

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *mstid* indicates a particular MST instance. The parameter { *unit/slot/port* | **all** } indicates the desired switch port or all ports.

If 0 (defined as the default CIST ID) is passed as the *mstid*, then the status summary is displayed for one or all ports within the common and internal spanning tree.

Syntax **show spanning-tree mst port summary** *mstid* {*unit/slot/port* | **all**}

Mode Privileged Exec and User Exec

Unit/Slot/Port—Valid unit, slot and port number separated by forward slashes.

Type—Currently not used.

STP State—The forwarding state of the port in the specified spanning tree instance

Port Role—The role of the specified port within the spanning tree.

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Syntax **show spanning-tree mst summary**

Mode Privileged Exec and User Exec

MST Instance ID List

List of multiple spanning trees IDs currently configured.

For each MSTID:

Associated FIDs—List of forwarding database identifiers associated with this instance.

Associated VLANs—List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Syntax **show spanning-tree summary**

Mode Privileged Exec and User Exec

Spanning Tree Adminmode—Enabled or disabled.

Spanning Tree Version—Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1D) based upon the Force Protocol Version parameter

Configuration Name—Identifier used to identify the configuration currently being used.

Configuration Revision Level—Identifier used to identify the configuration currently being used.

Configuration Digest Key—Identifier used to identify the configuration currently being used.

MST Instances—List of all multiple spanning tree instances configured on the switch

show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The *vlanid* corresponds to an existing VLAN ID.

Syntax **show spanning-tree vlan *vlanid***

Mode Privileged Exec and User Exec

VLAN Identifier—The VLANs associated with the selected MST instance.

Associated Instance—Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree

spanning-tree

This command sets the spanning-tree operational mode to enabled.

The **no** version of this command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Syntax **[no] spanning-tree**

Default disabled

Mode Global Config

spanning-tree bpdumigrationcheck

This command enables BPDU migration check on a given interface, by using *unit/slot/port*, or all interfaces, by using the **all** keyword.

The **no** version of this command disables BPDU migration check on all interfaces or the designated interface.

Syntax [no] **spanning-tree bpdumigrationcheck** {*unit/slot/port* | **all**}

Mode Global Config

Command History

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

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *name* is a string of at most 32 characters.

The **no** version of this command resets the Configuration Identifier Name to its default.

Syntax [no] **spanning-tree configuration name** *name*

Default The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.

Mode Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

The **no** version of this command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, in other words, 0.

Syntax **spanning-tree configuration revision 0-65535**

Default 0

Mode Global Config

spanning-tree edgeport

This command specifies that this port is an edge port (portfast) within the common and internal spanning tree. This will allow this port to transition to forwarding state without delay.

The **no** version of this command specifies that this port is not an Edge Port within the common and internal spanning tree.

Syntax **[no] spanning-tree edgeport**

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

Command History	Version 2.3	Added Interface Range mode.
Related Commands	interface	Identifies an interface and enters the Interface Config mode.
	interface range	Defines an interface range and accesses the Interface Range mode

spanning-tree forceversion

This command sets the Force 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** version of this command sets the Force Protocol Version parameter to the default value, in other words, 802.1s.

Syntax [no] **spanning-tree forceversion 802.1d | 802.1w | 802.1s**

Default 802.1s

Mode Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to $(\text{Bridge Max Age} / 2) + 1$.

The **no** version of this command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, in other words, 15.

Syntax [no] **spanning-tree forward-time 4-30**

Default 15

Mode Global Config

spanning-tree hello-time

This command sets the Admin Hello Time parameter to a new value for the common and internal spanning tree.

Syntax **spanning-tree hello-time 1-10**

The hellotime value is in whole seconds within a range of 1 to 10 with the value being less than or equal to $(\text{Bridge Max Age} / 2) - 1$.

The **no spanning-tree hello-time** command sets the admin Hello Time parameter for the common and internal spanning tree to the default value.

Default 2

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

Command History	Version 2.3	Added Interface Range mode.
	<hr/>	
Related Commands	interface	Identifies an interface and enters the Interface Config mode.
	interface range	Defines an interface range and accesses the Interface Range mode

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to "2 times (Bridge Forward Delay - 1)".

The **no** version of this command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, in other words, 20.

Syntax **spanning-tree max-age** *6-40*

no spanning-tree max-age

Default 20

Mode Global Config

spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is in a range of 1 to 127.

The **no** version of this command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Syntax **spanning-tree max-hops** *1-127*

[no] spanning-tree max-hops

Default 20

Mode Global Config

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If the *mstid* parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the *mstid*, then the configurations are performed for the common and internal spanning tree instance.

If the “cost” token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. The pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

If the “external-cost” token is specified, this command sets the external-path cost for MST instance “0” in other words, CIST instance. The external pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the external pathcost value will be set based on Link Speed.

If the “port-priority” token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Syntax `spanning-tree mst mstid {{cost 1-200000000 | auto} | port-priority 0-240}`

no spanning-tree mst

Default cost: auto; external-cost: auto; port-priority: 128

Mode Interface Config

**Related
Commands**

[interface](#)

Identifies an interface and enters the Interface Config mode.

[interface range](#)

Defines an interface range and accesses the Interface Range mode

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree to the respective default values. If the *mstid* parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the *mstid*, then the configurations are performed for the common and internal spanning tree instance.

If the “cost” token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value, in other words, a pathcost value based on the Link Speed.

If the “external-cost” token is specified, this command sets the external path cost for this port for mst “0” instance, to the default value, in other words, a pathcost value based on the Link Speed.

If the “port-priority” token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *mstid* parameter, to the default value, in other words, 128.

Syntax **no spanning-tree mst** *mstid* {**cost** | **port-priority**}

Mode Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The instance *mstid* is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by SFTOS is 4.

The **no** version of this command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Syntax **spanning-tree mst instance** *mstid*

[**no**] **spanning-tree mst instance** *mstid*

Mode Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If 0 (defined as the default CIST ID) is passed as the *mstid*, then this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value again is a number within a range of 0 to 61440. The twelve least significant bits will be masked according to the 802.1s specification. This will cause the priority to be rounded down to the next lower valid priority.

The **no** version of this command sets the bridge priority for a specific multiple spanning tree instance to the default value, in other words, 32768. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the *mstid*, then this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, in other words, 32768.

Syntax	spanning-tree mst priority <i>mstid</i> 0-61440
	no spanning-tree mst priority <i>mstid</i>
Default	32768
Mode	Global Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.
Command History	Version 2.3 Added Interface Range mode.
Related Commands	interface Identifies an interface and enters the Interface Config mode.
	interface range Defines an interface range and accesses the Interface Range mode

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN. The VLAN will no longer be associated with the common and internal spanning tree. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The *vlanid* corresponds to an existing VLAN ID.

The **no** version of this command removes an association between a multiple spanning tree instance and a VLAN. The VLAN will again be associated with the common and internal spanning tree. The instance *mstid* is a number that corresponds to the desired existing multiple spanning tree instance. The *vlanid* corresponds to an existing VLAN ID.

Syntax	spanning-tree mst vlan <i>mstid</i> <i>vlanid</i>
	no spanning-tree mst vlan <i>mstid</i> <i>vlanid</i>
Mode	Global Config

spanning-tree port mode enable

This command sets the Administrative Switch Port State for this port to enabled.

The **no** version of this command sets the Administrative Switch Port State for this port to disabled.

