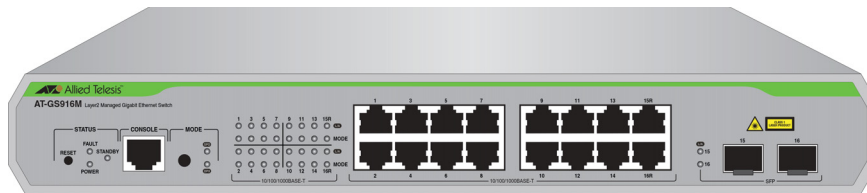
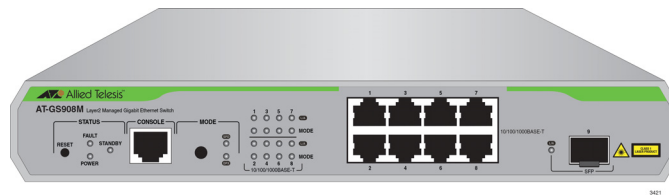


## AT-GS900M Series

Gigabit Ethernet Switch



# Management Software Version 2.3.2 Command Line Interface Reference

## Copyright

Copyright © 2014, Allied Telesis, Inc.

All rights reserved.

This product includes software licensed under the Berkeley Software Distribution (BSD) License. As such, the following language applies for those portions of the software licensed under the BSD License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of Allied Telesis, Inc. nor the names of the respective companies above may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Allied Telesis, Inc., hereby disclaims all copyright interest of the following products:

- \* UCD-SNMP: copyright 1989, 1991, 1992 by Carnegie Mellon University, derivative work copyright 1996, 1998 by the Regents of the University California
- \* Net-SNMP: part 1- copyright 1989, 1991, 1992 by Carnegie Mellon University, derivative work copyright 1996, 1998-2000 by the Regents of the University California; part 2 - copyright 2001-2003, Networks Associates Technology, Inc.; part 3 - copyright 2001-2003 by Cambridge Broadband Ltd.; part 4 - copyright 2003 Sun Microsystems, Inc.
- \* Mathopd: this product includes Mathopd 1.6 copyright (c) 1996 - 2005 by Michiel Boland

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in this product, please send us a request by registered mail including a check for US\$15 to cover production and shipping costs, and a CD with the GPL code will be mailed to you.

GPL Code Request

Allied Telesis, Inc.  
3041 Orchard Parkway  
San Jose, California 95134

No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, AlliedWare Plus, and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

# Contents

---

<b>Preface</b> .....	13
Document Conventions.....	14
Where to Find Web-based Guides.....	15
Contacting Allied Telesis.....	16
<b>Section I: Getting Started</b> .....	<b>17</b>
<b>Chapter 1: Command Line Interface</b> .....	19
Management Sessions.....	20
Local Management.....	20
Remote Management.....	20
Manager Account.....	21
Command Format.....	22
Command Line Interface Features.....	22
Command Formatting Conventions.....	22
<b>Chapter 2: Starting a Management Session</b> .....	23
Overview .....	24
Requirements for Remote Management .....	24
What to Configure First.....	24
Starting a Local Management Session .....	25
Starting a Remote Management Session Using Telnet.....	26
Starting a Remote Management Session Using the Web Browser.....	27
Adding a Management IP Address .....	28
Changing the Login Password .....	29
Assigning a Name to the Switch .....	30
Keyboard Shortcuts for Command Line Interface.....	31
Using Online Help .....	33
Saving Your Changes .....	34
Starting the Switch with The Default Setting.....	35
Ending a Management Session .....	36
<b>Chapter 3: Basic CLI Management Commands</b> .....	37
BYE.....	39
CLS.....	40
DISABLE SYSTEM FAN-STARTSTOP-ALARM.....	41
ENABLE SYSTEM FAN-STARTSTOP-ALARM.....	42
EXIT.....	43
HELP.....	44
LOGOFF.....	46
LOGOUT.....	47
QUIT.....	48
RESTART .....	49

SET INSTALL .....	50
SET PASSWORD.....	51
SET SYSTEM.....	52
SET SYSTEM SFP-TEMPHRESHOLD .....	53
SET TIME .....	54
SHOW CPU .....	55
SHOW DEBUG.....	56
SHOW INSTALL.....	57
SHOW SYSTEM.....	58
SHOW TIME .....	61
<b>Chapter 4: Basic Operations .....</b>	<b>63</b>
File System Overview .....	64
File Types.....	64
File Name.....	64
Downloading a File to the Switch .....	65
Downloading a File from a TFTP Server.....	65
Downloading a File Using FTP.....	65
Uploading a File from the Switch.....	67
Uploading a File to a TFTP Server.....	67
Uploading a File Using FTP .....	67
Updating the Management Software .....	69
Updating the Management Software Using TFTP .....	69
Updating the Management Software Using FTP.....	69
<b>Chapter 5: Basic Operations Commands .....</b>	<b>71</b>
ACTIVATE SCRIPT .....	73
CLEAR FLASH TOTALLY .....	74
COPY .....	75
CREATE CONFIG.....	76
DELETE FILE .....	77
DISABLE FTP SERVER.....	78
ENABLE FTP SERVER.....	79
LOAD.....	80
SET CONFIG.....	81
SET FTP LISTENPORT .....	82
SET LOADER.....	83
SET TFTP LISTENPORT .....	84
SHOW CONFIG .....	85
SHOW FILE.....	86
SHOW FTP.....	88
SHOW LOADER.....	89
SHOW TFTP .....	90
UPLOAD.....	91
<b>Section II: Switch Management .....</b>	<b>93</b>
<b>Chapter 6: Log Commands .....</b>	<b>95</b>
DISABLE LOG.....	96
DISABLE LOG OUTPUT .....	97
ENABLE LOG.....	98
ENABLE LOG OUTPUT .....	99
FLUSH LOG OUTPUT .....	100
PURGE LOG .....	101

SET LOG OUTPUT.....	102
SHOW CRASHLOG.....	105
SHOW LOG.....	106
SHOW LOG COUNTER.....	108
SHOW LOG OUTPUT.....	109
SHOW LOG STATUS.....	110
<b>Chapter 7: SNMP Commands .....</b>	<b>111</b>
ADD SNMP COMMUNITY.....	113
CREATE SNMP COMMUNITY.....	115
DELETE SNMP COMMUNITY.....	118
DESTROY SNMP COMMUNITY.....	119
DISABLE INTERFACE LINKTRAP.....	120
DISABLE SNMP.....	121
DISABLE SNMP COMMUNITY.....	122
DISABLE SNMP COMMUNITY TRAP.....	123
DISABLE SNMP TRAP.....	124
ENABLE INTERFACE LINKTRAP.....	125
ENABLE SNMP.....	126
ENBLE SNMP COMMUNITY.....	127
ENABLE SNMP COMMUNITY TRAP.....	128
ENABLE SNMP TRAP.....	129
SET SNMP COMMUNITY.....	130
SET SNMP LISTENPORT.....	132
SET SNMP TRAP LISTENPORT.....	133
SHOW INTERFACE.....	134
SHOW SNMP.....	137
SHOW SNMP COMMUNITY.....	140
SHOW SNMP TRAP.....	142
<b>Chapter 8: Simple Network Time Control (SNTP) Commands .....</b>	<b>145</b>
ADD NTP PEER.....	146
DELETE NTP PEER.....	147
DISABLE NTP.....	148
DISABLE SUMMER-TIME.....	149
ENABLE NTP.....	150
ENABLE SUMMER-TIME.....	151
PURGE NTP.....	152
RESET NTP.....	153
SET NTP.....	154
SET SUMMER-TIME.....	157
SHOW NTP.....	158
SHOW SUMMER-TIME.....	160
<b>Chapter 9: Telnet Commands .....</b>	<b>161</b>
DISABLE TELNET SERVER.....	162
ENABLE TELNET SERVER.....	163
SET ASYN.....	164
SET CONSOLE.....	165
SET TELNET.....	167
SHOW ASYN.....	168
SHOW CONSOLE.....	169
SHOW TELNET.....	171
TELNET.....	172

<b>Chapter 10: HTTP Commands</b> .....	173
DISABLE HTTP SERVER .....	174
ENABLE HTTP SERVER .....	175
SET HTTP LISTENPORT .....	176
SHOW HTTP SERVER .....	177
<b>Chapter 11: RADIUS Authentication Server Commands</b> .....	179
ADD RADIUSSERVER SERVER .....	180
DELETE RADIUSSERVER SERVER .....	181
DISABLE RADIUSACCOUNTING .....	182
ENABLE RADIUSACCOUNTING .....	183
SET AUTHENTICATION .....	184
SET RADIUS .....	185
SET RADIUSACCOUNTING .....	186
SHOW AUTHENTICATION .....	188
SHOW RADIUS .....	190
SHOW RADIUSACCOUNTING .....	191
 <b>Section III: Layer 2 Switching</b> .....	 <b>193</b>
<b>Chapter 12: IP Management Commands</b> .....	195
ADD IP IPADDRESS .....	196
DELETE IP .....	198
DISABLE IP DHCP .....	199
DISABLE IP REMOTEASSIGN .....	200
ENABLE IP DHCP .....	201
ENABLE IP REMOTEASSIGN .....	202
PING .....	203
SET IP .....	204
SHOW IP .....	206
<b>Chapter 13: VLAN Commands</b> .....	209
ADD VLAN PORT .....	210
CREATE VLAN .....	212
DELETE VLAN PORT .....	213
DESTROY VLAN .....	214
SET VLAN PORT .....	215
SHOW VLAN .....	216
<b>Chapter 14: Switching Commands</b> .....	219
ACTIVATE SWITCH PORT AUTONEGOTIATE .....	222
ADD SWITCH TRUNK .....	223
CREATE SWITCH TRUNK .....	224
DELETE SWITCH TRUNK .....	226
DESTROY SWITCH TRUNK .....	227
DISABLE SWITCH BPDFORWARDING .....	228
DISABLE SWITCH EAPFORWARDING .....	229
DISABLE SWITCH INFILTERING .....	230
DISABLE SWITCH LOOPDETECTION .....	231
DISABLE SWITCH MIRROR .....	232
DISABLE SWITCH PORT .....	233
DISABLE SWITCH PORT AUTOMDI .....	234
DISABLE SWITCH PORT FLOW .....	235

DISABLE SWITCH POWERSAVE.....	236
DISABLE SWITCH STORMDETECTION .....	237
ENABLE SWITCH BPDUFORWARDING.....	238
ENABLE SWITCH EAPFORWARDING.....	239
ENABLE SWITCH INFILTERING .....	240
ENABLE SWITCH LOOPDETECTION.....	241
ENABLE SWITCH MIRROR .....	242
ENABLE SWITCH PORT.....	243
ENABLE SWITCH PORT AUTOMDI .....	244
ENABLE SWITCH PORT FLOW .....	245
ENABLE SWITCH POWERSAVE.....	246
ENABLE SWITCH STORMDETECTION .....	247
RESET SWITCH.....	248
RESET SWITCH LOOPDETECTION COUNTER .....	249
RESET SWITCH PORT .....	250
RESET SWITCH STORMDETECTION COUNTER .....	251
SET SWITCH LIMITATION.....	252
SET SWITCH LOOPDETECTION .....	253
SET SWITCH MIRROR .....	255
SET SWITCH PORT.....	257
SET SWITCH STORMDETECTION .....	263
SET SWITCH TRUNK.....	266
SHOW SWITCH.....	267
SHOW SWITCH COUNTER.....	268
SHOW SWITCH LOOPDETECTION .....	269
SHOW SWITCH MIRROR .....	271
SHOW SWITCH PORT.....	272
SHOW SWITCH PORT COUNTER.....	274
SHOW SWITCH STORMDETECTION .....	276
SHOW SWITCH TRUNK .....	278
<b>Chapter 15: Ethernet Protected Switched Ring (EPSR) Commands .....</b>	<b>279</b>
ADD EPSR DATAVLAN.....	280
CREATE EPSR.....	281
DELETE EPSR DATAVLAN .....	283
DESTROY EPSR.....	284
DISABLE EPSR .....	285
ENABLE EPSR .....	286
PURGE EPSR.....	287
SHOW EPSR .....	288
SHOW EPSR COUNTER .....	289
<b>Chapter 16: Forwarding Database (FDB) Commands .....</b>	<b>291</b>
ADD SWITCH FILTER.....	292
DELETE SWITCH FILTER.....	294
DISABLE SWITCH AGEINGTIMER.....	295
ENABLE SWITCH AGEINGTIMER.....	296
RESET SWITCH FDB.....	297
SET SWITCH AGEINGTIMER.....	298
SHOW SWITCH FDB.....	299
SHOW SWITCH FILTER .....	301
<b>Chapter 17: DHCP Snooping Commands .....</b>	<b>303</b>
ADD DHCP Snooping.....	305
CREATE DHCP Snooping MACFILTER.....	306

DELETE DHCP Snooping .....	308
DESTROY DHCP Snooping Macfilter .....	309
DISABLE DHCP Snooping .....	310
DISABLE DHCP Snooping ARP Security .....	311
DISABLE DHCP Snooping Log .....	312
DISABLE DHCP Snooping Option82 .....	313
ENABLE DHCP Snooping .....	314
ENABLE DHCP Snooping ARP Security .....	316
ENABLE DHCP Snooping Log .....	317
ENABLE DHCP Snooping Option82 .....	318
PURGE DHCP Snooping .....	319
RESET DHCP Snooping Counter .....	320
RESET DHCP Snooping Database .....	321
SET DHCP Snooping CheckInterval .....	322
SET DHCP Snooping CheckOption .....	323
SET DHCP Snooping Macfilter .....	324
SET DHCP Snooping Port .....	326
SHOW DHCP Snooping .....	328
SHOW DHCP Snooping Counter .....	329
SHOW DHCP Snooping Database .....	330
SHOW DHCP Snooping Macfilter .....	331
SHOW DHCP Snooping Port .....	332
<b>Chapter 18: Power Over Ethernet (PoE) Commands .....</b>	<b>333</b>
DISABLE PoE Port .....	334
ENABLE PoE Port .....	335
SET PoE Detect .....	336
SET PoE Guardband .....	337
SET PoE Management .....	338
SET PoE Port .....	339
SET PoE Threshold .....	341
SHOW PoE .....	342
SHOW PoE Port .....	343
<b>Chapter 19: Power Saving Commands .....</b>	<b>345</b>
CREATE Trigger .....	346
DESTROY Trigger .....	349
DISABLE Trigger .....	350
ENABLE Trigger .....	351
PURGE Trigger .....	352
SET LED Mode .....	353
SET LED Port .....	354
SET Trigger .....	356
SHOW LED .....	359
SHOW Trigger .....	360
<b>Chapter 20: Rapid Spanning Tree Protocol (RSTP) Commands .....</b>	<b>361</b>
DISABLE STP .....	362
ENABLE STP .....	363
PURGE STP .....	364
SET STP .....	365
SET STP Port .....	368
SHOW STP .....	371
SHOW STP PortConfig .....	374
SHOW STP PortState .....	375