Syntax	[no] spanning-tree port mode enable	
Default	disabled	
Mode	Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Modified: Added enable keyword. Added Interface Range and Interface VLAN modes.
Related Commands	interface	Identifies an interface and enters the Interface Config mode.
	interface range	Defines an interface range and accesses the Interface Range mode

spanning-tree port mode enable all

This command sets the Administrative Switch Port State for all ports to enabled.

The **no** version of this command sets the Administrative Switch Port State for all ports to disabled.

Syntax	[no] spanning-tree port mode enable all	
Default	disabled	
Mode	Global Config	
Command History	Version 2.3	Modified: Added enable keyword.

spanning-tree port mode enable all

This chapter provides a detailed explanation of available Quality of Service (QoS) commands. The chapter is divided into the following sections:

- [Class of Service \(CoS\) Commands](#)
- [Differentiated Services \(DiffServ\) Commands on page 285](#)
- [Provisioning \(IEEE 802.1p\) Commands on page 285](#)

Class of Service (CoS) Commands

This section provides a detailed explanation of the QoS CoS commands:

- [classofservice dot1p-mapping on page 276](#)
- [classofservice trust on page 277](#)
- [cos-queue max-bandwidth on page 277](#)
- [cos-queue min-bandwidth on page 278](#)
- [cos-queue random-detect on page 278](#)
- [cos-queue strict on page 279](#)
- [random-detect exponential-weighting-constant on page 279](#)
- [random-detect queue-parms on page 280](#)
- [show classofservice dot1p-mapping on page 281](#)
- [show classofservice trust on page 281](#)
- [show interfaces cos-queue on page 282](#)
- [show interfaces random-detect on page 282](#)
- [show interfaces tail-drop-threshold on page 283](#)
- [tail-drop queue-parms on page 284](#)
- [traffic-shape on page 285](#)

By default, SFTOS 2.4.1 configures all egress queues in weighted round robin mode with equal minimum bandwidths. This means that no egress queue will be 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.

By default, bandwidth is divided into 28 slices (we get 28 by adding 1 through 7—representing seven priority queues), and then it is allocated so that the highest priority queue gets the most bandwidth. When you use a CoS command to assign a priority queue, you set the priority from 0 to 6 (highest priority).



Note: Honoring 802.1p bits is enabled by default. 802.1p honoring can be disabled with **no classofservice trust** (in either Global Config and Interface Config modes).

Table 22 Default CoS Queue Prioritization

Queue	Fraction (%) of Total Bandwidth
0	1/28 (3.57%)
1	2/28 (7.14%)
2	3/28 (10.71%)
3	4/28 (14.28%)
4	5/28 (17.86%)
5	6/28 (21.43%)
6	7/28 (25%)

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class.

Syntax **classofservice dot1p-mapping** *userpriority* *trafficclass*

The *userpriority* range is 0-7.

The *trafficclass* range is 0-3.

The **no** form of this command is not supported.

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

Command History	Version 2.3	Interface Range mode added
Related Commands	classofservice dot1pmapping	Maps an 802.1p priority to an internal traffic class.
	interface range	Defines an interface range and accesses the Interface Range mode
	show classofservice dot1p-mapping	Displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface

classofservice trust

This command sets the class of service trust mode of an interface to Dot1p (802.1p). (The *ip-precedence* and *ip-dscp* options, for IP Precedence and IP DSCP packet markings, are not available in SFTOS 2.4.1.)

Syntax `classofservice trust dot1p`

The **no classofservice trust** command sets the interface mode to untrusted.

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

Command History	Version 2.3	Interface Range mode added
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode

cos-queue max-bandwidth

This command specifies the maximum transmission bandwidth limit for each interface queue. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The total number of queues supported per interface is platform-specific (four queues in the S2410).

Syntax `[no] cos-queue max-bandwidth bw-0...bw-3`

For the variable, *bw* represents bandwidth, and the suffix number represents one of the four S2410 queues. For example, enter 40-3 for a maximum bandwidth of 40% in queue 3.

The **no cos-queue max-bandwidth** command restores the default for each queue's maximum bandwidth value.

Modes	Global Config	
Command History	Version 2.4.1	Introduced
Related Commands	cos-queue min-bandwidth	Specify the minimum transmission bandwidth guarantee for each interface queue.
	traffic-shape	Specify the maximum transmission bandwidth limit for the interface as a whole.

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is platform-specific (four in the S2410).

Syntax **cos-queue min-bandwidth** *bw-0... bw-3*

The **no cos-queue min-bandwidth** command restores the default for each queue's minimum bandwidth value.

Modes	Global Config	
Command History	Version 2.4.1	Modified: Removed Interface Config mode
Related Commands	cos-queue max-bandwidth	Specify the maximum transmission bandwidth guarantee for each interface queue.

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue (up to four in the S2410).

Syntax [**no**] **cos-queue random-detect** *queue-id [queue-id [queue-id [queue-id]]]*

The **no** version of this command disables WRED, thereby restoring the default tail drop operation for the specified queue(s).

Modes Global Config

Usage	Specific WRED parameters are configured using the random-detect queue-parms and random-detect exponential-weighting-constant commands.	
Command History	Version 2.4.1	Modified: Removed Interface Config mode
Related Commands	random-detect exponential-weighting-constant	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.
	show interfaces random-detect	Display the WRED configuration for each supported drop precedence level of each queue for the specified interface.

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue (up to four in the S2410).

Syntax **[no] cos-queue strict** *queue-id* [*queue-id* [*queue-id* [*queue-id*]]]

The **no** version of this command restores the default weighted scheduler mode for each specified queue.

Modes Global Config

random-detect exponential-weighting-constant

Set the decay exponent used by the WRED average queue depth calculation for the interface.

Syntax **[no] random-detect random-detect exponential-weighting-constant** *1-15*

Mode Global Config

Command History	Version 2.4.1	Introduced
Related Commands	random-detect queue-parms	Set the WRED parameters for each drop precedence level supported by a queue.
	show interfaces random-detect	Display the WRED configuration for each supported drop precedence level of each queue for the specified interface.

random-detect queue-parms

This command sets the WRED parameters for each drop precedence level supported by a queue. The actual number of queue drop precedence levels is platform-specific (S2410 has four). Use the **no** form of this command to restore the default values for the queue WRED parameters.

Syntax	[no] random-detect queue-parms <i>queue-id-1</i> [<i>queue-id-2</i> ... <i>queue-id-n</i>] min-thresh 0-16 0-16 0-16 max-thresh 0-16 0-16 0-16 drop-prob-scale 0-15 0-15 0-15	
Parameters	<i>queue-id-1</i> [<i>queue-id-2</i> ... <i>queue-id-n</i>]	Enter a queue ID from 0 to 3. Enter from one ID up to four. Range: 0 to 3
	min-thresh 0-16 0-16 0-16	Enter the keyword min-thresh followed by the desired minimum threshold value for each associated queue (first threshold value is associated with queue 1, etc.). Range: 1 to 16
	max-thresh 0-16 0-16 0-16	Enter the keyword max-thresh followed by the desired maximum threshold value for each associated queue. Range: 1 to 16
	drop-prob-scale 0-15 0-15 0-15	Enter the keyword drop-prob-scale followed by the desired value for each associated queue. See Usage, below. Range: 1 to 15
Mode	Global Config	
Usage	The drop-prob-scale value is the WRED (weighted random early discard) drop probability scale factor expressed as an integer. This value, S, specifies that one out of every (2**S) packets are dropped by WRED when the average queue length reaches its maximum threshold value.	
Command History	Version 2.4.1	Introduced
Related Commands	random-detect exponential-weighting-constant	Set the decay exponent used by the WRED average queue depth calculation for the interface.
	show interfaces random-detect	Display the WRED configuration for each supported drop precedence level of each queue for the specified interface.

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface.

Syntax `show classofservice dot1p-mapping [unit/slot/port]`

The *unit/slot/port* parameter is optional. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Mode Privileged Exec

Report Fields The following information is repeated for each user priority.

User Priority—The 802.1p user priority value

Traffic Class—The traffic class internal queue identifier to which the user priority value is mapped

Example

```

Force10 #show classofservice dot1p-mapping 1/0/1
User Priority      Traffic Class
-----
0                  1
1                  0
2                  0
3                  1
4                  2
5                  2
6                  3
7                  3
  
```

Example of Output from the show mac-addr-table count Command

Related Commands	classofservice	Maps an 802.1p priority to an internal traffic class
	dot1p-mapping	

show classofservice trust

This command displays the current trust mode setting for a specific interface. The *unit/slot/port* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the port trust mode of the interface is displayed. If omitted, the port trust mode of each interface in the system is shown. If the platform does not support independent per-port class of service mappings, the output represents the system-wide port trust mode used for all interfaces.

Syntax `show classofservice trust [unit/slot/port]`

Mode Privileged Exec

Report Fields Non-IP Traffic:

Class—The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to either 'trust ip-dscp' or 'trust ip-precedence'.

Untrusted Traffic Class—The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface.

Syntax **show interfaces cos-queue** [*unit/slot/port*]

The *unit/slot/port* parameter is optional, and , if specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Mode Privileged Exec

Report Fields Interface—This displays the *unit/slot/port* of the interface. If displaying the global configuration, this output line is replaced with a "Global Configuration" indication.

Interface Shaping Rate—The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface.

The following information is repeated for each queue on the interface:

Queue ID—Queue identification number

An interface supports *n* queues numbered 0 to (*n*-1). The specific *n* value is platform dependent.

Min. Bandwidth—The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort.

Scheduler Type—Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme.

Queue Management Type—The queue depth management technique used for all queues on this interface.

show interfaces random-detect

This command displays the weighted random early discard (WRED) configuration for each supported drop precedence level of each queue for the specified interface.

Syntax	show interfaces random-detect <i>slot/port</i>							
	The <i>slot/port</i> parameter is optional. If specified, the class-of-service WRED configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.							
Mode	Privileged Exec							
Report Fields	Interface — This displays the <i>slot/port</i> of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.							
	The following information is repeated for each queue on the interface.							
	Queue IdQueue identification number — An interface supports <i>n</i> queues numbered 0 to (<i>n</i> -1). The number <i>n</i> is platform dependent and corresponds to the number of supported queues (traffic classes).							
	The following information is repeated for each drop precedence level defined for the preceding Queue ID.							
	Drop Precedence Level — The drop precedence level for this queue, from 1 to <i>p</i> . The specific <i>p</i> value is platform-dependent.							
	WRED Minimum Threshold — The WRED minimum threshold value for this drop precedence level, expressed in sixteenths of the overall device queue size (e.g., 0/16, 1/16, 2/16..., 16/16). This is a configured value.							
	WRED Maximum Threshold — The WRED maximum threshold value for this drop precedence level, expressed in sixteenths of the overall device queue size (e.g., 0/16, 1/16, 2/16..., 16/16). This is a configured value.							
	WRED Drop Probability Scale — The WRED drop probability scale factor expressed as an integer. This value, <i>S</i> , specifies that one out of every ($2^{**}S$) packets are dropped by WRED when the average queue length reaches its maximum threshold value. This is a configured value.							
Command History	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Version 2.4.1</th> <th style="text-align: left;">Introduced</th> </tr> </thead> <tbody> <tr> <td>random-detect</td> <td rowspan="2">Set the decay exponent used by the WRED average queue depth calculation for the interface.</td> </tr> <tr> <td>exponential-weighting-constant</td> </tr> <tr> <td>random-detect queue-parms</td> <td>Set the decay exponent used by the WRED average queue depth calculation for the interface.</td> </tr> </tbody> </table>	Version 2.4.1	Introduced	random-detect	Set the decay exponent used by the WRED average queue depth calculation for the interface.	exponential-weighting-constant	random-detect queue-parms	Set the decay exponent used by the WRED average queue depth calculation for the interface.
Version 2.4.1	Introduced							
random-detect	Set the decay exponent used by the WRED average queue depth calculation for the interface.							
exponential-weighting-constant								
random-detect queue-parms	Set the decay exponent used by the WRED average queue depth calculation for the interface.							
Related Commands								

show interfaces tail-drop-threshold

This command displays the tail-drop threshold configuration for each supported drop precedence level of each queue for the specified interface.

Syntax **show interfaces tail-drop-threshold *slot/port***

The *slot/port* parameter is optional. If specified, the tail-drop configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Mode	Privileged Exec				
Report Fields	<p>Interface — This displays the slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.</p> <p>The following information is repeated for each queue on the interface.</p> <p>Queue IdQueue identification number — An interface supports n queues numbered 0 to (n-1). The number n is platform dependent and corresponds to the number of supported queues (traffic classes).</p> <p>The following information is repeated for each drop precedence level defined for the preceding Queue ID.</p> <p>Drop Precedence Level — The drop precedence level for this queue, from 1 to p. The specific pvalue is platform-dependent.</p> <p>Tail Drop Threshold — The tail drop queue threshold value for this drop precedence level, expressed in sixteenths of the overall device queue size (e.g., 0/16, 1/16, 2/16..., 16/16). This is a configured value.</p>				
Command History	<table border="1"> <tr> <td>Version 2.4.1</td> <td>Introduced</td> </tr> </table>	Version 2.4.1	Introduced		
Version 2.4.1	Introduced				
Related Commands	<table border="1"> <tr> <td>random-detect queue-parms</td> <td>Set the decay exponent used by the WRED average queue depth calculation for the interface.</td> </tr> <tr> <td>tail-drop queue-parms</td> <td>sets the tail drop threshold parameter for each drop precedence level supported by a queue (four queues in SFTOS 2.4.1).</td> </tr> </table>	random-detect queue-parms	Set the decay exponent used by the WRED average queue depth calculation for the interface.	tail-drop queue-parms	sets the tail drop threshold parameter for each drop precedence level supported by a queue (four queues in SFTOS 2.4.1).
random-detect queue-parms	Set the decay exponent used by the WRED average queue depth calculation for the interface.				
tail-drop queue-parms	sets the tail drop threshold parameter for each drop precedence level supported by a queue (four queues in SFTOS 2.4.1).				

tail-drop queue-parms

This command sets the tail drop threshold parameter for each drop precedence level supported by a queue (four queues in SFTOS 2.4.1). The **no** form of this command restores the default values for the queue tail drop threshold parameters.