<b>Chapter 21: Multiple Spanning Tree Protocol (MSTP) Commands</b> .....	<b>377</b>
ADD MSTP MSTI VLAN.....	379
CREATE MSTP MSTI.....	380
DELETE MSTP MSTI VLAN.....	381
DESTROY MSTP MSTI.....	382
DISABLE MSTP.....	383
DISABLE MSTP DEBUG MSTI.....	384
ENABLE MSTP.....	385
ENABLE MSTP DEBUG MSTI.....	387
PURGE MSTP.....	389
RESET MSTP COUNTER PORT.....	390
SET MSTP.....	391
SET MSTP CIST.....	393
SET MSTP CIST PORT.....	394
SET MSTP MSTI.....	397
SET MSTP MSTI PORT.....	398
SHOW MSTP.....	399
SHOW MSTP COUNTER PORT.....	401
SHOW MSTP DEBUG MSTI.....	402
<b>Section IV: Security and Traffic Control</b> .....	<b>403</b>
<b>Chapter 22: Access Filter Commands</b> .....	<b>405</b>
ADD ACCESS FILTER.....	406
DELETE ACCESS FILTER ENTRY.....	408
DISABLE ACCESS FILTER.....	410
ENABLE ACCESS FILTER.....	411
SET ACCESS FILTER.....	412
SET ACCESS FILTER ENTRY.....	413
SHOW ACCESS FILTER.....	415
<b>Chapter 23: Internet Group Management Protocol (IGMP) Snooping Commands</b> .....	<b>417</b>
ADD IGMP Snooping MCGROUP.....	418
DELETE IGMP Snooping.....	421
DISABLE IGMP Snooping.....	422
ENABLE IGMP Snooping.....	423
SET IGMP Snooping.....	424
SET IGMP Snooping MCGROUP.....	426
SHOW IGMP Snooping.....	427
<b>Chapter 24: Multicast Listener Discovery (MLD) Snooping Commands</b> .....	<b>429</b>
ADD MLD Snooping MCGROUP.....	430
DELETE MLD Snooping.....	432
DISABLE MLD Snooping.....	433
ENABLE MLD Snooping.....	434
SET MLD Snooping.....	435
SET MLD Snooping MCGROUP.....	437
SHOW MLD Snooping.....	439
<b>Chapter 25: Quality of Service (QoS) Commands</b> .....	<b>441</b>
DISABLE QoS.....	442
ENABLE QoS.....	443
PURGE QoS.....	444

SET QOS DSCP.....	445
SET QOS HWPRIORITY.....	446
SET QOS HWQUEUE.....	448
SET QOS SCHEDULING.....	449
SHOW QOS.....	450
SHOW QOS DSCP.....	451
SHOW QOS HWPRIORITY.....	452
SHOW QOS HWQUEUE.....	453
SHOW QOS SCHEDULING.....	454
<b>Chapter 26: Policy-Based QoS Commands.....</b>	<b>455</b>
ADD QOS FLOWGROUP.....	457
ADD QOS POLICY.....	458
ADD QOS TRAFFICCLASS.....	459
CREATE CLASSIFIER.....	460
CREATE QOS FLOWGROUP.....	463
CREATE QOS POLICY.....	465
CREATE QOS TRAFFICCLASS.....	468
DELETE QOS FLOWGROUP.....	471
DELETE QOS POLICY.....	472
DELETE QOS TRAFFICCLASS.....	473
DESTROY CLASSIFIER.....	474
DESTROY QOS FLOWGROUP.....	475
DESTROY QOS POLICY.....	476
DESTROY QOS TRAFFICCLASS.....	477
PURGE CLASSIFIER.....	478
RESET QOS POLICY COUNTER.....	479
SET CLASSIFIER.....	480
SET QOS FLOWGROUP.....	483
SET QOS POLICY.....	485
SET QOS TRAFFICCLASS.....	487
SHOW CLASSIFIER.....	489
SHOW QOS FLOWGROUP.....	493
SHOW QOS POLICY.....	494
SHOW QOS POLICY COUNTER.....	495
SHOW QOS TRAFFICCLASS.....	496
<b>Chapter 27: Port-Based Authentication Commands.....</b>	<b>497</b>
ADD PORTAUTH PORT SUPPLICANTMAC.....	499
DELETE PORTAUTH PORT SUPPLICANTMAC.....	501
DISABLE PORTAUTH.....	502
DISABLE PORTAUTH PORT LOGTYPE.....	503
DISABLE WEBAUTHSERVER.....	505
ENABLE PORTAUTH.....	506
ENABLE PORTAUTH PORT LOGTYPE.....	507
ENABLE WEBAUTHSERVER.....	509
SET PORTAUTH AUTHMETHOD.....	510
SET PORTAUTH CSIDFORMAT.....	511
SET PORTAUTH DHCPSEVER.....	513
SET PORTAUTH PORT (Authenticator Port for All Methods).....	514
SET PORTAUTH PORT (802.1X Authenticator Port).....	518
SET PORTAUTH PORT (802.1X Supplicant Port).....	522
SET PORTAUTH PORT (Authenticator Port for MAC and Web).....	524
SET PORTAUTH PORT (Canceling the Authentication Type).....	527
SET PORTAUTH PORT SUPPLICANTMAC.....	528

SET PORTAUTH USERIDFORMAT..... 529  
 SET WEBAUTHSERVER ..... 531  
 SHOW PORTAUTH ..... 532  
 SHOW PORTAUTH PORT AUTHENTICATOR..... 534  
 SHOW PORTAUTH PORT SUPPLICANT ..... 536  
 SHOW WEBAUTHSERVER ..... 538

**Command Index ..... 539**



# Preface

---

This is the command line interface management guide for the AT-GS900M series of Gigabit Ethernet switches. The manual includes how to start a management session and how to manage the switch by using commands in Command Line Interface (CLI).

For how to manage the switch using web browser interface, see the *AT-GS900M Series Web Browser User's Guide*.

This preface contains the following sections:

- ❑ “Document Conventions” on page 14
- ❑ “Where to Find Web-based Guides” on page 15
- ❑ “Contacting Allied Telesis” on page 16



## **Caution**

The software described in this document may contain certain encryption/security or cryptographic functionality and for exporting those products/software, USA export restrictions apply as per 15 C.F.R. Part 730-772 (particularly Part 740.17). At present, as per United States of America's export regulations our products/software cannot be exported to Cuba, Iran, North Korea, North Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please refer to export regulations of USA.

---

# Document Conventions

---

This document uses the following conventions:

---

**Note**

Notes provide additional information.

---

**Caution**

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

---

**Warning**

Warnings inform you that performing or omitting a specific action may result in bodily injury.

---

## Where to Find Web-based Guides

---

The installation and user guides for all of the Allied Telesis products are available for viewing in portable document format (PDF) from our web site at [www.alliedtelesis.com/support/documentation](http://www.alliedtelesis.com/support/documentation).

## Contacting Allied Telesis

---

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at [www.alliedtelesis.com/support](http://www.alliedtelesis.com/support). You can find links for the following services on this page:

- ❑ 24/7 Online Support— Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis experts.
- ❑ USA and EMEA phone support— Select the phone number that best fits your location and customer type.
- ❑ Hardware warranty information— Learn about Allied Telesis warranties and register your product online.
- ❑ Replacement Services— Submit a Return Materials Authorization (RMA) request via our interactive support center.
- ❑ Documentation— View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.
- ❑ Software Downloads— Download the latest software releases for your managed products.

For sales or corporate information, go to [www.alliedtelesis.com/purchase](http://www.alliedtelesis.com/purchase) and select your region.



## Section I

# Getting Started

---

This section contains the following chapters:

- ❑ Chapter 1, "Command Line Interface" on page 19
- ❑ Chapter 2, "Starting a Management Session" on page 23
- ❑ Chapter 3, "Basic CLI Management Commands" on page 37
- ❑ Chapter 4, "Basic Operations" on page 63
- ❑ Chapter 5, "Basic Operations Commands" on page 71



## Chapter 1

# Command Line Interface

---

This chapter has the following sections:

- “Management Sessions” on page 20
- “Manager Account” on page 21
- “Command Format” on page 22

## Management Sessions

---

You can manage the switch locally or remotely. Local management is conducted through the Console port on the switch. Remote management is conducted using Telnet.

### Local Management

To access Command Line Interface (CLI) locally, the switch has a Console port. To start a local management session, you must connect the switch to a terminal or a PC with a terminal emulator program using the management cable.

---

#### Note

The initial management session of the switch must be from a local management session.

---

### Remote Management

You can manage the switch remotely with the following tools:

- Telnet client
- HTTP web browser

Before starting an initial remote management session, you must assign a management IP address to the switch from the local management session. See “Adding a Management IP Address” on page 28.

#### Telnet

The switch has a Telnet server that you can use to access CLI remotely from Telnet clients on your management workstation. Remote Telnet sessions give you access to the same commands and the same management functions as local management sessions.

#### HTTP Web Browser

The switch has a HTTP server. The server is used to remotely manage the switch over the network with a web browser application. Allied Telesis supports MS Internet Explorer.

Before starting an initial management session using HTTP, you must enable the HTTP server on the switch. By default, the HTTP server is disabled. To start a Web session, see “Starting a Remote Management Session Using the Web Browser” on page 27.

## Manager Account

---

You must log on to manage the switch. The switch comes with one manager account. The user name of the account is “manager” and the default password is “friend.” The user name and password are case-sensitive.

## Command Format

---

The following sections describe the command line interface features and the command syntax conventions.

### Command Line Interface Features

The command line interface has these features:

- ❑ Command history - Use the up and down arrow keys.
- ❑ Keyword abbreviations - Any keyword can be recognized by typing an unambiguous prefix, for example, type “sh” and the software responds with “show.”
- ❑ Tab key - Pressing the Tab key fills in the rest of a keyword automatically. For example, typing “sh” and then pressing the Tab key enters “show” on the command line.

### Command Formatting Conventions

This manual uses the following command format conventions:

- ❑ `screen text font` - This font illustrates the format of a command and command examples.
- ❑ [ ] - Brackets indicate optional parameters or keywords.
- ❑ | - Vertical line separates parameter or keyword options for you to choose from.
- ❑ *Italics* - Italics indicate variables you provide.

## Chapter 2

# Starting a Management Session

---

This chapter has the following sections:

- “Overview” on page 24
- “Starting a Local Management Session” on page 25
- “Starting a Remote Management Session Using Telnet” on page 26
- “Adding a Management IP Address” on page 28
- “Changing the Login Password” on page 29
- “Assigning a Name to the Switch” on page 30
- “Keyboard Shortcuts for Command Line Interface” on page 31
- “Using Online Help” on page 33
- “Saving Your Changes” on page 34
- “Starting the Switch with The Default Setting” on page 35
- “Ending a Management Session” on page 36

## Overview

---

You can manage the switch locally or remotely. Local management is conducted through the Console port on the switch. Remote management is performed through Telnet or the Web browser interface from workstations on your network.

---

**Note**

The initial configuration of the switch must be from a local management session. See “Starting a Local Management Session” on page 25.

---

The switch comes with the Telnet server so that you can start a remote management session through a Telnet client on your management workstation.

### Requirements for Remote Management

Here are the requirements for remote management of the switch from a Telnet client on your network:

- ❑ You must assign the switch a management IP address to access the switch using Telnet and the Web browser. For instructions, see or “Adding a Management IP Address” on page 28.
- ❑ The management workstation must be a member of the same subnet as the management IP address on the switch, or must have access to the switch through routers or other Layer 3 devices.

---

**Note**

To manage the switch through the web browser interface, see the *AT-GS900M Series Switch Web Browser User’s Guide*.

---

### What to Configure First

Here are a few suggestions on what to configure during your initial management session of the switch:

- ❑ “Adding a Management IP Address” on page 28
- ❑ “Changing the Login Password” on page 29
- ❑ “Assigning a Name to the Switch” on page 30



## Starting a Local Management Session


---

To start a local management session on the switch, perform the following procedure:

1. Connect the RJ-45 connector on the management cable to the console port on the switch. The Console port is located on the back panel on the AT-GS900M series switch.
2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
  - Baud rate: 9600 bps
  - Data bits: 8
  - Stop bits: 1
  - Parity: None
  - Flow control: None
4. Press Enter on the terminal or terminal emulator program on the PC.  
You are prompted for a user name and password.
5. Enter a user name and password.

If this is the initial management session of the switch, enter “manager” as the user name “friend” as the password. The user name and password are case-sensitive.

When your login is successful, the command line prompt appears as shown in Figure 1.



```
Manager >
```

Figure 1. Command Line Prompt

## Starting a Remote Management Session Using Telnet

---

The switch has a Telnet server installed. You can use Telnet to manage the switch remotely.

To start a Telnet management session, perform the following procedure:

1. Assign a management IP address to the switch.

See “Adding a Management IP Address” on page 28.

2. In the Telnet client on your remote management workstation, enter the management IP address of the switch.

Prompts are displayed for a user name and password.

3. Enter a user name and password of a management account on the switch.

The switch comes with one management account. The user name is “manager” and the password is “friend.” User names and passwords are case-sensitive.

The management session starts and the command line interface prompt is displayed, as shown in Figure 1 on page 25.

---

**Note**

The Telnet server is enabled on the switch by default.

---

## Starting a Remote Management Session Using the Web Browser

---

The switch has an HTTP server installed. You can use HTTP to manage the switch through the Web browser.

To start a HTTP management session, perform the following procedure:

1. Assign a management IP address to the switch.

See “Adding a Management IP Address” on page 28.

2. Enable the HTTP server on the switch.

See “ENABLE HTTP SERVER” on page 175.

3. Open a web browser on the management workstation.

4. Enter the management IP address of the switch followed by `htt://`.

For example, `http://192.168.1.1`

The AT-GS900 series switch login page is displayed.

5. Enter a user name and password of a management account on the switch.

The switch comes with one management account. The user name is “manager” and the password is “friend.” User names and passwords are case-sensitive.

---

**Note**

The HTTP server is disabled on the switch by default.

---

## Adding a Management IP Address

---

You must assign the switch a management IP address to start a remote management session. The switch can have one IPv4 address on the switch.

The following example assigns the switch the IPv4 management address 192.168.0.3, the subnet mask of 255.255.255, and the default gateway 192.168.0.255:

```
Manager > set ip ipaddress=192.168.0.3 mask=255.255.255.0  
gateway=192.168.0.255
```

The following example assigns the switch the IPv4 management address from the DHCP server:

```
Manager > enable ip dhcp  
Manager > set ip ipaddress=dhcp
```

## Changing the Login Password

---

To protect the switch from unauthorized access, change the password of the manager account. The password is set with the SET PASSWORD command. Here is the format of the command.

```
set password
```

The password is case-sensitive. The password can be from 0 to 16 alphanumeric characters. When no password is specified, you can login to the switch without password.

The following example of the command changes the password of the manager account to "clearsky2a":

```
Manager > set password
```

```
Old password : xxxxxx  
New password : xxxxxxxx  
Confirm      : xxxxxxxx
```

```
Password has been changed
```

---

**Note**

Write down the new password and keep it in a safe and secure location. When you forget the manager password, you are not able to manage the switch. Contact Allied Telesis Technical Support for assistance.

---

## Assigning a Name to the Switch

---

The switch is easier to identify if you assign the switch a name. The switch's name replaces the "Manager" in the command line prompt.

A name is assigned to the switch with the SET SYSTEM command. Here is the format of the command:

```
set system name=name
```

The following example assigns the switch the name "Switch1":

```
Manager > set system name=Switch1  
Switch1 >
```

## Keyboard Shortcuts for Command Line Interface

---

The useful keyboard shortcuts are listed in Table 1.

Table 1. Basic Command Line Commands

Keyboard Shortcut	Description
Ctrl + a	Moves the cursor to the beginning of the line.
Ctrl + b or ←	Moves the cursor one character to the left.
Ctrl + c	Stops executing the command and returns to the command prompt.
Ctrl + d	Deletes the selected character or logout if no character is selected.
Ctrl + e	Moves the cursor to the end of the line.
Ctrl + f or →	Moves the cursor one character to the right.
Ctrl + h or backspace	Deletes a character left to the cursor.
Ctrl + i or tab	Performs one of the following: <ul style="list-style-type: none"> <li>❑ Enter the shortcut with no character: the first words of the available commands are listed.</li> <li>❑ Enter the shortcut with a partial command: it expands the command.</li> <li>❑ Enter the shortcut with a command: available keywords for the command are displayed.</li> </ul>
Ctrl + k	Deletes all characters from the cursor to the end of the line.
Ctrl + n or ↓	Displays the next line in the command history.
Ctrl + p or ↑	Displays the previous line in the command history.
Ctrl + u	Deletes all characters at the command line.
Delete	Deletes highlighted characters.

Table 1. Basic Command Line Commands (Continued)

<b>Keyboard Shortcut</b>	<b>Description</b>
Spacebar	Performs one of the following: <ul style="list-style-type: none"><li data-bbox="802 365 1390 464">❑ Enter the shortcut with no character: the first words of the available commands are listed.</li><li data-bbox="802 478 1409 548">❑ Enter the shortcut with a partial command: it expands the command.</li><li data-bbox="802 562 1373 661">❑ Enter the shortcut with a command: available keywords for the command are displayed.</li></ul>
F1 or ?	Displays online help.



## Using Online Help

---

The AT-GS900M Series CLI provides online help.

- ❑ When you enter the HELP command without parameters as shown below, a list of the help topics is displayed.

```
Manager > help
```

- ❑ When you enter the HELP command with a topic, the help information about the topic is displayed. For example:

```
Manager > help vlan
```

- ❑ When you type a command in the command line and press the F1 key, the description of the command is displayed. For example:

```
Manager > set system
```

Then, press the F1 key.

## Saving Your Changes

---

The switch does not save changes when you shut down or restart the switch. If you want to restart the switch with the configuration that you changed, save changes into a configuration file and assign the configuration file as the start-up configuration file.

To save the changes to a configuration file, do the following:

1. View the configuration files that are currently saved on the switch by using the SHOW FILE command:

```
Manager > show file
```

2. Save the changes into a configuration file of *config1.cfg* using the CREATE command:

```
Manager > create config=config1.cfg
```

If a file with the same name already exists, the switch overwrites the file.

3. Assign the file as a start-up configuration file using the SET CONFIG command.

```
Manager > set config=config1.cfg
```

4. Restart the switch

```
Manager > restart
```

## Starting the Switch with The Default Setting

---

To start the switch with the default settings, do the following:

1. Assign the startup configuration as none using the SET CONFIG command:

```
Manager > set config=none
```

2. Restart the switch

```
Manager > restart
```

## Ending a Management Session

---

The following commands ends the current management session:

- LOGOUT
- LOGOFF
- QUIT
- EXIT
- BYE

---

**Note**

Pressing [Ctrl] + D also ends the current session when no command is at the prompt.

---

The following example ends the session:

```
Manager > logoff
```

## Chapter 3

# Basic CLI Management Commands

The basic Command Line Interface (CLI) management commands are summarized in Table 2.

Table 2. Basic CLI Management Commands

Command	Description
“BYE” on page 39	Ends the current management session.
“CLS” on page 40	Clears the screen.
“DISABLE SYSTEM FAN-STARTSTOP-ALARM” on page 41	Disables sending alarm messages when the fan starts or stops.
“ENABLE SYSTEM FAN-STARTSTOP-ALARM” on page 42	Enables sending alarm messages when the fan starts or stops.
“EXIT” on page 43	Ends the current management session.
“HELP” on page 44	Displays help information.
“LOGOFF” on page 46	Ends the current management session.
“LOGOUT” on page 47	Ends the current management session.
“QUIT” on page 48	Ends the current management session.
“RESTART” on page 49	Resets the hardware components of the switch and restart the switch
“SET INSTALL” on page 50	Specifies a configuration file as the boot configuration file.
“SET PASSWORD” on page 51	Changes the login password.
“SET SYSTEM” on page 52	Sets values for the sysName, sysLocation, and sysContact MIB objects.
“SET SYSTEM SFP-TEMPTHRESHOLD” on page 53	Sets the temperature threshold for SFP modules. When the temperature exceeds this value, the switch sends alarm messages.
“SET TIME” on page 54	Sets the system time and date.
“SHOW CPU” on page 55	Displays the CPU usage of the switch.

Table 2. Basic CLI Management Commands (Continued)

<b>Command</b>	<b>Description</b>
“SHOW DEBUG” on page 56	Displays the debug information.
“SHOW INSTALL” on page 57	Displays the name of the boot configuration file.
“SHOW SYSTEM” on page 58	Displays the system information.
“SHOW TIME” on page 61	Displays the system time.

# BYE

---

## Syntax

bye

## Parameters

None

## Description

Use this command to end the current management session.

The LOGOFF, LOGOUT, QUIT, and EXIT commands do the same as the BYE command.

## Example

The following command ends the current management session:

```
Manager > bye
```

# CLS

---

## **Syntax**

`cls`

## **Parameters**

None

## **Description**

Use this command to clear the screen.

## **Example**

This example clears the screen:

```
Manager > cls
```



## DISABLE SYSTEM FAN-STARTSTOP-ALARM

---

### Syntax

```
disable system fan-startstop-alarm
```

### Parameters

None

### Description

Use this command to stop sending alarm messages when the fan starts and stops. Alarm messages are:

- SNMP trap
- Syslog message
- Log message
- Event message

By default, when the fan starts and stops, the switch sends alarm messages.

### Confirmation Command

“SHOW SYSTEM” on page 58

### Example

The following example disables the fan and alarm messages:

```
manager > disable system fan-startstop-alarm
```

## ENABLE SYSTEM FAN-STARTSTOP-ALARM

---

### Syntax

```
enable system fan-startstop-alarm
```

### Parameters

None

### Description

Use this command to send alarm messages when the fan starts and stops. Alarm messages are:

- SNMP trap
- Syslog message
- Log message
- Event message

By default, when the fan starts and stops, the switch sends alarm messages.

### Confirmation Command

“SHOW SYSTEM” on page 58

### Example

The following example enables the fan and alarm messages:

```
manager > enable system fan-startstop-alarm
```

# EXIT

---

## Syntax

`exit`

## Parameters

None

## Description

Use this command to end the current management session.

The LOGOFF, LOGOUT, QUIT, and BYE commands do the same as the EXIT command.

## Example

The following command ends the current management session:

```
Manager > exit
```

# HELP

---

## Syntax

```
help [command|topic]
```

## Parameters

*command*

Specifies a command such as set password, create file, etc.

*topic*

Specifies a topic keyword listed in Table 3.

## Description

Use this command to display information about a specified command, information about a specified topic, a list of available topics.

Without a command or topic specified, the command displays a list of available help topics. Table 3 shows help a list of topics that you can specify with this command.

Table 3. Help Topic Keywords

Topic keyword (shortcut key)	Help Topic
accessfilter (a)	Access filter
classifier (cl)	Classifier
configuration (co)	Configuration
epsr (e)	EPSR transit aware
fdb (fd)	MAC address table (forwarding database)
filesystem (fi)	File system
http (h)	HTTP
igmpsnooping (ig)	IGMP snooping
ip	IP
loader (loade)	Loader
log	Log
loopdetection (loo)	Loop detection

Table 3. Help Topic Keywords (Continued)

Topic keyword (shortcut key)	Help Topic
mld Snooping (ml)	MLD snooping
mstp (ms)	MSTP
ntp (n)	NTP
poe	PoE
portauth (ports)	Port authentication
portlead (portl)	Port LED
qos (qo)	QoS
radius (r)	Radius
script (sc)	Script
snmp (sn)	SNMP
stormdetection (sto)	Storm detection
stp	STP
switch (sw)	Switch
system (sy)	System
Terminal (t)	Terminal service
trigger (tr)	Trigger
vlan (v)	VLAN
webauthserver (we)	Web Authentication Server
keybind (k)	Key bind

**Example**

The following command displays a list of help topics:

```
Manager > help
```

The following command displays about the SET CPU command:

```
Manager > help set cpu
```

The following command displays information about VLAN:

```
Manager > help v
```

## LOGOFF

---

### Syntax

logoff

### Parameters

None

### Description

Use this command to end the current management session.

The LOGOUT, QUIT, EXIT, and BYE commands do the same as the LOGOFF command.

### Example

The following command ends the current management session:

```
Manager > logoff
```

# LOGOUT

---

## Syntax

logout

## Parameters

None

## Description

Use this command to end the current management session.

The LOGOUT, QUIT, EXIT, and BYE commands do the same as the LOGOFF command.

## Example

The following command ends the current management session:

```
Manager > logout
```

# QUIT

---

## Syntax

`quit`

## Parameters

None

## Description

Use this command to end the current management session.

The LOGOFF, LOGOUT, BYE, and EXIT commands do the same as the QUIT command.

## Example

The following command ends the current management session:

```
Manager > quit
```



# RESTART

---

## Syntax

restart

## Parameters

None

## Description

Use this command to reset the hardware components and restart the switch.

## Example

The following command prompts you to confirm to reboots the switch. At the prompt, type y:

```
Manager > restart
```

```
Do restart system now? (Y/N):
```

## SET INSTALL

---

### Syntax

```
set install=preferred release=software_file
```

### Parameter

*software\_file*

Specifies the name of the management software image file. The file name must be in the following format:

```
gs900mv2_vnnnn.rel
```

---

### Note

The preferred keyword is the only option to set install command.

---

### Description

Use this command to select a software image file as the boot configuration file that runs on the switch next time the switch reboots. The switch can save up to two management software image files in the file system.

### Confirmation Command

“SET INSTALL” on page 50

### Example

The following command selects the gs900mv2\_v232.rel image file as the boot configuration file to run on the switch after the switch reboots:

```
manager > set install=preferred release=gs900mv2_v232.rel
```

# SET PASSWORD

---

## Syntax

```
set password
```

## Parameters

None

## Description

Use this command to change the login password. The password can be up to 16 alphanumeric characters. Special characters and spaces are allowed. The password is case-sensitive. When no password is entered, you can login without password.

## Confirmation Command

“SHOW SYSTEM” on page 58

## Example

The following command prompts you to enter passwords. At the prompt, type your new password.

```
Manager > set password
```

```
Old password: *****
```

```
New password: *****
```

```
Confirm      : *****
```

```
Password has been changed.
```

## SET SYSTEM

---

### Syntax

```
set system name="system_name" | location="location_name" |  
contact="contact_name"
```

### Parameter

*system\_name*

Specifies a value for the sysName MIB object.

*location\_name*

Specifies a value for the sysLocation MIB object.

*contact\_name*

Specifies a value for the sysContact MIB object.

### Description

Use this command to specify the values of MIB objects: sysName, sysLocation, and sysContact:

### Confirmation Command

“SHOW SYSTEM” on page 58

### Example

The following command specifies the value of the sysName MIB object to GS916MV2:

```
manager > set system name="GS926MV2"
```

The following command deletes the value of the sysLocation MIB object:

```
Manager > set system loaction=""
```

## SET SYSTEM SFP-TEMPTHRESHOLD

---

### Syntax

```
set system sfp-tempthreshold=temperature
```

### Parameter

*temperature*

Specifies the temperature threshold. The value must be 40, 45, or 50°C.

### Description

Use this command to set the temperature threshold for the SFP modules. When the internal temperature of the SFP module exceeds the temperature threshold, the switch sends alarm messages such as SNMP traps and log messages.

By default, the temperature threshold for the GS908M V2 and GS924M V2 switches is 45°C and one for the GS916M V2 switch is 50°C.

Here are the guidelines for setting the temperature threshold for the SFP module:

- ❑ When the AT-SPLX40, AT-SPZ80, AT-SPBD80-A, or AT-SPBD80-B SFP module is attached to the GS908M V2 or GS924M V2 switch, the temperature threshold must be 45°C.
- ❑ This command is available only for the GS908M V2, GS916M V2, and GS924M V2 switches.

### Confirmation Command

“SHOW SYSTEM” on page 58

### Example

The following command specifies the temperature threshold for SFP modules to 40°C:

```
manager > set system sfp-tempthreshod=40
```

## SET TIME

---

### Syntax

```
set Time=time|date=date
```

### Parameter

*time*

Specifies the system time. The format is hh:mm:ss.

*date*

Specifies the system date. The format is yyyy-mm-dd.

### Description

Use this command to specify the system time and system date.

### Confirmation Command

“SHOW TIME” on page 61

### Example

The following command specifies the system time to 9:15AM and system date to July 7, 2014:

```
Manager > set time=09:15:00 date=2014-07-07
```

The following command changes only the system time:

```
Manager > set time=08:45:00
```

## SHOW CPU

---

### Syntax

show cpu

### Parameter

None

### Description

Use this command to display the CPU usage. See Figure 2 for an example of the command output.

```
CPU Utilisation ( as a percentage )
-----
Average over last second ..... 9
Average over last minute ..... 8
Average over last 5 minutes ..... 5
Average over last 15 minutes ..... 6
-----
```

Figure 2. SHOW CPU Command

### Example

The following command displays the CPU usage of the switch:

```
manager > show cpu
```

# SHOW DEBUG

---

### Syntax

show debug

### Parameter

None

### Description

Use this command to display the debug information. See Figure 3 for an example of the command output.

```
SHOW SYSTEM
:
SHOW FILE
:
SHOW CONFIG DYNAMIC
:
SHOW LOG
:
SHOW CRASHLOG
```

Figure 3. SHOW DEBUG Command

### Example

The following command displays the debug information of the switch:

```
Manager > show debug
```



## SHOW INSTALL

---

### Syntax

```
show install
```

### Parameter

None

### Description

Use this command to display the management software information. See Figure 4 for an example of the command output.

```

Install      Release
-----
Preferred   flash:gs900mv2_v232.re1
-----

Current install
-----
Preferred   flash:gs900mv2_v232.re1
-----

```

Figure 4. SHOW INSTALL Command

The fields are described in Table 4.