Syntax	[no] tail-drop queue-parms <i>queue-id-1</i> [<i>queue-id-2</i> ... <i>queue-id-n</i>] threshold <i>0-16 0-16 0-16</i>				
Parameters	<table border="1"> <tr> <td><i>queue-id-1</i> [<i>queue-id-2</i> ... <i>queue-id-n</i>]</td> <td>Enter a queue ID from 0 to 3. Enter from one ID up to four. Range: 0 to 3</td> </tr> <tr> <td>threshold <i>0-16 0-16 0-16</i></td> <td>Enter the keyword threshold, followed by the desired threshold for the specified queues. Range: 1 to 16</td> </tr> </table>	<i>queue-id-1</i> [<i>queue-id-2</i> ... <i>queue-id-n</i>]	Enter a queue ID from 0 to 3. Enter from one ID up to four. Range: 0 to 3	threshold <i>0-16 0-16 0-16</i>	Enter the keyword threshold , followed by the desired threshold for the specified queues. Range: 1 to 16
<i>queue-id-1</i> [<i>queue-id-2</i> ... <i>queue-id-n</i>]	Enter a queue ID from 0 to 3. Enter from one ID up to four. Range: 0 to 3				
threshold <i>0-16 0-16 0-16</i>	Enter the keyword threshold , followed by the desired threshold for the specified queues. Range: 1 to 16				
Mode	Global Config and Interface Config				
Command History	<table border="1"> <tr> <td>Version 2.4.1</td> <td>Introduced</td> </tr> </table>		Version 2.4.1	Introduced	
Version 2.4.1	Introduced				
Related Commands	<table border="1"> <tr> <td>show interfaces</td> <td rowspan="2">Display the tail-drop threshold configuration for each supported drop precedence level of each queue for the specified interface.</td> </tr> <tr> <td>tail-drop-threshold</td> </tr> </table>		show interfaces	Display the tail-drop threshold configuration for each supported drop precedence level of each queue for the specified interface.	tail-drop-threshold
show interfaces	Display the tail-drop threshold configuration for each supported drop precedence level of each queue for the specified interface.				
tail-drop-threshold					

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Syntax	traffic-shape <i>bw</i>
Parameters	<i>bw</i> Enter the shaping bandwidth percentage from 0 to 100 in increments of 5.
	Use the no traffic-shape command to restore the default interface shaping rate value.
Modes	Global Config
Usage Information	This command is only for egress (output) rate-shaping.

Differentiated Services (DiffServ) Commands

DiffServ commands are not included in SFTOS 2.4.1.

Provisioning (IEEE 802.1p) Commands

The commands described in this section are:

- [classofservice dot1pmapping on page 285](#)
- [show classofservice dot1pmapping on page 286](#)
- [vlan port priority all on page 286](#)
- [vlan priority on page 286](#)

classofservice dot1pmapping

This command maps an 802.1p priority to an internal traffic class for a device when in ‘Global Config’ mode. The number of available traffic classes may vary with the platform. Userpriority and trafficclass can both be in the range from 0-6.

Syntax	classofservice dot1pmapping <i>userpriority trafficclass</i>		
Mode	Global Config or Interface Config; Interface Range		
Command History	<table border="1"> <tr> <td>Version 2.3</td> <td>Interface Range mode added</td> </tr> </table>	Version 2.3	Interface Range mode added
Version 2.3	Interface Range mode added		

show classofservice dot1p mapping

This command displays the current 802.1p priority mapping to internal traffic classes for all or specific interfaces.

Syntax **show classofservice dot1p mapping** [*unit/slot/port*]

Mode Privileged Exec and User Exec

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-6. Any subsequent per port configuration will override this configuration setting.

Syntax **vlan port priority all** *priority*

Mode Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0-6.

Syntax **vlan priority** *priority*

Default 0

Mode Interface Config

This chapter covers the following commands:

- [{deny|permit} on page 288](#)
- [mac access-list extended on page 290](#)
- [mac access-list extended rename on page 291](#)
- [mac access-group on page 292](#)
- [show mac access-lists on page 292](#)



Note: SFTOS 2.4.1 does not support IP-based ACL commands.

An Access Control List (ACL) ensures that only authorized users and types of traffic to have access to specific resources, while blocking unwarranted attempts to reach network resources.

The following conditions pertain to ACLs in SFTOS:

- Maximum of 1064 ACLs, each with a maximum of 64 rules
- ACL configuration for IP packet fragments is not supported.
- The maximum number of rules per ACL translates into the number of hardware classifier entries used when an ACL is attached to an interface. Increasing these values in the SFTOS software increases the RAM and NVSTORE usage.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored.

For details on using ACL commands, see the Access Control chapter in the *SFTOS Configuration Guide*. ACLs factor into quality of service. For more on quality of service (QoS), see [Quality of Service \(QoS\) Commands on page 275](#).

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. See [Implementation Notes on page 164](#) in the [Security Commands](#) chapter for details.

{deny|permit}

This command creates a new rule for the selected MAC access list. Each rule is appended to the list of configured rules for the list. Note that an implicit “deny all” MAC rule always terminates the access list.

Syntax `{deny|permit} {srcmac srcmacmask | any} {{dstmac dstmacmask | any | bpdud} [ethertypekey | 0x0600-0xFFFF] [vlan {eq 0-4095 | range 0-4095 0-4095}] [cos 0-7] [secondary-vlan {eq 0-4095 | range 0-4095 0-4095}] [secondary-cos 0-7] [assign-queue queue-id_0-6] [redirect slot/port]`

Parameters	deny permit	The rule may either deny or permit traffic according to the specified classification fields.
	<i>srcmac</i> <i>srcmacmask</i> any <i>dstmac</i> <i>dstmacmask</i> any bpdud	Note: In SFTOS 2.4.1, only the source MAC is supported. The source (<i>srcmac srcmacmask</i> any) and destination (<i>dstmac dstmacmask</i> any bpdud) MAC value and mask pairs must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. (See the Usage section, below.) The bpdud keyword may be specified for the destination MAC value/mask pair indicating a well-known BPDU MAC value of 01-80-c2-xx-xx-xx (hex), where 'xx' indicates a don't care.
	<i>ethertypekey</i>	(Optional) The Ethertype (<i>ethertypekey</i>) may be specified as either a keyword or a four-digit hexadecimal value from 0x0600 to 0xFFFF. The currently supported <i>ethertypekey</i> keyword values are: appletalk , arp , ibmsna , ipv4 , ipv6 , ipx , mplsmcast , mplsucast , netbios , novell , pppoe , rarp . Each of these translates into its equivalent Ethertype value(s). (See the Usage section, below.)
	vlan { eq 0-4095 range 0-4095 0-4095}	(Optional) To specify a filter on a VLAN, enter vlan eq followed by the VLAN ID. Or, for a VLAN range, use vlan range , followed by the lowest VLAN ID and then the highest VLAN ID in the range.
	cos 0-7	(Optional) Use the cos keyword to specify a filter based on the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

secondary-vlan	(Optional) As above, for the vlan keyword.
secondary-cos	(Optional) As above, for the cos keyword.
assign-queue	(Optional) The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <i>queue-id</i> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. (See the Usage section, below.)
redirect	(Optional) The redirect parameter redirects traffic matching this rule to the specified egress port. The redirected packet carries the same MAC address as it would have if it had not been redirected (the MAC address of the next hop defined in the routing table). Basically, it looks like a mirrored packet on the redirect port. (See the Usage section, below.)



Note: The **no** form of this command is not supported, as the rules within an ACL group cannot be deleted individually. Rather, the entire ACL group must be deleted and re-specified.

Usage

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword **any** to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The *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.

The Ethertype (*ethertypekey*) may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *ethertypekey* values are: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, and **rarp**. Each of these translates into its equivalent Ethertype value(s), as shown in [Table 23](#).

Table 23 Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191

Table 23 Ethertype Keyword and 4-digit Hexadecimal Value (continued)


Ethertype Keyword	Corresponding Value
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The **assign-queue** and **redirect** parameters are only valid for a **permit** rule.