Table 4. SHOW INSTALL Command

Field	Description
Install Release	Displays the name of the software image file that is selected to run the switch by the SET INSTALL command. See "SET INSTALL" on page 50.
Current Install	Displays the name of the software image file that is currently running.

### Example

The following command displays the management software information:

```
manager > show install
```

## SHOW SYSTEM

---

### Syntax

```
show system
```

### Parameter

None

### Description

Use this command to display the system information of the switch. See Figure 5 for an example of the command output.

```
Switch System Status                               Date 2011-05-19 Time 13:58:46
Board      Bay      Board Name
-----
Base       -        GS916M V2
-----
Memory -   DRAM : 65536 kB  FLASH : 16384 kB  MAC : 00-00-F4-27-2D-77
-----
SysDescription : CentreCOM GS916M V2 Ver 2.3.2 B04
SysContact      :
SysLocation     :
SysName         :
SysUpTime       : 831900(02:18:39)
Release Version : 2.3.2
Release built   : B04 (Apr 21 2011 at 16:43:27)

Flash PROM      : Good
RAM             : Good
SW chip         : Good
UART            : Good
PoE             : Good

FAN1           : Normal
1.2V           : Normal          2.5V           : Normal
3.3V           : Normal          12.0V          : Normal
Temperature     : Normal

SFP Temperature Threshold : 45 C
FAN START/STOP ALARM      : Enabled

Configuration
Boot configuration file : system.cfg (exist)
Current configuration   : system.cfg
```

Figure 5. SHOW SYSTEM Command

The fields are described in Table 5.

Table 5. SHOW SYSTEM Command

Field	Description
Bay	N/A
Board Name	Displays the name of the device.
DRAM	Displays the size of the DRAM on the switch.
FLASH	Displays the size of the FLASH memory on the switch.
MAC	Displays the MAC address of the switch.
SysDescription	Displays the system description, the value of the sysDesr MIB-II object.
SysContact	Displays the contact, the value of the sysContact MIB-II object.
SysLocation	Displays the location, the value of the sysLocation MIB-II object.
SysName	Displays the contact, the value of the sysName MIB-II object.
SysUpTime	Displays the time since the switch last restarted.
Release Version	Displays the version of the management software
Release built	Displays the time stamp of the management software.
Flash PROM	Displays the result of the checksum calculation for the program data in Flash memory. The options are Good and Failed.
RAM	Displays the result of the RAM test at rebooting. The options are Good and Failed.
SW chip	Displays the result of the switch chip test at rebooting. The options are Good and Failed.
UART	Displays the result of the UART test at rebooting. The options are Good and Failed.
PoE	Displays the result of the PoE test at rebooting. The options are Good and Failed. It is available only for GS908M V2-4PS models.
FAN1	Displays the status of the fan. The options are Normal, Warning, and Failed. Failed means that the switch failed to read the data. It is not available for GS908M V2 models.

Table 5. SHOW SYSTEM Command (Continued)

Field	Description
1.2V	Displays the status of each power supply. The options are Normal, Warning, and Failed. Failed means that the switch failed to read the data. The status of 12V is not available for GS908M V2 models.
2.5V	
3.3V	
12V	
Temperature	Displays the status of the internal temperature. The options are Normal, Warning, and Failed. Failed means that the switch failed to read the data.
SFP Temperature Threshold	Displays the temperature threshold when the SFP module is attached to the switch. The options are 40°C, 45°C or 50°C. It is not available for GS908M V2-4PS models.
FAN START/STOP ALARM	Displays the setting of alarm messages when the fan starts and stops. The options are enabled and disabled. It is not available for GS908M V2-4PS models.
Boot Configuration file	Displays the name of the boot configuration file.
Current configuration	Displays the name of the configuration file that is currently running the switch.

**Example**

The following command displays the system information:

```
Manager > show system
```

# SHOW TIME

---

## Syntax

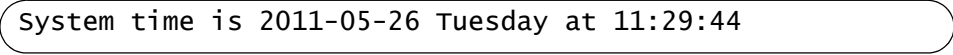
```
show time
```

## Parameter

None

## Description

Use this command to display the system time of the switch. See Figure 6 for an example of the command output.

The output of the 'show time' command is displayed within a rounded rectangular border. The text inside the border reads: 'System time is 2011-05-26 Tuesday at 11:29:44'.

```
System time is 2011-05-26 Tuesday at 11:29:44
```

Figure 6. SHOW TIME Command

## Example

The following command displays the system time of the switch:

```
Manager > show time
```



## Chapter 4

# Basic Operations

---

This chapter has the following sections:

- “File System Overview” on page 64
- “Downloading a File to the Switch” on page 65
- “Uploading a File from the Switch” on page 67
- “Updating the Management Software” on page 69

## File System Overview

---

The switch has a file system built in the flash memory. You can access files on the file system using CLI commands.

**File Types** The file types that you can store on the file system on the switch are listed in Table 6:

Table 6. File Type and File Extension

File Type	Extension
Configuration file	.cfg
Script file such as batch and trigger	.scp
Management software image file	.rel

**File Name** Here are the requirement for a file name:

- The file name must be up to 16 alphanumeric characters without a period and file extension.
- The file name is case-sensitive.
- The file name can include hyphen, underscore, period, and parentheses.



## Downloading a File to the Switch

---

You can download files onto the switch either from TFTP server or using FTP. You can download the following file types to the switch:

- ❑ New releases of the management software (.rel)
- ❑ Configuration files (.cfg)
- ❑ Script file (.scp)

### Downloading a File from a TFTP Server

To download a configuration file from a TFTP server, use LOAD command.

The following example downloads the file config1.cfg on the TFTP server to the switch. The TFTP server has an IP address of 192.168.10.10:

```
Manager > load method=TFTP FILE=config1.cfg
server=192.168.10.10
```

To download a software image file from a TFTP server, use LOAD command with the FIRMWARE keyword.

The following example downloads the software image file *gs900mv2\_v232.re1* to the switch. The TFTP server has an IP address of 192.168.10.10:

```
manager > load method=TFTP FILE=gs900mv2_v232.re1
server=192.168.10.10 firmware
```

### Downloading a File Using FTP

To download a configuration file using FTP, perform the following steps:

1. From the command prompt of the management workstation, type the following commands. The IP address of FTP server is 192.168.10.5:

```
C:\> FTP 192.168.10.5
```

2. Enter the user name at the prompt:

```
Connected to 192.168.10.5
220 FTP server ready.
User (192.168.10.5:(none)): manager
```

3. Enter the password at the prompt:

```
331 Password required for manager
Password: *****
```

4. After the login, enter the file transfer PUT command at the FTP prompt:

```
230 User logged in.
ftp> put config2.cfg
```

5. Confirm that the file is transferred successfully.

The following is a message example:

```
200 PORT command successful.  
150 Opening ASCII mode data connection for config2.cfg.  
266 Transfer Complete.  
fgp: 546 bytes received in 0.03 Seconds 17.61 kbytes/sec.  
  
ftp>
```

## Uploading a File from the Switch

---

You can save files from the switch to the TFTP server or transfer files on the switch to the FTP client.

### Uploading a File to a TFTP Server

To upload a configuration file on the switch to a TFTP server, use the `UPLOAD` command.

The following example uploads the file `config3.cfg` on the switch to the TFTP server. The TFTP server has the IP address of `192.168.10.10`:

```
Manager > upload method=TFTP FILE=config3.cfg
server=192.168.10.10
```

You may fail to upload files onto a TFTP server. You may need to create files and give write permission for all users before uploading files from the switch. The following example creates a file, `config3.cfg` on a TFTP server and gives write permission to all users:

```
UNxNOS[1]# cd/tftpboot
UNxNOS[2]# touch config3.cfg
UNxNOS[3]# chmod 666 config3.cfg
```

### Uploading a File Using FTP

To transfer a configuration file on the switch to the FTP client, perform the following steps:

1. From the command prompt of the management workstation, type the following commands. The IP address of FTP server is `192.168.10.5`:

```
C:\> FTP 192.168.10.5
```

2. Enter the user name at the prompt:

```
Connected to 192.168.10.5
220 FTP server ready.
User (192.168.10.5:(none)): manager
```

3. Enter the password at the prompt:

```
331 Password required for manager
Password: *****
```

4. After logging in, enter the file transfer `GET` command at the FTP prompt:

```
230 User logged in.
ftp> get config4.cfg
```

5. Confirm that the file is transferred successfully.

The following is a message example:

```
200 PORT command successful.  
150 Opening ASCII mode data connection for config1.cfg.  
266 Transfer Complete.  
fgp: 546 bytes received in 0.03Seconds 17.61Kbytes/sec.
```

```
ftp>
```

## Updating the Management Software

---

When a new release of management software for the AT-GS900M Series switch is available, the image file will be posted on the Allied Telesis website.

To update the management software on the switch, download the file from the switch using either TFTP server or FTP server.

Here are the guidelines for updating the management software:

- ❑ You must assign the switch a management IP address. See “Adding a Management IP Address” on page 28.
- ❑ There must be a TFTP server or FTP server on your network.
- ❑ The management software image file has the rel file extension.
- ❑ The switch can store only two management software image files.

### Updating the Management Software Using TFTP

To update the management software using TFTP, perform the following tasks:

1. Download the new management software from the Allied Telesis website and store it on the TFTP server on your network.
2. Start a local or remote management session on the switch.
3. Check for the space on the system by using the SHOW FILE command.

If the switch has two management software image files, delete one or both files. In addition, make free space by deleting other files if necessary.

4. Download the management software image file from TFTP server by using LOAD command. See “LOAD” on page 80.



#### Caution

Do not turn off the switch during the downloading and writing process. When powered off during the process, the switch may not restart.

---

5. Restart the switch using the RESTART command.

### Updating the Management Software Using FTP

To update the management software using FTP, perform the following tasks:

1. Download the new management software from the Allied Telesis website and store it on the FTP server on your network.

2. Start a local or remote management session on the switch.
3. Check for the space on the system by using the SHOW FILE command.

If the switch has two management software image files, delete one or both files. In addition, make free space by deleting other files if necessary.

---

**Note**

The switch can store only two management software image files.

---

4. Download the management software image file from FTP server by using LOAD command. See “LOAD” on page 80.



**Caution**

Do not turn off the switch during the downloading and writing process. When powered off during the process, the switch may not restart.

---

5. Restart the switch using the RESTART command.

## Chapter 5

# Basic Operations Commands

The basic operations commands are summarized in Table 7.

Table 7. Basic Operations Commands

Command	Description
“ACTIVATE SCRIPT” on page 73	Runs the specified script.
“CLEAR FLASH TOTALLY” on page 74	Deletes all the files stored on the flash memory.
“COPY” on page 75	Copies a configuration file in the flash memory.
“CREATE CONFIG” on page 76	Copies a configuration file in the system memory and save it in the flash memory.
“DELETE FILE” on page 77	Deletes a file from the flash memory.
“DISABLE FTP SERVER” on page 78	Disables the FTP server on the switch.
“ENABLE FTP SERVER” on page 79	Enables the FTP server on the switch.
“LOAD” on page 80	Downloads a file from the TFTP server.
“SET CONFIG” on page 81	Specifies a configuration file as the boot configuration file.
“SET FTP LISTENPORT” on page 82	Changes the TCP port for FTP control.
“SET LOADER” on page 83	Sets the values for the LOAD and UPLOAD commands.
“SET TFTP LISTENPORT” on page 84	Changes the UDP port for the TFTP server.
“SHOW CONFIG” on page 85	Displays a list of configuration files stored in the switch or the content of the specified configuration file.
“SHOW FILE” on page 86	Displays a list of files stored in the switch or the content of the specified file.
“SHOW FTP” on page 88	Displays the settings of the FTP server.

Table 7. Basic Operations Commands (Continued)

<b>Command</b>	<b>Description</b>
"SHOW LOADER" on page 89	Displays the settings of the loader.
"SHOW TFTP" on page 90	Displays the UDP port for the TFTP server.
"UPLOAD" on page 91	Uploads configuration or script files to the TFTP server.



## ACTIVATE SCRIPT

---

### Syntax

```
activate script=file_name
```

### Parameter

*file\_name*

Specifies a .cfg or .scp.

### Description

Use this command to run the specified script. A running command is displayed after the =>.

### Example

The following command runs the system.cfg and shows running commands:

```
Manager > activate script=system.cfg
```

```
=> add ip interface=default ipaddress=192.168.1.5  
mask=255.255.255.0
```

```
Operation successful.
```

```
=> enable ntp
```

```
Operation successful.
```

```
=> add ntp peer=192.168.1.1
```

```
Operation successful.
```

## **CLEAR FLASH TOTALLY**

---

### **Syntax**

```
clear flash totally
```

### **Parameters**

None

### **Description**

Use this command to delete all the files stored on the flash memory except the management software image file that the system is currently running of.

### **Confirmation Command**

“SHOW CONFIG” on page 85

### **Example**

The following command initializes the flash memory on the switch:

```
Manager > clear flash totally
```

# COPY

---

## Syntax

```
copy sourcefile_name destfile_name
```

## Parameters

*sourcefile\_name*

Specifies the name of a configuration file you want to copy.

*destfile\_name*

Specifies the name of the new copy of the file. The destination filename can be from 1 to 20 alphanumeric characters. It is case-sensitive. The extension must be “.cfg” or “.scp.” The file name can include hyphen (-), underscore (\_), period (.), and parentheses (()).

## Description

Use this command to copy a configuration file in the Flash memory on the switch. You cannot copy software image file (.rel).

## Confirmation Command

“SHOW FILE” on page 86

## Examples

This command copies the configuration file “test1.cfg” and saves it as “test1backup.cfg”:

```
Manager > copy config1.cfg config2.cfg
```

## CREATE CONFIG

---

### Syntax

```
create config=file_name
```

### Parameters

*file\_name*

Specifies the name of a new file. The file name can be from 1 to 20 alphanumeric characters including a period and extension. The file name is case-sensitive. The extension must be “.cfg” or “.scp.” The file name can include hyphen (-), underscore (\_), period (.), and parentheses (()).

### Description

Use this command to copy a configuration file on the system memory and save it on the flash memory. If the new file name is the same as the name of an existing file, the command overwrites the existing file.

### Confirmation Command

“SHOW CONFIG” on page 85

### Example

The following command copies the configuration on the system memory and saves it as the config2.cfg file on the flash memory:

```
Manager > create config=config2.cfg
```

## DELETE FILE

---

### Syntax

```
delete file=file_name
```

### Parameter

*filename*

Specifies the file name of a file to delete from the switch. You can also specify a file name using one wild card (\*). The wild card (\*) must be at the beginning or end of the file name.

### Description

Use this command to delete a file from the switch.

### Confirmation Command

“SHOW FILE” on page 86

### Example

The following command deletes the management software image file `gs900mv2_v232.rel`:

```
Manager > delete file=gs900mv2_v232.rel
```

The following command deletes all the files with the `.scp` extension:

```
Manager > delete file=*.scp
```

## DISABLE FTP SERVER

---

### Syntax

```
disable ftp server
```

### Parameters

None

### Description

Use this command to disable the FTP server on the switch. By default, the FTP server is enabled.

### Confirmation Command

“SHOW FTP” on page 88

### Example

The following command disables the FTP server:

```
Manager > disable ftp server
```

## ENABLE FTP SERVER

---

### Syntax

```
enable ftp server
```

### Parameters

None

### Description

Use this command to enable the FTP server on the switch. By default, the FTP server is enabled.

### Confirmation Command

“SHOW FTP” on page 88

### Example

The following command enables the FTP server:

```
Manager > enable ftp server
```

# LOAD

---

## Syntax

```
load [method=tftp] [file=file_name] [destfile=file_name]
[server=ip_address] [firmware]
```

## Parameters

*file*

Specifies the path and name of a file to download.

*destfile*

Specifies a new file name for the downloaded file.

*file\_name*

The file name can be from 1 to 20 alphanumeric characters including a period and extension. The extension can be .cfg, .scp., or .rel. It is case-sensitive. The file name can include hyphen (-), underscore (\_), period (.), and parentheses (()).

*ip\_address*

Specifies the IPv4 address of TFTP server.

*firmware*

Specifies a management software image file to be downloaded. The management software image file has the rel file extension.

## Description

Use this command to download a configuration, script or management software image file from a TFTP server.

## Confirmation Command

“SHOW LOADER” on page 89

“SHOW TFTP” on page 90

## Example

The following command downloads the gs900mv2\_v232.rel file from the TFTP server with the IP address of 192.168.1.1:

```
manager> load method=tftp file=gs900mv2_v232.rel
server=192.168.1.1 firmware
```



# SET CONFIG

---

## Syntax

```
set config=[file_name|none]
```

## Parameters

*file\_name*

Specifies the name of a configuration file. When rebooting, the switch uses this file as the start-up configuration file.

none

Specifies no file. When rebooting, the switch starts with the default configuration.

## Description

Use this command to assign the start-up configuration file.

## Confirmation Command

“SHOW CONFIG” on page 85

## Example

The following command resets the switch to the default configuration:

```
Manager> set config=none
```

The following command assigns the config3.cfg file as the start-up configuration file:

```
Manager> set config=config3.cfg
```

## SET FTP LISTENPORT

---

### Syntax

```
set ftp listenport=port_number
```

### Parameter

*port\_number*

Specifies the port number of TCP port for FTP control. The port number is from 1 to 65535.

### Description

Use this command to change the TCP port for FTP control. By default, the FTP control port is 21.

### Confirmation Command

“SHOW FTP” on page 88

### Example

The following command changes the TCP port for FTP control to 150.

```
Manager> set ftp listenport=150
```

# SET LOADER

---

## Syntax

```
set loader [method=tftp] [file=file_name]  
[destfile=file_name] [server=ip_address]
```

## Parameters

*file*

Specifies the path and name of a file to download.

*destfile*

Specifies a new file name for the downloaded file.

*file\_name*

The file name can be from 1 to 20 alphanumeric characters including a period and extension. The extension can be .cfg, .scp., or .rel. It is case-sensitive. The file name can include hyphen (-), underscore (\_), period (.), and parentheses ().

*ip\_address*

Specifies the IPv4 address of TFTP server.

## Description

Use this command to set parameters that are used for the LOAD and UPLOAD commands.

## Confirmation Command

“SHOW LOADER” on page 89

## Example

The following command specifies the IP address of the TFTP server:

```
Manager> set loader server=192.168.1.1
```

## SET TFTP LISTENPORT

---

### Syntax

```
set tftp listenport=port_number
```

### Parameter

*port\_number*

Specifies the port number of UDP port for the TFTP server. The port number is from 1 to 65535.

### Description

Use this command to change the UDP port for the TFTP server. By default, the UDP port for the TFTP server is 69.

### Confirmation Command

“SHOW TFTP” on page 90

### Example

The following command changes the UDP port for the TFTP server to 100.

```
Manager> set tftp listenport=100
```

# SHOW CONFIG

---

## Syntax

```
show config [dynamic=module_name] |[all=module_name]
```

## Parameters

### *module\_name*

Specifies the module name such as vlan, ip, igmpsnooping, mldsnooping, mac, trunk.

### dynamic

Specifies the no file. When rebooting, the switch starts with the default configuration.

### all

Specifies no file. When rebooting, the switch starts with the default configuration.

## Description

Use this command to display the configuration settings assign the start-up configuration file.

## Example

The following command resets the switch to the default configuration:

```
Manager> show config=none
```

The following command assigns the config3.cfg file as the start-up configuration file:

```
Manager> show config=config3.cfg
```

## SHOW FILE

---

### Syntax

```
show file[=file_name]
```

### Parameter

*file\_name*

Specifies the file name of a file to display its content. You can also specify a file name using one wild card (\*). The wild card (\*) must be at the beginning or end of the file name.

### Description

Use this command to display a list of the files stored on the switch or the content of the specified file. You can specify only a configuration file (.cfg) or script file (.scp).

Figure 7 shows an output example to display a list of files stored on the switch.

```
Manager > show file
```

Filename	Device	Size	Created	Attribute
config1.cfg	flash	2525	2011-04-21 15:55:40	script
config2.cfg	flash	897	2011-05-18 17:38:09	script
gs900mv2_v232.rel	flash	7159743	2011-04-25 16:08:03	relpkg

Available blocks: 5      (about 1 block = 128kB)

Figure 7. SHOW FILE Command

Figure 8 on page 87 shows an output example to display the content of the specified configuration file.

```
Manager > show file=config1.cfg

File : config1.cfg

1:
2:#
3:# SYSTEM configuration
4:#
5:
6:#
7:# LOAD configuration
8:#
9:
10:#
11:# CONSOLE configuration
12:#
13:
14:#
15:# VLAN configuration
16:#
17:
18:#
19:# IP configuration
20:#
21:add ip interface=default ipaddress=192.168.1.105
mask=255.255.255.0
22:
```

Figure 8. SHOW FILE Command with a File Name

### Examples

The following command displays a list of the files stored on the switch:

```
Manager > show file
```

The following command displays the content of config1.cfg:

```
Manager > show file=config1.cfg
```

## SHOW FTP

---

### Syntax

```
show ftp
```

### Parameters

None

### Description

Use this command to display the information about the FTP server. An example is shown in Figure 9.

```

FTP Module Configuration:
-----
FTP Server                : Enabled
FTP Server Listen Port    : 21
-----

```

Figure 9. SHOW FTP Command

The fields are described in Table 8 .

Table 8. SHOW FTP Command

Field	Description
FTP server	Displays the FTP server is enabled or disabled.
FTP server Listen port	Displays the TCP port for FTP control.

### Example

This example displays the status of the FTP server:

```
Manager > show ftp
```



# SHOW LOADER

---

## Syntax

```
show loader
```

## Parameters

None

## Description

Use this command to display the information about the loader. The settings are used for the LOAD and UPLOAD commands. An example is shown in Figure 10.

```
Loader Information
-----
Defaults:
Method ..... tftp
File ..... -
Destination File ... -
Server ..... 192.168.1.1
-----
```

Figure 10. SHOW LOADER Command

## Example

This example displays the status of the loader:

```
Manager > show loader
```

## SHOW TFTP

---

### Syntax

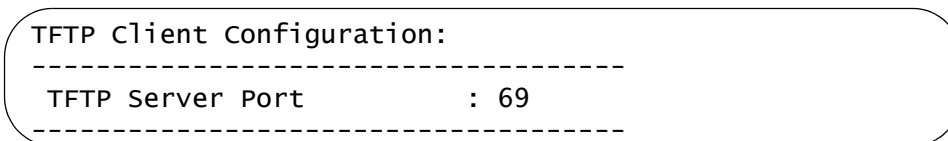
```
show tftp
```

### Parameters

None

### Description

Use this command to display the setting of the TFTP server port. An example is shown in Figure 11.



```
TFTP Client Configuration:
-----
TFTP Server Port          : 69
-----
```

Figure 11. SHOW TFTP Command

### Example

This example displays the TFTP server port:

```
Manager > show tftp
```

# UPLOAD

---

## Syntax

```
upload [method=tftp] [file=file_name] [destfile=file_name]  
[server=ip_address]
```

## Parameters

*file*

Specifies the name of a file to upload.

*destfile*

Specifies a new file name for the uploaded file.

*file\_name*

The file name can be from 1 to 20 alphanumeric characters including a period and extension. The extension can be .cfg or .scp. It is case-sensitive. The file name can include hyphen (-), underscore (\_), period (.), and parentheses ().

*ip\_address*

Specifies the IPv4 address of TFTP server.

## Description

Use this command to upload configuration and script files to the TFTP server.

## Example

The following command uploads the setup.cfg file and saves it as the config1.cfg file to the TFTP server with the IP address of 192.168.1.1:

```
Manager> upload file=setup.cfg destfile=config1.cfg  
server=192.168.1.1
```



## Section II

# Switch Management

---

This section contains the following chapters:

- ❑ Chapter 6, “Log Commands” on page 95
- ❑ Chapter 7, “SNMP Commands” on page 111
- ❑ Chapter 8, “Simple Network Time Control (SNTP) Commands” on page 145
- ❑ Chapter 9, “Telnet Commands” on page 161
- ❑ Chapter 10, “HTTP Commands” on page 173
- ❑ Chapter 11, “RADIUS Authentication Server Commands” on page 179



## Chapter 6

# Log Commands

---

The log commands are summarized in Table 9.

Table 9. Log Commands

Command	Description
“DISABLE LOG” on page 96	Disables logging.
“DISABLE LOG OUTPUT” on page 97	Disables the permanent log, the syslog, or both.
“ENABLE LOG” on page 98	Enables logging.
“ENABLE LOG OUTPUT” on page 99	Enables the permanent log, the syslog, or both.
“FLUSH LOG OUTPUT” on page 100	Deletes the log messages of the specified log.
“PURGE LOG” on page 101	Deletes the log settings and counters.
“SET LOG OUTPUT” on page 102	Configure the permanent log and syslog.
“SHOW CRASHLOG” on page 105	Displays log messages stored in the Non-Volatile (NV) memory.
“SHOW LOG” on page 106	Displays log messages.
“SHOW LOG COUNTER” on page 108	Displays log counters.
“SHOW LOG OUTPUT” on page 109	Displays the log settings.
“SHOW LOG STATUS” on page 110	Displays the log status.

## DISABLE LOG

---

### Syntax

```
disable log
```

### Parameters

None

### Description

Use this command to disable logging. By default, logging is enabled.

### Confirmation Command

“SHOW LOG” on page 106

### Example

The following command disables logging:

```
Manager > disable log
```



## DISABLE LOG OUTPUT

---

### Syntax

```
disable log output[=permanent|syslog]
```

### Parameters

permanent

Specifies the permanent log to disable.

syslog

Specifies the syslog to disable.

### Description

Use this command to disable the permanent log, the syslog, or both.

### Confirmation Command

“SHOW LOG” on page 106

### Example

The following command disables both the permanent log and syslog:

```
manager > disable log output
```

The following command disables the permanent log:

```
manager > disable log output=permanent
```

## ENABLE LOG

---

### Syntax

```
enable log
```

### Parameters

None

### Description

Use this command to enable logging. By default, logging is enabled.

### Confirmation Command

“SHOW LOG” on page 106

### Example

The following command enables logging:

```
Manager > enable log
```

## ENABLE LOG OUTPUT

---

### Syntax

```
enable log output[=permanent|syslog]
```

### Parameters

permanent

Specifies the permanent log to enable.

syslog

Specifies the syslog to enable.

### Description

Use this command to enable the permanent log, the syslog, or both.

### Confirmation Command

“SHOW LOG” on page 106

### Example

The following command enables both the permanent log and syslog:

```
manager > enable log output
```

The following command enables the permanent log:

```
manager > enable log output=permanent
```

## FLUSH LOG OUTPUT

---

### Syntax

```
flush log output[=permanent|syslog]
```

### Parameters

permanent

Specifies the permanent log to delete its log messages.

syslog

Specifies the syslog to delete its log messages.

### Description

Use this command to delete the log messages of the specified log.

### Confirmation Command

“SHOW LOG” on page 106

### Example

The following command deletes the log messages of both permanent log and syslog:

```
manager > flush log output
```

The following command deletes the log messages of the syslog:

```
manager > flush log output=syslog
```

# PURGE LOG

---

## Syntax

```
purge log output[=permanent|syslog]
```

## Parameters

permanent

Specifies the permanent log to delete its setting and counter.

syslog

Specifies the syslog to delete its setting and counter.

## Description

Use this command to delete the log settings and counters.

## Confirmation Command

“SHOW LOG” on page 106

## Example

The following command deletes the settings and log counters:

```
Manager > purge log
```

The following command deletes the setting and counter of the syslog:

```
Manager > purge log=syslog
```

## SET LOG OUTPUT

---

### Syntax

```
set log output[=permanent|syslog] [server=ip_address]  
[listenport=port_number] [severity=[operator]severity]  
[facility=facility|default]
```

### Parameters

#### output

Specifies the permanent or syslog keyword. By default, the permanent keyword is specified.

#### permanent

Specifies the permanent log to set the parameters.

#### syslog

Specifies the syslog to set the parameters.

#### *ip\_address*

Specifies the IPv4 address of the syslog server. This is only available for the syslog.

#### *port\_number*

Specifies the number of UDP port for the syslog server. The port number is from 1 to 65535. By default, the UDP port for the syslog server is 514. This is only available for the syslog.

#### *operator*

Specifies one of the operators shown in Table 11 on page 103.

#### *severity*

Specifies the severity level of log messages to be sent. The severity level are 0 to 7. See Table 10 on page 103.

#### *facility*

Specifies the syslog facility. You can specify using a facility keyword or code as shown in Table 12 on page 103. This is only available for syslog.

#### default

Specifies the syslog facility to be the default value.

### Description

Use this command to configure the permanent log and syslog.

The severity levels are explained in Table 10.