Mode	Mac Access List Config	
Related Commands	interface range	Identify an interface range and access the Interface Range mode.
	mac access-group (port channel)	In the Interface Port Channel Config mode, attach a MAC ACL to the selected port channel.
	mac access-group	Attach a specific MAC Access Control List (ACL) identified by <i>name</i> to an interface in the ingress direction.
	mac access-list extended	Create a MAC ACL.
	show mac access-lists	Display the rules defined for the MAC access list specified by <i>name</i> .

mac access-list extended

This command creates a MAC Access Control List (ACL) identified by *name*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. .

 **Note:** The CLI mode is changed to Mac Access List Config (prompt is “*hostname* (Mac-Access-List Config)#”) when this command is successfully executed. If a MAC ACL by this name already exists, this command simply invokes the mode.

The **no** version of this command deletes a MAC ACL identified by *name* from the system.

Syntax	mac access-list extended <i>name</i>	
Parameters	<i>name</i>	Case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. The string may include alphabetic, numeric, dash, dot or underscore characters only. The string must start with a letter.
Mode	Global Config	
Related Commands	{deny permit}	Creates a new rule for the MAC access list selected by the mac access-list extended command.
	interface range	Defines an interface range and accesses the Interface Range mode

mac access-group (port channel)	In the Interface Port Channel Config mode, attaches a MAC ACL to the selected port channel
mac access-group	Attaches a specific MAC Access Control List (ACL) identified by <i>name</i> to an interface in the ingress direction
mac access-list extended rename	Changes the name of an existing MAC ACL.
show mac access-lists	Displays the rules defined for the MAC access list specified by <i>name</i> .

mac access-list extended rename

This command changes the name of an existing MAC ACL. The *name* parameter is the name of an existing MAC ACL. The *newname* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *newname* already exists.

Syntax `mac access-list extended rename name newname`

Parameters	<i>name</i>	The ACL name assigned during the creation of the ACL by using the mac access-list extended command
	<i>newname</i>	Case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. The string may include alphabetic, numeric, dash, dot or underscore characters only. The string must start with a letter.

Mode Global Config

Related Commands	{deny permit}	Creates a new rule for the MAC access list selected by the mac access-list extended command.
	interface range	Defines an interface range and accesses the Interface Range mode
	mac access-group (port channel)	In the Interface Port Channel Config mode, attaches a MAC ACL to the selected port channel
	mac access-group	Attaches a specific MAC Access Control List (ACL) identified by <i>name</i> to an interface in the ingress direction
	mac access-list extended	Creates a MAC Access Control List (ACL)
	show mac access-lists	Displays the rules defined for the MAC access list specified by <i>name</i>

mac access-group

This command attaches a specific MAC Access Control List (ACL) identified by *name* to an interface in the ingress direction. This command, when used in Interface Config mode, only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

Syntax `mac access-group name [1-4294967295] in`

The **no mac access-group *name*** command removes the MAC ACL identified by *name* from the interface in the ingress direction.

Parameters	<i>name</i>	The <i>name</i> must be the name of an existing MAC ACL.
	1-4294967295	(OPTIONAL) Enter a sequence number that indicates the order of this ACL relative to other ACLs already assigned to this port channel. A lower sequence number indicates higher precedence order. If the selected number is already in use for this port channel, this ACL replaces the currently attached ACL using that sequence number. If you do not specify a number with this command, a number that is one greater than the highest sequence number currently in use for this port channel is used for this ACL.
	in	The in parameter is required. SFTOS supports only the ingress direction.
Modes	Global Config, Interface Config; Interface Range, which is indicated by the (conf-if-range-interface)# prompt, such as (conf-if-range-vlan 10-20)#.	
Command History	Version 2.3	Added Interface VLAN and Interface Range modes.
Related Commands	interface range	Defines an interface range and accesses the Interface Range mode
	mac access-group (port channel)	In the Interface Port Channel Config mode, attaches a MAC ACL to the selected port channel
	mac access-list extended	Creates a MAC Access Control List (ACL) identified by name, consisting of classification fields defined for the Layer 2 header of an Ethernet frame.
	show mac access-lists	Displays the rules defined for the MAC access list specified by <i>name</i> .

show mac access-lists

This command displays the rules defined for all MAC ACLs or that specified by *name*.

Syntax `show mac access-lists [name]`

Mode Privileged Exec

When the command is used with the *name* option, the report displays details for the identified MAC access list, in the following fields:

Field Descriptions

Rule Number—The ordered rule number identifier defined within the ACL.

Action—Displays the action associated with each rule. The possible values are Permit or Deny.

Match all—TRUE OR FALSE

Source MAC Address—Displays the source MAC address for this rule.

Source MAC Mask—Displays the source MAC mask for this rule.

Destination MAC Address—Displays the destination MAC address for this rule.

Destination MAC Mask—Displays the destination MAC mask for this rule.

Ethertype—Displays the Ethertype keyword or custom value for this rule.

VLAN ID—Displays the VLAN identifier value or range for this rule.

COS—Displays the COS (802.1p) value for this rule.

Secondary VLAN ID—Displays the Secondary VLAN identifier value or range for this rule.

Secondary COS—Displays the Secondary COS (802.1p) value for this rule.

Assign Queue—Displays the queue identifier to which packets matching this rule are assigned.

Redirect Interface—Displays the *unit/slot/port* to which packets matching this rule are forwarded.

When the command is used without the *name* option, the report displays a summary of all defined MAC access lists in the system, in the following fields:

Field Descriptions

Name—The name of the MAC access list

Number of Rules—The number of user-configured rules defined for this ACL

This does not include the implicit 'deny all' rule defined at the end of every MAC ACL

Interfaces—The list of interfaces (*unit/slot/port*) to which the MAC ACL is attached in a given direction

Direction—Denotes the direction in which the MAC ACL is attached to the set of interfaces listed. The only current possible value is Inbound.

Related Commands

[mac access-list extended](#) Creates a MAC Access Control List (ACL) identified by name, consisting of classification fields defined for the Layer 2 header of an Ethernet frame.