Table 10. Severity Level

Severity Level	Severity
7	Critical
6	Urgent
5	Important
4	Notice
3	Information
2	Detail
1	Trivial
0	Debug

The severity parameter examples are listed in Table 11.

Table 11. Operator Example

Symbol	Example	Description
<	severity=<5	Log messages with severity level 5 and less are sent to the specified output.
>	severity=>5	Log messages with severity level 5 and greater are sent to the specified output.
!	severity=!5	All log messages except severity level 5 are sent to the specified output.
None	severity=5	Log messages with severity level 5 are sent to the specified output.

The syslog facility values are listed in Table 12.

Table 12. Syslog Facility

Facility Code	Facility Keyword	Description
0	kernel	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemon
4	auth	Security/authorization messages

Table 12. Syslog Facility (Continued)

Facility Code	Facility Keyword	Description
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock Daemon
10	authpriv	Security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	audit	Log audit
14	alert	Log alert
15	cron2	Clock daemon
16	local0	Local use 0
17	local1	Local use 1
18	local2	Local use 2
19	local3	Local use 3
20	local4	Local use 4
21	local5	Local use 5
22	local6	Local use 6
23	local7	Local use 7

### Confirmation Command

“SHOW LOG OUTPUT” on page 109

### Example

The following command specifies the IPv4 address of the sysLog server and log messages with severity level 5 and higher to be sent to the sysLog server:

```
Manager > set log output=syslog server=192.168.1.1
severity=>5
```



# SHOW CRASHLOG

---

## Syntax

```
show crashlog
```

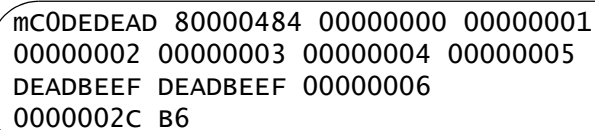
## Parameters

None

## Description

Use this command to display crash logs in the Non-Volatile (NV) memory on the switch.

An example of the command output is shown in Figure 12.

The output of the 'show crashlog' command is displayed within a rounded rectangular box. The output consists of four lines of hexadecimal data: 'mCODEDEAD 80000484 00000000 00000001', '00000002 00000003 00000004 00000005', 'DEADBEEF DEADBEEF 00000006', and '0000002C B6'.

```
mCODEDEAD 80000484 00000000 00000001  
00000002 00000003 00000004 00000005  
DEADBEEF DEADBEEF 00000006  
0000002C B6
```

Figure 12. SHOW CRASHLOG Command

## Example

The following command displays crash logs:

```
Manager> show crashlog
```

## SHOW LOG

---

### Syntax

```
show log [date=[operator] date] [time=[operator] time]  
[severity=[operator] severity] [reverse[=count]]  
[tail[=count]]
```

### Parameters

#### *operator*

Specifies one of the operators: <, >, or !. See Table 11 on page 103.

#### *date*

Specifies the date. The format is yyyy-mm-dd. When the date parameter is not specified, the command displays log messages with any date.

#### *time*

Specifies the system time. The format is hh:mm:ss. When the date parameter is not specified, the command displays log messages with any time.

#### *severity*

Specifies the severity level of log messages to be displayed. The severity levels are 0 to 7 shown in Table 10 on page 103. When the severity parameter is not specified, the command displays log messages with any severity level.

#### *reverse*

Specifies to display log messages in reverse date order. When the count is not specified, all log messages are displayed.

#### *tail*

Specifies to display the specified count of the most recent log messages. When the count is not specified, the most recent 20 log messages are displayed.

#### *count*

Specifies the number of log messages to display.

### Description

Use this command to display a list of log messages. You can specify date, time, severity level, the number of displayed log messages, and display order.

To stop showing log messages, type Ctrl+c.

An example of the command output is shown in Figure 13.

Date	Time	Lv	Message
2011-03-25	14:09:28	7	Switch startup, Ver 2.3.2 B01 Mar 24 2011, 21:24:14
2011-03-25	14:09:28	6	Port 7: interface is up
2011-03-25	14:09:42	3	User login on serial port
2011-03-31	14:06:27	3	User logout on serial port

Figure 13. SHOW LOG Command

### Examples

The following command displays 10 log messages that have severity level 5 and greater in reverse date order:

```
Manager > show log severity=>5 reverse=10
```

The following command displays log messages on 7/7/2014 and after:

```
Manager > show log date=>2014-07-07
```

## SHOW LOG COUNTER

---

### Syntax

```
show log counter
```

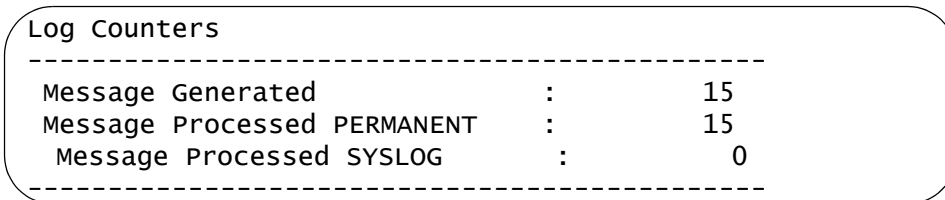
### Parameters

None

### Description

Use this command to display diagnostic log counters:

An example of the command output is shown in Figure 14.



Log Counters		
Message Generated	:	15
Message Processed PERMANENT	:	15
Message Processed SYSLOG	:	0

Figure 14. SHOW LOG COUNTER Command

### Example

The following command displays diagnostic log counters:

```
Manager> show log counter
```

## SHOW LOG OUTPUT

---

### Syntax

```
show log output
```

### Parameters

None

### Description

Use this command to display the log settings:

An example of the command output is shown in Figure 15.

Output	Type	Status	Server	Port	Msg	LogLv	Facility
PERMANENT	NVS	Enabled	-	-	3000	>0	-
SYSLOG	SYSLOG	Disabled	Not set	514	-	>0	DEFAULT

Figure 15. SHOW LOG OUTPUT Command

### Example

The following command displays the log settings:

```
Manager> show log output
```

# SHOW LOG STATUS

---

### Syntax

show log status

### Parameters

None

### Description

Use this command to display the log status:

An example of the command output is shown in Figure 16.

```
Log System Status
-----
Log Module Status ..... Enabled
Log Message Generation ..... Enabled
Permanent Output ..... Enabled
Syslog Output ..... Disabled
Next Message ID ..... 3008
Number of Output Definitions ... 2
-----
```

Figure 16. SHOW LOG STATUS Command

### Example

The following command displays the log status:

Manager> show log status

## Chapter 7

# SNMP Commands

The SNMPv1 and SNMPv2c commands are summarized in Table 13.

Table 13. SNMPv1 and SNMPv2 Commands

Command	Description
“ADD SNMP COMMUNITY” on page 113	Changes the settings of the trap host, manager, trap parameters for an SNMP community.
“CREATE SNMP COMMUNITY” on page 115	Creates a new SNMP community.
“DELETE SNMP COMMUNITY” on page 118	Removes the specified settings of the SNMP community.
“DESTROY SNMP COMMUNITY” on page 119	Deletes the specified SNMP community.
“DISABLE INTERFACE LINKTRAP” on page 120	Disables generating SNMP traps when the link is up or down at the specified port interface.
“DISABLE SNMP” on page 121	Disables SNMP.
“DISABLE SNMP COMMUNITY” on page 122	Disables the specified SNMP community.
“DISABLE SNMP COMMUNITY TRAP” on page 123	Disables sending SNMP traps to the specified community.
“DISABLE SNMP TRAP” on page 124	Disables generating SNMP traps.
“ENABLE INTERFACE LINKTRAP” on page 125	Enables generating SNMP traps when the link is up or down at the specified port interface.
“ENABLE SNMP” on page 126	Enables SNMP.
“ENABLE SNMP COMMUNITY” on page 127	Enables the specified SNMP community.
“ENABLE SNMP COMMUNITY TRAP” on page 128	Enables sending SNMP traps to the specified community.

Table 13. SNMPv1 and SNMPv2 Commands (Continued)

<b>Command</b>	<b>Description</b>
"ENABLE SNMP TRAP" on page 129	Enables generating SNMP traps.
"SET SNMP COMMUNITY" on page 130	Changes the settings of the access and open parameters for an SNMP community.
"SET SNMP LISTENPORT" on page 132	Changes the UDP port for SNMP.
"SET SNMP TRAP LISTENPORT" on page 133	Changes the UDP port for SNMP Trap.
"SHOW INTERFACE" on page 134	Displays the MIB information about the specified port interface.
"SHOW SNMP" on page 137	Displays the SNMP configuration and SNMP counters.
"SHOW SNMP COMMUNITY" on page 140	Displays a list of communities and the settings or the information about the specified community.
"SHOW SNMP TRAP" on page 142	Displays a list of trap statuses or the information about the specified trap.



## ADD SNMP COMMUNITY

---

### Syntax

```
add snmp community=community [traphost=ip_address]  
[manager=ip_address] [trap=trap]
```

### Parameters

*community*

Specifies an existing community name.

traphost

Specifies the IP address of a host where SNMP traps are sent.

manager

Specifies the IP address of an SNMP management server.

*ip\_address*

Specifies an IPv4 address.

*trap*

Specifies a trap type or multiple trap types. To specify multiple trap types, use a comma (.). To send no traps, use the none keyword; to set all trap types, use the all keyword.

- coldstart
- warmstart
- authentication
- link
- fan
- temperature
- voltage
- login
- newroot
- topologychange
- poe
- loopdetection
- stormdetection

- intrusion
- mstp
- epsr
- trigger
- sfp
- newaddress
- all

### **Description**

Use this command to change the settings of the traphost, manager, trap parameters for an SNMP community.

---

#### **Note**

To create a new community, use the CREATE SNMP COMMUNITY command. See “CREATE SNMP COMMUNITY” on page 115. To change the settings of the access and open parameters, see “SET SNMP COMMUNITY” on page 130.

---

### **Confirmation Command**

“SHOW SNMP COMMUNITY” on page 140

### **Example**

The following command adds a traphost to the private community:

```
Manager > add snmp community=private traphost=192.168.1.11
```

## CREATE SNMP COMMUNITY

---

### Syntax

```
create snmp community=community [access=read|write]
[traphost=ip_address] [manager=ip_address]
[open=on|off|yes|no|true|false] [trap=trap]
```

### Parameters

#### *community*

Specifies a community name using up to 20 alphanumeric characters including a hyphen (-), underscore (\_), period (.), parentheses (()), plus (+), and at sign (@). The community name is *not* case-sensitive; however, it is displayed as entered.

#### access

Specifies the access permission to the community using the read or write keyword. By default, the access permission is read.

#### read

Gives the community to only the read permission. A community with the read permission is allowed to use the get and get-next SNMP commands.

#### write

Gives the community to the read and write permission. A community with the write permission is allowed to use the get, get-next, and set SNMP commands.

#### traphost

Specifies the IP address of a host where SNMP traps are sent.

#### manager

Specifies the IP address of an SNMP management server.

#### *ip\_address*

Specifies an IPv4 address.

#### open

Specifies to respond SNMP requests from the hosts specified by the traphost and manager parameters or only the host specified by the manager parameter.

#### on, yes, true

Responds SNMP requests from hosts specified by both traphost and manager parameters.

`off`, `no`, `false`

Responds to SNMP requests from only the host specified by the `manager` parameter.

*trap*

Specifies a trap type or multiple trap types. To specify multiple trap types, use a comma (,). By default, all trap types are specified. To send no traps, use the `none` keyword; to set all trap types, use the `all` keyword.

- `coldstart`
- `warmstart`
- `authentication`
- `link`
- `fan`
- `temperature`
- `voltage`
- `login`
- `newroot`
- `topologychange`
- `poe`
- `loopdetection`
- `storedetection`
- `intrusion`
- `mstp`
- `epsr`
- `trigger`
- `sfp`
- `newaddress`
- `all`
- `none`

## Description

Use this command to create an SNMP community. You can create up to 32 communities. One community can have up to four traphosts.

---

### Note

To add more traphosts, use the ADD SNMP COMMUNITY command. See “ADD SNMP COMMUNITY” on page 113.

---

To start sending SNMP traps, you must execute the ENABLE SNMP TRAP and ENABLE SNMP COMMUNITY TRAP commands.

## Confirmation Command

“SHOW SNMP COMMUNITY” on page 140

## Example

The following command creates the snmp community private with the write access, assigns the IP address of the manager and traphost.:

```
Manager > create snmp community=private access=write  
manager=192.168.1.1 traphost=192.168.1.10
```

## DELETE SNMP COMMUNITY

---

### Syntax

```
delete snmp community=community [traphost=ip_address]  
[manager=ip_address] [trap=trap]
```

### Parameters

*community*

Specifies an existing community name.

traphost

Specifies the IP address of a host where SNMP traps are sent.

manager

Specifies the IP address of an SNMP management server.

*ip\_address*

Specifies an IPv4 address.

*trap*

Specifies a trap type or multiple trap types. To specify multiple trap types, use a comma (.). For a list of trap types, see "CREATE SNMP COMMUNITY" on page 115.

### Description

Use this command to delete a community setting of traphost, manager, and trap types.

### Confirmation Command

"SHOW SNMP COMMUNITY" on page 140

### Example

The following command deletes the traphost 192.168.1.11 from the private community:

```
Manager > delete snmp community=private  
traphost=192.168.1.11
```

## DESTROY SNMP COMMUNITY

---

### Syntax

```
destroy snmp community=community
```

### Parameters

*community*  
Specifies a community name.

### Description

Use this command to delete the specified community from the switch.

### Confirmation Command

“SHOW SNMP COMMUNITY” on page 140

### Example

The following command deletes the community private:

```
Manager > destroy snmp community=private
```

## DISABLE INTERFACE LINKTRAP

---

### Syntax

```
disable interface =if_index|interface|all linktrap
```

### Parameters

*if\_index*

Specifies a switch port number.

*interface*

Specifies a port interface name. The port interface name is a prefix of port followed by a port number, such as port1, port2 and port16.

all

Specifies all port interfaces.

### Description

Use this command to disable generating SNMP traps when the link is up or down at the specified port interface. By default, generating SNMP traps is disabled when the link is up or down at port interfaces.

### Confirmation Command

“SHOW INTERFACE” on page 134

### Example

The following command disables generating traps when the link is up or down at port1:

```
Manager > disable interface=port1 linktrap
```



## DISABLE SNMP

---

### Syntax

```
disable snmp
```

### Parameters

None

### Description

Use this command to disable the SNMP feature. By default, SNMP is disabled.

### Confirmation Command

“SHOW SNMP” on page 137

### Example

The following command disables SNMP:

```
Manager > disable snmp
```

## DISABLE SNMP COMMUNITY

---

### Syntax

```
disable snmp community=community
```

### Parameters

*community*

Specifies a community name.

### Description

Use this command to disable the specified community. By default, the community is disabled.