show mac access-lists

Index

Symbols

{deny|permit} 288

Numerics

10/100 Ethernet port 3, 79

802.3ad 28

802.3x flow control 200

A

Access Control Lists (ACLs) 287

accessing DHCP Pool Config mode 209

ACL wildcard masks 287

ACLs 287

addport 249

Address Aging Timeout 114

areaid 41

ARP

aging 204–214

audience 22

authentication login 169

Authentication traps 101

B

Backspace 43

bandwidth division 276

b-node (Broadcast) 210

Boot Menu Options 33

bootfile 204

bpdumigrationcheck, spanning-tree 266

bridge aging-time 106

broadcasts

broadcast storm recovery mode 200

Bulk Configuration

see interface range 108

bulk configuration 108

C

class command 49

Class Map Mode 49

classofservice dot1p-mapping 276

classofservice dot1p-mapping 285

classofservice trust 277

clear commands

clear config 138

clear pass 157

clear traplog 139

clear vlan 121

clear config 38, 138

clear counters 138

clear dot1x statistics 170

clear igmpsnooping 139

clear ip dhcp binding 204

clear ip dhcp conflict 205

clear ip dhcp server statistics 204

clear pass 157

clear port-channel 139

clear radius statistics 170

clear traplog 139

clear vlan 121

CLI (Command Line Interface) 31

CLI banner 141

client-identifier 205

client-name 205

Command Line Interface (CLI) 31

Command Modes, Using 44

Command Syntax Conventions 39

config commands

config arp agetime 204–214

config lags adminmode 251–252

config lags create 251

config lags deleteport 251

config lags linktrap 252

config lags name 253

config login session 158

config port admin-mode 119, 257

config port linktrap 103

config switchconfig broadcast 200

config switchconfig flowcontrol 200

config users add 34, 159

config users passwd 34, 159

config vlan add 108

config vlan delete 108, 123

config vlan garp gvrp 228

config vlan garp jointime 225

config vlan garp leavealltime 227

config vlan garp leavetime 226

config vlan interface acceptframe 133–134

config vlan makestatic 124

config vlan name 125

config vlan participation 133–134

config vlan ports gvrp 228–229

config vlan ports ingressfilter 133–134

config vlan ports pvid 134, 137

config vlan ports tagging 131–132, 135, 137

Config Interface Vlan mode 50

config users delete 159

config users passwd 159

config vlan ports ingressfilter 134–135
configuration guide 23
configuration reset 138
Configuration Scripting 146
configure 106
configure command 47
configuring a range 108
Contact and Patents Information 23
control characters 43
copy 37–38, 139
copy (clibanner) 141
copy system 34
Copyright 2
CoS Queue Prioritization 276
cos-queue max-bandwidth 277
cos-queue min-bandwidth 278
cos-queue random-detect 278
cos-queue strict 279
Ctrl characters 43
CX4 cable configuration 3
CX4 pre-emphasis commands 3

D
Default Gateway 37
Delete 43
deleteport (global config) 251
deleteport (interface config) 250
deny|permit 288
Deprecated Commands 4
description 122
destination MAC 4
destination port 112
device configuration commands 115–116, 227, 234
DHCP client 205
DHCP Pool Config 205
DHCP Pool Config mode 47
DHCP Pool Config mode, accessing 209
DHCP Pool Configuration Mode 49
DHCP Server 203
DiffServ 4
dir 56
disconnect 158
dns-server 206
document conventions 39
domain-name 206
dot1x defaultlogin 170
dot1x initialize 171
dot1x login 171
dot1x max-req 171
dot1x port-control 172
dot1x port-control all 172
dot1x re-authenticate 173
dot1x re-authentication 173
dot1x system-auth-control 174

dot1x timeout 174
dot1x user 175
Double VLAN tagging 221
Double VLAN Tunneling (Web UI panel) 221, 223–224
downloading 33
drop precedence 280
dvlan-tunnel etherType 221
Dynamic Host Configuration Protocol (DHCP) 203

E

edge port, STP 267
egress rate shaping 285
enable 107
enable command 47
enable passwd 142
encapsulation (VLAN) 123
EtherChannel 249
Ethernet Management port 3, 79
Ethernet Range 109
Ethernet Range mode 47
Ethernet trunk 249
Exit 43

F

flow control 200
forwarding database, differences between the terminal and Web interfaces 51
frame acceptance mode 133–134

G

GARP commands 225
GARP Multicast Registration Protocol (GMRP) 231
General Attribute Registration Protocol (GARP) 225
Global Config mode 47–48
gmrp adminmode 231
GMRP commands 225
gmrp interfacemode all 232
GVRP
 enabling or disabling 228–229
 join time 225
 leave time 226
gvrp adminmode enable 228
GVRP command 225
gvrp interfacemode enable 228

H

hardware installation guide 23
hardware-address 207
h-node (hybrid) 211
host 207
hostname 57
hostname, setting 57
How to Use This Document 22

HTML 51
HTTP 51

I

IEEE 802.1Q 133–134
IfIndex 79
igmp enable 236
igmp enable (interface) 236
igmp fast-leave (interface) 237
igmp groupmembership-interval 237
igmp igmp maxresponse (interface) 243
igmp interfacemode enable all 238
igmp maxresponse 239
igmp mcrctexpiretime 239
igmp mrouter 240
igmp mrouter interface enable 240
IGMP Snooping 4
in-band connectivity 52
ingress filtering 133–134
Installing the S2410 System 23
interface 108
interface (access Interface Config mode) 108
interface command 47, 49
Interface Config Mode 48
Interface Config mode 47
interface managementethernet 36, 58
interface range 108
Interface Range mode command
 addport 250
 classofservice dot1p-mapping 276
 classofservice dot1pmapping 285
 classofservice trust 277
 deleteport 250
 dot1x max-req 172
 dot1x port-control 172
 dot1x re-authentication 173
 dot1x timeout 175
 dvlan-tunnel ethertype 221
 igmp groupmembership-interval 238
 igmp maxresponse 239
 igmp mcrctexpiretime 239
 igmp mrouter 240
 ip rip send version 137
 mac access-group 292
 no port-security max-dynamic 165
 port lacpmode 254
 port-security 164
 port-security mac-address 166
 port-security mac-address move 166
 port-security max-static 165
 protocol vlan group 127
 shutdown 119, 252, 257
 snmp trap link-status 103
 snmp-server enable trap violation 101

 spanning-tree edgeport 267
 spanning-tree hello-time 268
 spanning-tree mst priority 272
 spanning-tree port mode enable 273
 vlan acceptframe 133
 vlan ingressfilter 133
 vlan pvid 137

interface vlan 44, 46, 123
interface vlan command 47, 124
Interface VLAN mode 120, 123
Internet. See Web interface
inventory 114–116, 119, 169, 227, 229, 233–234
inverted mask 289
IP ACLs 4
ip address 36
ip address (management) 58
ip dhcp bootp automatic 208
ip dhcp conflict logging 208
ip dhcp excluded-address 208
ip dhcp ping packets 209
ip dhcp pool 209
ip dhcp pool command 47
ip dvmrp trapflags 94
ip http javamode enable 53, 196
ip http secure-port 196
ip http secure-protocol 196
ip http secure-server enable 197
ip http server enable 197
ip pim-trapflags 94
ip ssh maxsessions 192
ip ssh protocol 193
ip ssh server enable 193
ip ssh timeout 194
ip telnet maxsessions 88
ip telnet server enable 89
ip telnet timeout 88
ipaddr 41
iSupport 23

J

JavaScript(TM) 51
join time 225
Jumbo Frame size 4

K

key 189
key, tacacs-server 188
Keyboard Shortcuts 43

L

LAG (802.3ad) 249
LAGs
 configuring 251

- deleting ports from 251
- enabling or disabling 251–252
- link traps 252
- logical ID 256
- name 253
- summary information 256
- user-assigned name 256

lease 209

leave time 226–227

Line Config mode 47, 49

lineconfig command 47

link aggregate group (LAG) 249

Link Aggregation (IEEE 802.3ad) 28

link aggregations. See LAGs

link traps

- interface 103
- LAG 252

logging buffered 149

logging buffered wrap 150

logging cli-command 150

logging console 151

logging host 151

logging host remove 152

logging persistent 152

logging port 152

logging syslog 153

logical slot/port 42

logout 34, 143

logout commands 143

M

Mac Access List Config mode 48, 290

mac access-group 292

mac access-list extended 290

mac access-list extended command 48

mac access-list extended rename 291

MAC ACLs 4

MAC address 207

MAC Database Commands 106

mac-access-list extended command 49

macaddr 41

mac-address (management VLAN) 59

mac-type (management VLAN) 59

makestatic 124

management commands 88

management route default 36, 60

mask 207

max-hops, spanning-tree 269

maximum Jumbo Frame size 4

maximum LAG ports 4

Maximum MAC ACL rules 4

Maximum number of ACLs 4

maximum number of LAGs 4

Microsoft client identifier 205

mirrored port 112, 117

m-node (mixed) 210

mode

- Ethernet Range 47
- Port Channel 47
- VLAN Range 47

mode access 47

mode dvlan-tunnel 222

Mode-based Topology 45

modes 47–48

monitor session 112

monitor session 1 mode 113

monitored port 117

mtu 61

mtu (VLAN) 125

multicast 231

Multicast Forwarding Database 231

multicast packets 231

Multi-Link Trunking (MLT) 249

N

name (VLAN) 125

NetBIOS mapping 210

NetBIOS node type 210

netbios-name-server 210

netbios-node-type 210

network 210

network configuration commands 88

Network Connectivity Configuration panel 53

network mac-address 62

network mac-type 62

network mgmt_vlan 126

network mgmt_vlan. See vlan participation.

network parms 62

network protocol 62

next-server 211

NIC bonding 249

NIC teaming 249

no monitor 113

no monitor session 1 114

no spanning-tree mst 270

Node Manager 21

number of LAGs 4

O

objectives 21

option 211

P

participation (VLAN) 126

passwords

- changing user 159
- resetting all 142, 157

- setting user 34, 159
- user 159
- patents 23
- PDUs 225, 227
- ping 144
- p-node (peer-to-peer) 210
- Policy Class Mode 49
- policy map command 49
- Policy Map Mode 49
- port (for TACACS+) 190
- port channel 249
- Port Channel mode 47
- Port Channel Range 109, 252, 257
- Port ID format 3
- port lacpmode 253
- port lacpmode enable all 254
- port lacpmode enable all command 4
- port lacpmode enable command 4
- port lacpmode lacptimeout (global) 254
- port lacpmode lacptimeout (interface) 255
- port mirroring 112, 116
- port mode, spanning-tree 273
- port monitoring 116
- port teaming 249
- port trunking 249
- port-based security 288
- port-channel 251
- port-channel adminmode (global) 251
- port-channel adminmode (interface) 252
- port-channel enable (interface) 252
- port-channel enable all (global) 251
- port-channel linktrap 252
- port-channel name 253
- port-channel staticcapability 253
- portfast 267
- ports
 - administrative mode 119, 257
 - deleting from LAGs 251
 - frame acceptance mode 133–134
 - GVRP 228–229
 - information 117
 - ingress filtering 133–134
 - link traps 103
 - tagging 131–132, 135, 137
 - VLAN IDs 134, 137
- port-security 164
- port-security mac-address 165
- port-security mac-address move 166
- port-security max-dynamic 164
- port-security max-static 165
- pre-emphasis commands 3
- priority 190
- priority (TACACS+) 190
- priority (VLAN) 126

- Privileged Exec Mode 48
- Privileged Exec mode 47
- probe port 112
- Products and Services Liability 23
- prompt, Interface VLAN mode 124
- protocol (management VLAN) 63
- Protocol Data Units. See PDUs
- protocol group 127
- protocol vlan group 127
- protocol vlan group all 128
- pvid (VLAN) 128

Q

- QinQ 221
- QoS
 - ACLs 28
- QoS DiffServ 4
- queue drop precedence levels 280
- Quick Reference 23
- quit 143

R

- radius accounting mode 181
- radius server host 181
- radius server key 182
- radius server msgauth 183
- radius server primary 183
- radius server retransmit 183
- radius server timeout 184
- random-detect exponential-weighting-constant 279
- random-detect queue-parms 280
- range configuration 108
- Range, Port Channel 252, 257
- rate shaping 285
- Refresh button 53
- Related Documents 23
- release notes 23
- reload 38, 144
- remotecon maxsessions 91
- reset system command 144
- RFC 1700 205
- Router Config OSPF Mode 49
- Router Config RIP Mode 49
- router ospf command 49
- router rip command 49
- routerid 41
- RSMLT 249

S

- Save button 53
- script apply 147
- script delete 147
- script list 147

script show 148
script validate 148
serial baudrate 91
serial timeout 92
service dhcp 212
service port 79
serviceport commands 3
serviceport ip 37, 63
serviceport protocol 64
session-limit 89
sessions
 closing 143, 158
 displaying 158
session-timeout 89
set garp timer join 225
set garp timer leave 226
set garp timer leaveall 227
set gmrp adminmode 232
set gmrp interfacemode 233
set gmrp interfacemode all 233
set gvrp adminmode 229
set gvrp interfacemode 229
set gvrp interfacemode all 229
set igmp (interface) 241
set igmp (system) 241
set igmp fast-leave 241
set igmp groupmembership-interval (global) 241
set igmp groupmembership-interval (interface) 242
set igmp interface 242
set igmp interfacemode all 242
set igmp maxresponse (global) 243–244
set igmp mcrtexpiretime (interface) 244
set igmp mrouter 245
set prompt 57
setting the hostname 57
SFTOS CLI 31
SFTOS Command Reference 23
SFTOS Configuration Guide 23
show accounting 185
show arp switch 64
show authentication 175
show authentication users 176
show classofservice dot1p-mapping 281
show classofservice dot1p-mapping 286
show classofservice trust 281
show commands
 show inventory 114–116, 119, 169, 227, 229,
 233–234
 show lags summary 256
 show login session 158
 show port 117
 show stats switch detailed 66, 68, 70, 75–77
 show switchconfig 199
 show tacacs 191
 show terminal 144
 show users 158
 show vlan detailed 77, 129, 280, 282–284
show dot1q-tunnel 223
show dot1x 176
show dot1x detail 178
show dot1x users 179
show dvlan-tunnel 224
show forwardingdb agetime 114
show garp 227
show gmrp configuration 233
show gvrp configuration 229
show hardware 33, 65
show igmpsnooping 245
show igmpsnooping fast-leave 246
show igmpsnooping mrouter interface 246
show interface 65, 75–76
show interface ethernet 67
show interface managementethernet 36
show interfaces 77
show interfaces cos-queue 282
show interfaces description 78
show interfaces random-detect 282
show interfaces tail-drop-threshold 283
show inventory 194
show ip dhcp binding 212
show ip dhcp conflict 214
show ip dhcp global configuration 213
show ip dhcp pool configuration 213
show ip dhcp server statistics 214
show ip http 198
show logging 78, 153
show logging buffered 154
show logging hosts 155
show logging persistent 154
show logging traplogs 156
show login session 34, 158, 161
show mac access-lists 292
show mac-address-table 114
show mac-address-table gmrp 234
show mac-address-table igmpsnooping 247
show mac-address-table multicast 115–116
show mac-address-table stats 116
show mac-addr-table 78
show mac-addr-table all 79–80
show mac-addr-table count 80, 281
show mac-addr-table vlan 80
show monitor session 116
show msglog 80
show network 81
show port 117
show port all 34
show port protocol 119
show port-channel 256