### Confirmation Command

“SHOW SNMP COMMUNITY” on page 140

### Example

The following command disables the community private:

```
Manager > disable snmp community=private
```

## DISABLE SNMP COMMUNITY TRAP

---

### Syntax

```
disable snmp community=community trap
```

### Parameters

*community*

Specifies a community name.

### Description

Use this command to disable sending traps to the specified community. By default, sending traps to the community is disabled.

### Confirmation Command

“SHOW SNMP COMMUNITY” on page 140

### Example

The following command disables sending traps to the community private:

```
Manager > disable snmp community=private trap
```

## DISABLE SNMP TRAP

---

### Syntax

```
disable snmp trap=trap
```

### Parameters

*trap*

Specifies a trap type or multiple trap types. To specify multiple trap types, use a comma (.). To specify all trap types, use the keyword all. For a list of trap types, see “CREATE SNMP COMMUNITY” on page 115.

### Description

Use this command to disable generating the specified trap type. By default, generating traps is disabled.

### Confirmation Command

“SHOW SNMP TRAP” on page 142

### Example

The following command disables generating the coldstart traps:

```
Manager > disable snmp trap=coldstart
```

## ENABLE INTERFACE LINKTRAP

---

### Syntax

```
enable interface=if_index|interface|all linktrap
```

### Parameters

*if\_index*

Specifies a port number.

*interface*

Specifies a port interface name. The port interface name is a prefix of port followed by a port number, such as port1, port2 and port16.

all

Specifies all port interfaces.

### Description

Use this command to enable generating SNMP traps when the link is up or down at the specified port interface. By default, generating SNMP traps is disabled when the link is up or down at port interfaces.

### Confirmation Command

“SHOW INTERFACE” on page 134

### Example

The following command enables generating traps when the link is up or down at port1:

```
Manager > enable interface=port1 linktrap
```

## ENABLE SNMP

---

### Syntax

```
enable snmp
```

### Parameters

None

### Description

Use this command to enable the SNMP feature. By default, SNMP is disabled.

### Confirmation Command

“SHOW SNMP” on page 137

### Example

The following command enables SNMP:

```
Manager > enable snmp
```

## ENABLE SNMP COMMUNITY

---

### Syntax

```
enable snmp community=community
```

### Parameters

*community*

Specifies a community name.

### Description

Use this command to enable the specified community. By default, the community is disabled.

### Confirmation Command

“SHOW SNMP COMMUNITY” on page 140

### Example

The following command enables the community private:

```
Manager > enable snmp community=private
```

## ENABLE SNMP COMMUNITY TRAP

---

### Syntax

```
enable snmp community=community trap
```

### Parameters

*community*

Specifies a community name.

### Description

Use this command to enable sending traps to the specified community. By default, sending traps to the community is disabled.

### Confirmation Command

“SHOW SNMP COMMUNITY” on page 140

### Example

The following command enables sending traps to the community private:

```
Manager > enable snmp community=private trap
```



## ENABLE SNMP TRAP

---

### Syntax

```
enable snmp trap=trap
```

### Parameters

*trap*

Specifies a trap type or multiple trap types. To specify multiple trap types, use a comma (.). To specify all trap types, use the keyword all. For a list of trap types, see “CREATE SNMP COMMUNITY” on page 115.

### Description

Use this command to enable generating the specified trap type. By default, generating traps is disabled.

### Confirmation Command

“SHOW SNMP TRAP” on page 142

### Example

The following command enables generating the coldstart traps:

```
Manager > enable snmp trap=coldstart
```

## SET SNMP COMMUNITY

---

### Syntax

```
set snmp community=community [access=read|write]  
[open=on|off|yes|no|true|false]
```

### Parameters

#### *community*

Specifies a community name using up to 20 alphanumeric characters including a hyphen (-), underscore (\_), period (.), parentheses (()), plus (+), and at sign (@). The community name is *not* case-sensitive; however, it is displayed as entered.

#### access

Specifies the access permission to the community using the read or write keyword. By default, the access permission is read.

#### read

Gives the community to only the read permission. A community with the read permission is allowed to use the get and get-next SNMP commands.

#### write

Gives the community to the read and write permission. A community with the write permission is allowed to use the get, get-next, and set SNMP commands.

#### open

Specifies to respond SNMP requests from the hosts specified by the traphost and manager parameters or only the host specified by the manager parameter.

#### on, yes, true

Responds SNMP requests from hosts specified by both traphost and manager parameters.

#### off, no, false

Responds SNMP requests from only the host specified by the manager parameter.

### Description

Use this command to change the settings of access and open parameters for an SNMP community.

---

**Note**

To create a new community, use the CREATE SNMP COMMUNITY command. See “CREATE SNMP COMMUNITY” on page 115. To change the settings of the trap host, manager, and trap parameters, see “ADD SNMP COMMUNITY” on page 113.

---

**Confirmation Command**

“SHOW SNMP COMMUNITY” on page 140

**Example**

The following command changes the community private with the read access:

```
Manager > set snmp community=private access=read
```

## SET SNMP LISTENPORT

---

### Syntax

```
set snmp listenport=port_number
```

### Parameters

*port\_number*

Specifies the number of UDP port for SNMP. The port number is from 1 to 65535. By default, the UDP port for SNMP is 161.

### Description

Use this command to change the UDP port for SNMP.

### Confirmation Command

“SHOW SNMP” on page 137

### Example

The following command changes the UDP port for SNMP to 200:

```
Manager > set snmp listenport=200
```

## SET SNMP TRAP LISTENPORT

---

### Syntax

```
set snmp trap listenport=port_number
```

### Parameters

*port\_number*

Specifies the number of UDP port for SNMP Trap. The port number is from 1 to 65535. By default, the UDP port for SNMP Trap is 162.

### Description

Use this command to change the UDP port for SNMP Trap.

### Confirmation Command

“SHOW SNMP” on page 137

### Example

The following command changes the UDP port for SNMP Trap to 201:

```
Manager > set snmp trap listenport=201
```

## SHOW INTERFACE

---

### Syntax

```
show interface=if_index|interface|all [counter]
```

### Parameters

*if\_index*

Specifies a port number.

*interface*

Specifies a port interface name. The port interface name is the prefix port followed by a port number, such as port1, port2 and port16.

all

Specifies all port interfaces.

counter

Specifies to display the counter information.

### Description

Use this command to display the MIB information about the specified port interface. An example of the command output is shown in Figure 17.

```
Manager > show interface
Interfaces Information                               sysUpTime:           03:56:16
ifIndex Interface ifAdminStatus ifOperStatus ifLinkUpDownTrap ifLastChange
-----
1      port1      Up      Down      Enabled    00:00:00
2      port2      Up      Down      Disabled   00:00:00
3      port3      Up      Down      Disabled   00:00:00
4      port4      Up      Down      Disabled   00:00:00
5      port5      Up      Down      Disabled   00:00:00
6      port6      Up      Down      Disabled   00:00:00
7      port7      Up      Down      Disabled   00:00:00
8      port8      Up      Down      Disabled   00:00:00
9      port9      Up      Down      Disabled   00:00:00
10     port10     Up      Down      Disabled   00:00:00
11     port11     Up      Down      Disabled   00:00:00
12     port12     Up      Down      Disabled   00:00:00
13     port13     Up      Down      Disabled   00:00:00
14     port14     Up      Down      Disabled   00:00:00
15     port15     Up      Down      Disabled   00:00:00
16     port16     Up      Down      Disabled   00:00:00
-----
```

Figure 17. SHOW INTERFACE Command

Another example of the command output is shown in Figure 18.

```

Manager > show interface=1

interface ..... port1
ifIndex ..... 1
ifMTU ..... 9196
ifSpeed ..... 1000000000
ifAdminStatus ..... Up
ifOperStatus ..... Down
ifLinkUpDownTrapEnable .. Enabled

Interface Counters

ifInOctets      :                0      ifOutOctets      :                0
ifInUcastPkts  :                0      ifOutUcastPkts  :                0
ifInNUcastPkts:                0      ifOutNUcastPkts:                0
ifInDiscards   :                0      ifOutDiscards   :                0
ifInErrors     :                0      ifOutErrors     :                0

```

Figure 18. SHOW INTERFACE with Parameters Command

The fields are described in Table 14.

Table 14. SHOW INTERFACE Command

Field	Description
ifIndex	Displays the interface index.
Interface	Displays the interface name specified by the SET SWITCH PORT command.
ifAdminStatus	Displays the status specified by the administrator. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> Up</li> <li><input type="checkbox"/> Down</li> <li><input type="checkbox"/> Testing</li> </ul>
ifOperStatus	Displays the status of the interface. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> Up</li> <li><input type="checkbox"/> Down</li> <li><input type="checkbox"/> Testing</li> </ul>
ifLinkUpDownTrap	Displays Enabled or Disabled for generating traps when the link is up or down at the interface.
ifLastChange	Displays the sysUpTime since the interface became the current status.

Table 14. SHOW INTERFACE Command (Continued)

Field	Description
ifMTU	Displays the size of Maximum Transmission Unit (MTU).
ifSpeed	Displays the estimated bandwidth of the interface.
ifInOctets	Displays the number of received octets.
ifInUcastPkts	Displays the number of unicast packets that were transmitted to the upper network layer.
ifUnNUcasstPkts	Displays the number of broadcast and multicast packets that were transmitted to the upper network layer.
ifInDiscards	Displays the number of received packets that were discarded due to buffer overflow or other reasons.
ifInErrors	Displays the number of received packets that were discarded because the packets included an error.
ifOutOctets	Displays the number of transmitted octets.
ifOutUcastPkts	Displays the number of unicast packets including discarded packets that were requested to transmit by the upper network layer.
ifOutNUcastPkts	Displays the number of broadcast and multicast packets including discarded packets that were requested to transmit by the upper network layer.
ifOutDiscards	Displays the number of transmitted packets that were discarded due to buffer overflow or other reasons.
ifOutErrors	Displays the number of transmitted packets that were discarded because the packets included an error.

### Example

The following example displays the MIB information about port 1 and statics:

```
Manager > show interface=1 counter
```



## SHOW SNMP

---

### Syntax

```
show snmp
```

### Parameters

None

### Description

Use this command to display the SNMP configuration and SNMP counters. An example of the command output is shown in Figure 19.

```
SNMP Module Configuration:
-----
Status                : Disabled
SNMP Manager Listen Port : 161
SNMPTRAP Listen Port   : 162
-----

SNMP counters:
-----
inPkts                :          0      outPkts                :          0
inBadVersions         :          0      outTooBigs            :          0
inBadCommunityNames  :          0      outNoSuchNames       :          0
inBadCommunityUses   :          0      outBadValues         :          0
inASNParseErrs      :          0      outGenErrs           :          0
inTooBigs            :          0      outGetRequests       :          0
inNoSuchNames        :          0      outGetNexts          :          0
inBadValues          :          0      outSetRequests       :          0
inReadOnly           :          0      outGetResponses      :          0
inGenErrs            :          0      outTraps             :          0
inTotalReqVars       :          0
inTotalSetVars       :          0
inGetRequests        :          0
inGetNexts           :          0
inSetRequests        :          0
inGetResponses       :          0
inTraps              :          0
```

Figure 19. SHOW SNMP Command

The fields are described in Table 15.

Table 15. SHOW SNMP Command

<b>Field</b>	<b>Description</b>
Status	Displays SNMP is Enabled or Disabled.
SNMP Manager Listen Port	Displays the UDP port for SNMP.
SNMP TRAP Listen Port	Displays the UDP port for SNMP Trap.
inPkts	Displays the number of received SNMP packets.
inBadVersions	Displays the number of received SNMP packets with the version which is not supported.
inBadCommunityNames	Displays the number of received SNMP packets including a community name that was not recognized.
inBadCommunityUses	Displays the number of received SNMP packets that a community has no permission to.
inASNParseErrs	Displays the number of received SNMP packets that were not able to be decoded due to the ASN.1 syntax error.
inTooBigs	N/A
inNoSuchNames	N/A
inBadValue	N/A
inReadOnlys	N/A
inGenErrs	N/A
inTotalReqVars	Displays the number of MIB objects that the SNMP agent referred to in order to respond to GetRequest and GetNextRequest messages.
inTotalSetVars	Displays the number of MIB objects that were changed by SetRequest messages.
inGetRequests	Display the number of received GetRequest messages.
inGetNexts	Displays the number of received GetNextRequest messages.
inSetRequests	Displays the number of received SetRequest messages.
inGetResponses	N/A

Table 15. SHOW SNMP Command (Continued)

Field	Description
inTraps	N/A
outPkts	Displays the number of transmitted SNMP packets.
outTooBigs	N/A
outNoSuchName	Displays the number of transmitted SNMP messages that include “noSuchName” in the error field.
outBadValues	Displays the number of transmitted SNMP messages that include “badValue” in the error field.
outGenErrs	Displays the number of transmitted SNMP messages that include “genErr” in the error field.
outGetRequests	N/A
outGetNexts	N/A
outSetRequests	N/A
outGetResponses	Displays the number of transmitted GetResponse messages.
outTraps	Displays the number of transmitted SNMP traps.

### Example

The following example displays the SNMP configuration and SNMP counters:

```
Manager > show snmp
```

## SHOW SNMP COMMUNITY

---

### Syntax

```
show snmp community[=community | all]
```

### Parameters

*community*

Specifies a community name.

all

Specifies all communities.

### Description

Use this command to display a list of communities and the settings or the information about the specified community. An example of the command output is shown in Figure 20.

```

Manager > show snmp community
SNMP community information:
-----
Name           Status      Traps      Access      OpenAccess
-----
public         Enabled    Disabled   read-only   Yes
private        Enabled    Enabled    read-write  No
test           Disabled   Enabled    read-only   Yes
  
```

Figure 20. SHOW SNMP COMMUNITY Command

Another example of the command output is shown in Figure 21.

```

Manager > show snmp community=public
SNMP community information:
-----
Name ..... public
Access ..... read-only
Status ..... Disabled
Trap Status ..... Disabled
Open Access ..... Yes
Traps ..... COLDSTART, WARMSTART, AUTHENTICATION, LINK
              FAN, TEMPERATURE, VOLTAGE, NEWROOT, TOPOLOGYCHANGE
              LOOPDETECTION, STORMDETECTION, EPSR, MSTP
              TRIGGER, INTRUSION, SFP, NEWADDRESS, POE, LOGIN
Manager ..... 192.168.1.1
TrapHost ..... 192.168.1.1
TrapHost ..... 192.168.1.2
  
```

Figure 21. SHOW SNMP COMMUNITY Command with Parameter

The fields are described in Table 16.