[show port-channel brief](#) 255
[show port-channel summary](#) 257
[show port-security](#) 166
[show port-security dynamic](#) 167
[show port-security static](#) 168
[show port-security violation](#) 168
[show radius](#) 184
[show radius accounting statistics](#) 185
[show radius statistics \(authentication\)](#) 186
[show running-config](#) 81
[show serial](#) 92
[show serviceport](#) 37, 82
[show serviceport command](#) 36
[show snmpcommunity](#) 95
[show snmptrap](#) 95
[show snmp](#) 218
[show snmp client](#) 219
[show snmp server](#) 220
[show spanning-tree](#) 260
[show spanning-tree interface](#) 261
[show spanning-tree mst detailed](#) 262
[show spanning-tree mst port detailed](#) 262
[show spanning-tree mst port summary](#) 264
[show spanning-tree mst summary](#) 264
[show spanning-tree summary](#) 265
[show spanning-tree vlan](#) 265
[show storm-control](#) 199
[show sysinfo](#) 83, 222, 285–286
[show tacacs](#) 191
[show tech-support](#) 86
[show telnet](#) 90
[show terminal](#) 144
[show terminal length](#) 144
[show trapflags](#) 96
[show users](#) 34, 158
[show users authentication](#) 179
[show version](#) 84
[show vlan](#) 129
[show vlan port](#) 130, 137
[shutdown](#) 119, 257
[shutdown all](#) 119
[Simple Network Time Protocol \(SNTP\) commands](#) 215
[single-connection](#) 191
[slot/port format](#) 3
[SMLT](#) 249
[SNMP system management commands](#) 94
[snmp trap link-status](#) 103
[snmp trap link-status all](#) 103
[SNMP trap summary and trap details](#) 156
[SNMP v3 access privileges](#) 160
[snmp-server](#) 97
[snmp-server community](#) 97
[snmp-server community ipaddr](#) 98
[snmp-server community ipmask](#) 98
[snmp-server community mode](#) 98
[snmp-server community ro](#) 99
[snmp-server community rw](#) 99
[snmp-server enable trap violation](#) 101
[snmp-server enable traps bcstorm](#) 99
[snmp-server enable traps linkmode](#) 100
[snmp-server enable traps multiusers](#) 100
[snmp-server enable traps stpmode](#) 101
[snmp-server traps enable](#) 101
[snmptrap](#) 102
[snmptrap ipaddr](#) 102
[snmptrap mode](#) 102
[snmptrap snmpversion](#) 103
[snmp broadcast client poll-interval](#) 215
[snmp client mode](#) 216
[snmp client port](#) 216
[SNTP Commands](#) 215
[snmp server](#) 218
[snmp unicast client poll-interval](#) 217
[snmp unicast client poll-retry](#) 217
[snmp unicast client poll-timeout](#) 217
[source port](#) 112, 117
[spanning-tree](#) 265
[spanning-tree bpdumigrationcheck](#) 266
[spanning-tree configuration name](#) 266
[spanning-tree configuration revision](#) 266
[spanning-tree edgeport](#) 267
[spanning-tree forceversion](#) 267
[spanning-tree forward-time](#) 268
[spanning-tree hello-time](#) 268
[spanning-tree max-age](#) 269
[spanning-tree max-hops](#) 269
[spanning-tree mst](#) 269
[spanning-tree mst instance](#) 271
[spanning-tree mst priority](#) 271
[spanning-tree mst vlan](#) 272
[spanning-tree port mode enable](#) 272
[spanning-tree port mode enable all](#) 273
[special characters](#) 43
[speed commands](#) 3
[speedkeys](#) 43
[SSH, enable/disable](#) 193
[sshcon maxsessions. See ip ssh maxsessions.](#)
[sshcon timeout. See ip ssh timeout.](#)
[statistics](#)
 [switch, related 201 commands](#) 66, 68, 70, 75–77
[status HTML pages](#) 52
[storm-control broadcast](#) 200
[storm-control flowcontrol](#) 200
[Subnet Mask](#) 37
[switch](#) 199
 [configuring for in-band connectivity](#) 52
 [configuring for Web access](#) 52
 [inventory](#) 114–116, 119, 169, 227, 229, 233–234

- resetting 144
- statistics, related 201 commands 66, 68, 70, 75–77
- switch navigation icon in Web UI 53
- syntax conventions 39
- syslog servers 78, 80
- system information and statistics commands 201 commands 97
- system utilities 138–144
- System Utility Commands 138

T

- Tab 43
- TACACS
 - key 189
 - port 190
 - priority 190
 - show tacacs 191
 - single-connection 191
 - timeout 191
- TACACS Config mode 45, 48, 50
- tacacs-server host 188
- tacacs-server host ip-address command 48
- tacacs-server key 188
- tacacs-server timeout 189
- tagged 131
- tagging 131–132, 135, 137
- tail-drop queue-parms 284
- Tech Tips and FAQ, S-Series 23
- telnet 90
 - enable or disable 89
 - sessions, closing 143, 158
 - sessions, displaying 158
- telnetcon maxsessions 91
- telnetcon maxsessions. See ip telnet maxsessions.
- telnetcon timeout. See ip telnet timeout.
- terminal length 144–145
- terminal length command 144
- timeout 191
- timeouts
 - ARP 204–214
- timeouts, ARP 204–205
- Topology, Mode-based 45
- traceroute 145
- traffic-shape 285
- trap log, clearing 139
- trapflags (OSPF) 94
- TRAPMGR 156
- traputil.c 156
- trunks. See LAGs
- type 207

U

- unique identifier for a DHCP client 205
- unit/slot/port format 3
- untagged 131–132
- uploading 33
- User Account Management Commands 157
- User Exec Mode 48
- User Exec mode 47
- user, new 159
- username 34, 159
- users
 - adding 34, 159
 - displaying 158
 - passwords 34, 142, 157, 159
- users defaultlogin 180
- users login 180
- users snmpv3 accessmode 160
- users snmpv3 authentication 160
- users snmpv3 encryption 160
- Using Command Modes 44

V

- vlan 132
- vlan acceptframe 133
- vlan acceptframe command 4
- vlan commands (Global Config) 134–136
- vlan ingressfilter 133
- vlan ingressfilter command 4
- VLAN Mode 50
- VLAN mode 47
- vlan name. See name.
- vlan participation (interface) 133
- vlan participation (management) 87
- vlan participation all 134
- vlan participation all command 4
- vlan port acceptframe all 134
- vlan port acceptframe command 4
- vlan port ingressfilter all 134
- vlan port ingressfilter all command 4
- vlan port priority all 286
- vlan port pvid all 134
- vlan port pvid all command 4
- vlan port tagging all 135
- vlan port tagging all command 4
- vlan port untagging all 135
- vlan port untagging all command 4
- vlan priority 286
- vlan protocol group 137
- vlan protocol group add protocol 136
- vlan protocol group remove 136
- vlan pvid 137
- vlan pvid command 4
- VLAN Range 109

- VLAN Range mode 47
- vlan tagging 137
- vlan tagging command 4
- VLAN tunneling 221
- vlan untagging 137
- vlan untagging command 4
- VLANs
 - adding 108
 - changing the name of 125
 - deleting 108, 123
 - details 77, 129, 280, 282–284
 - frame acceptance mode 133–134
 - GVRP 228–229
 - IDs 134, 137
 - ingress filtering 133–134
 - jointime 225
 - leave all time 227
 - leave time 226
 - making static 124
 - participation in 133–134
 - resetting parameters 121
 - tagging 131–132, 135, 137

W

- Web connections, displaying 158
- Web interface
 - command buttons 53
 - configuring for Web access 52
 - panel 52
 - starting 52
- Web UI S50 switch navigation icon 53
- weighted random early discard (WRED) 278
- wildcard masks, ACL 287
- Windows Internet Naming Service (WINS) 210
- WINS 210
- WRED (weighted random early discard) 278, 282
- WRED average queue depth calculation 279
- WRED parameters 280
- write 146
- write memory 146

X

- Xmodem options 33