Table 16. SHOW SNMP COMMUNITY Command

Field	Description
Name	Displays the name of a community
Access	Displays the access permission to the community. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> read-only</li> <li><input type="checkbox"/> read-write</li> </ul>
Status	Displays whether the community is enabled or disabled.
Trap Status	Displays the trap is enabled or disabled.
Open Access	Displays the open access setting of the community. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes - SNMP agent responds SNMP requests from all the hosts and manager.</li> <li><input type="checkbox"/> No - SNMP agent responds SNMP requests only from the manager..</li> </ul>
Traps	Displays a list of trap types that are generated.
Manager	Displays the IP address of the SNMP manager of the community.
Trap Host	Displays the IP address of hosts that the community send SNMP traps to.

### Example

The following example displays a list of communities and their settings:

```
Manager > show snmp community
```

The following example displays the information about the community private:

```
Manager > show snmp community=private
```

## SHOW SNMP TRAP

---

### Syntax

```
show snmp trap[=trap | all]
```

### Parameters

*trap*

Specifies a trap type. For a list of trap types, see “CREATE SNMP COMMUNITY” on page 115.

all

Specifies all trap types.

### Description

Use this command to display a list of trap statuses or the information about the specified trap. An example of the command output is shown in Figure 22.

```

Manager > show snmp trap
SNMP Trap Information:
-----
Cold Start ..... Enabled
Warm Start ..... Enabled
Authentication ..... Enabled
Fan ..... Enabled
Link ..... Enabled
Temperature ..... Enabled
Voltage ..... Enabled
Newroot ..... Enabled
TopologyChange..... Enabled
PoE..... Enabled
Login ..... Enabled
LoopDetection..... Enabled
StormDetection..... Enabled
Epsr..... Enabled
Mstp..... Enabled
Trigger..... Enabled
Intrusion..... Enabled
Sfp ..... Enabled
Newaddress ..... Enabled
-----

```

Figure 22. SHOW SNMP TRAP Command

Another example of the command output is shown in Figure 23.

```

Manager > show snmp trap=coldstart

SNMP Trap Information
-----
Cold Start TRAP ..... Enabled
Community ..... public
Status ..... Enabled
Trap Status ..... Enabled
Trap Host ..... 192.168.1.1
Trap Host ..... 192.168.1.5
Community ..... private
Status ..... Enabled
Trap Status ..... Enabled
Trap Host ..... 192.168.2.1
-----

```

Figure 23. SHOW SNMP TRAP Command with Parameter

### Example

The following example displays a list of trap statuses:

```
Manager > show snmp trap
```

The following example displays the information about the trap type coldstart:

```
Manager > show snmp trap=coldstart
```





## Chapter 8

# Simple Network Time Control (SNTP) Commands

---

The SNTP commands are summarized in Table 17.

Table 17. SNTP Commands

Command	Description
“ADD NTP PEER” on page 146	Changes the IP address of the SNTP server.
“DELETE NTP PEER” on page 147	Deletes the SNTP server from the switch.
“DISABLE NTP” on page 148	Disables SNTP.
“DISABLE SUMMER-TIME” on page 149	Disables Daylight Saving Time.
“ENABLE NTP” on page 150	Enables SNTP.
“ENABLE SUMMER-TIME” on page 151	Enables Daylight Saving Time.
“PURGE NTP” on page 152	Deletes the settings of SNTP.
“RESET NTP” on page 153	Resets SNTP.
“SET NTP” on page 154	Specifies the IP address of the SNTP server, UTC offset, the UDP port for SNTP.
“SET SUMMER-TIME” on page 157	Specifies the Daylight Saving Time settings.
“SHOW NTP” on page 158	Displays the SNTP settings and SNTP counters.
“SHOW SUMMER-TIME” on page 160	Displays the Daytime Saving Time settings on the switch.

## ADD NTP PEER

---

### Syntax

```
add ntp peer=ip_address
```

### Parameters

*ip\_address*

Specifies an IPv4 address.

### Description

Use this command to configure the IP address of the SNTP server to synchronize the system time of the switch with the specified SNTP server. You can specify only one IP address of the SNTP server on the switch.

---

#### Note

To synchronize the system time with the SNTP server, you must enable SNTP. See “ENABLE NTP” on page 150.

---

### Confirmation Command

“SHOW NTP” on page 158

### Example

The following command specifies the IP address of the SNTP server:

```
Manager > add ntp peer=192.168.1.230
```

## DELETE NTP PEER

---

### Syntax

```
delete ntp peer
```

### Parameters

None

### Description

Use this command to delete the IP address of the SNTP server from the switch.

### Confirmation Command

“SHOW NTP” on page 158

### Example

The following command deletes the IP address of the SNTP server from the switch:

```
Manager > delete ntp peer
```

## **DISABLE NTP**

---

### **Syntax**

```
disable ntp
```

### **Parameters**

None

### **Description**

Use this command to disable SNTP. By default, SNTP is disabled.

### **Confirmation Command**

“SHOW NTP” on page 158

### **Example**

The following command disables SNTP:

```
Manager > disable ntp
```

## DISABLE SUMMER-TIME

---

### Syntax

```
disable summer-time
```

### Parameters

None

### Description

Use this command to disable Daylight Saving Time on the switch. By default, Daylight Saving Time is disabled.

### Confirmation Command

“SHOW SUMMER-TIME” on page 160

### Example

The following command disables Daylight Saving Time on the switch:

```
Manager > disable summer-time
```

## ENABLE NTP

---

### Syntax

```
enable ntp
```

### Parameters

None

### Description

Use this command to enable SNTP. By default, SNTP is disabled.

### Confirmation Command

“SHOW NTP” on page 158

### Example

The following command enables SNTP:

```
Manager > disable ntp
```

## ENABLE SUMMER-TIME

---

### Syntax

```
enable summer-time
```

### Parameters

None

### Description

Use this command to enable Daylight Saving Time on the switch. When Daylight Saving Time is enabled, the switch adjusts the local time according to the Daylight Saving Time settings on the switch. By default, Daylight Saving Time is disabled.

### Confirmation Command

“SHOW SUMMER-TIME” on page 160

### Example

The following command enables Daylight Saving Time on the switch:

```
Manager > enable summer-time
```

## PURGE NTP

---

### Syntax

```
purge ntp
```

### Parameters

None

### Description

Use this command to delete the settings of SNTP. This command does *not* disable SNTP.

### Confirmation Command

“SHOW NTP” on page 158

### Example

The following command deletes the settings of SNTP:

```
Manager > purge ntp
```



## RESET NTP

---

### Syntax

```
reset ntp
```

### Parameters

None

### Description

Use this command to delete the dynamic setting, reload the static setting, and transmit the SNTP request.

### Confirmation Command

“SHOW NTP” on page 158

### Example

The following command resets SNTP:

```
Manager > reset ntp
```

## SET NTP

---

### Syntax

```
set ntp [peer=ip_address] [utcoffset=time_zone | utc_offset]
[listenport=port_number]
```

### Parameters

*ip\_address*

Specifies an IPv4 address.

*time\_zone*

*time\_zone*

Specifies the time zone. See Table 18 on page 154.

*utc\_offset*

Specifies the UTC offset. The format is hh:mm:ss. See Table 18 on page 154.

*port\_number*

Specifies the number of UDP port for SNTP. The port number is from 1 to 65535. By default, the UDP port for SNTP is 123.

### Description

Use this command to specify the IP address of the SNTP server, UTC offset, the UDP port for SNTP. SNTP synchronizes the system time of the switch with the specified SNTP server. You can specify only one IP address of the SNTP server on the switch.

---

#### Note

To synchronize the system time with the SNTP server, you must enable SNTP. See “ENABLE NTP” on page 150.

---

The time zones and UTC offset are listed in Table 18.

Table 18. UTC Time Zone and UTC Offset

Time Zone Keyword	UTC Offset	Area
asia	+8:00:00	Asia
acdt	+10:30:00	Australian Central Daylight Time
acst	+9:30:00	Australian Central Standard Time
aedt	+11:00:00	Australian Eastern Daylight Time

Table 18. UTC Time Zone and UTC Offset (Continued)

<b>Time Zone Keyword</b>	<b>UTC Offset</b>	<b>Area</b>
aest	+10:00:00	Australian Eastern Standard Time
awst	+8:00:00	Australian Western Standard Time
bst	+1:00:00	British Standard Time
chaina	+8:00:00	China
gmt	+0:00:00	Greenwich Mean Time
uk	+0:00:00	Greenwich Mean Time
hk	+8:00:00	Hong Kong
jst	+9:00:00	Japan Standard Time
met	+1:00:00	Mid-European Time
nzdt	+13:00:00	New Zealand Daylight Time
nzst	+12:00:00	New Zealand Standard Time
sing	+8:00:00	Singapore
taiwan	+8:00:00	Taiwan
utc	+0:00:00	Universal coordinated Time
cdt	-5:00:00	US Central Daylight Time
cst	-6:00:00	US Central Standard Time
edt	-4:00:00	US Eastern Daylight Time
est	-5:00:00	US Eastern Standard Time
mdt	-6:00:00	US Mountain Daylight Time
mst	-7:00:00	US Mountain Standard Time
pdtd	-7:00:00	US Pacific Daylight Time
pst	-8:00:00	US Pacific Standard Time
default		
none		

**Confirmation Command**

“SHOW NTP” on page 158

### **Examples**

The following command specifies the IP address of the SNTP server:

```
Manager > set ntp peer=192.168.1.230
```

The following command specifies the timezone with PDT:

```
Manager > set ntp utcoffset=pst
```

The following command specifies the offset +9:00:

```
Manager > set ntp utcoffset=+9:00:00
```

## SET SUMMER-TIME

---

### Syntax

```
set summer-time start-date=date start-time=time  
end-date=date end-time=time offset=offset
```

### Parameters

*start-date*

Specifies the date when Daylight Saving Time starts.

*end-date*

Specifies the date when Daylight Saving Time starts.

*start-time*

Specifies the time when Daylight Saving Time starts.

*date*

Specifies a date in the format *yyyy-mm-dd*.

*time*

Specifies time in the format *hh:mm*.

*offset*

Specifies minutes difference between the standard time and the Daylight Saving Time. The value is 1 to 180 minutes.

### Description

Use this command to specify the Daylight Saving Time settings.

### Confirmation Command

“SHOW SUMMER-TIME” on page 160

### Examples

The following command specifies the the Daylight Saving Time settings:

```
Manager > set summer-time start-date=2015-03-08 start-time  
02:00 end-date=2015-11-01 end-time=02:00 offset=60
```

## SHOW NTP

---

### Syntax

```
show ntp
```

### Parameters

None

### Description

Use this command to display the SNTP settings and SNTP counters. An example of the command output is shown in Figure 24.

```

Manager > show ntp
-----
NTP Module Configuration
-----
Status                : Enabled
Host Address          : 192.168.1.5
UTC Offset            : +09:00:00(JST)
Last Updated         : 2011-04-12 at 11:23:16
Last Delta           : 0

Configured Peer      : 192.168.1.1
NTP Server Listen Port : 123

Counters
-----
Packets Sent         : 0000000001
Packets Received    : 0000000001
Packets w/head error : 0000000000
Packets w/data error : 0000000000

```

Figure 24. SHOW NTP Command

The fields are described in Table 19.

Table 19. SHOW NTP Command

Field	Description
Status	Displays SNTP is Enabled or Disabled.
Host Address	Displays the IP address of the SNTP server.
UTC Offset	Displays the offset from UTC.
Last Updated	Displays the last time when the system time was updated by the SNTP server.

Table 19. SHOW NTP Command (Continued)

Field	Description
Last Delta	Displays the offset that the system time was adjusted the last time.
Configured Peer	Displays the IP address of the SNTP peer.
NTP Server Listen Port	Displays the IP address of the UDP port for SNTP server.
Packets Sent	Displays the number of transmitted SNTP packets.
Packets Received	Displays the number of received SNTP packets.
Packets w/ head error	Displays the number of received SNTP packets that include a head error.
Packets w/ data error	Displays the number of received SNTP packets that include a data error.

**Example**

The following example displays the SNTP configuration and SNTP counters:

```
Manager > show ntp
```

## SHOW SUMMER-TIME

---

### Syntax

```
show summer-time
```

### Parameters

None

### Description

Use this command to display the Daylight Saving Time settings on the switch. An example of the command output is shown in Figure 25.

```
Local Time: Mon, 6 Aug 2014 13:56:06 +1200
UTC Time: Mon, 6 Aug 2014 01:56:06 +0000
Timezone: NZST
Timezone Offset: +12:00
Summer time zone: NZDT
Summer time starts: Last Sunday in September at 02:00:00
Summer time ends: First Sunday in April at 02:00:00
Summer time offset: 60 mins
Summer time recurring: Yes
```

Figure 25. SHOW SUMMER-TIME Command

### Example

The following example displays the Daylight Saving Time settings on the switch:

```
Manager > show summer-time
```



## Chapter 9

# Telnet Commands

---

The Telnet commands are summarized in Table 20.

Table 20. Telnet Commands

Command	Description
“DISABLE TELNET SERVER” on page 162	Disables the Telnet server on the switch.
“ENABLE TELNET SERVER” on page 163	Enables the Telnet server on the switch.
“SET ASYN” on page 164	Enables or disables logging in from the Console port.
“SET CONSOLE” on page 165	Specifies the settings of sessions from the Console port.
“SET TELNET” on page 167	Specifies the settings of sessions through Telnet.
“SHOW ASYN” on page 168	Displays whether logging in from the Console port is enabled or disabled.
“SHOW CONSOLE” on page 169	Displays the settings of the Console port, Telnet, and sessions from the Console port and Telnet.
“SHOW TELNET” on page 171	Displays the settings of Telnet.
“TELNET” on page 172	Starts a Telnet session from the local management session from the Console port.

## DISABLE TELNET SERVER

---

### Syntax

```
disable telnet server
```

### Parameters

None

### Description

Use this command to disable the Telnet server on the switch. By default, the Telnet server is enabled.

### Confirmation Command

“SHOW TELNET” on page 171

### Example

The following command disables the Telnet server:

```
Manager > disable telnet server
```

## ENABLE TELNET SERVER

---

### Syntax

```
enable telnet server
```

### Parameters

None

### Description

Use this command to enable the Telnet server on the switch. By default, the Telnet server is enabled.

### Confirmation Command

“SHOW TELNET” on page 171

### Example

The following command enables the Telnet server:

```
Manager > enable telnet server
```

## SET ASYN

---

### Syntax

```
set asyn login=on|off|yes|no|true|false
```

### Parameters

login

Enables or disables logging in from the Console port.

on, yes, true

Enables logging in from the Console port.

off, no, false

Disables logging in from the Console port.

### Description

Use this command to enable or disable logging in from the Console port. The command execution becomes effective once you logged out.

### Confirmation Command

“SHOW ASYN” on page 168

“SHOW TELNET” on page 171

### Example

The following command disables logging in from the Console port:

```
Manager > set asyn login=no
```

# SET CONSOLE

---

## Syntax

```
set console [page=lines|off|0] [timeout=timeout]  
[completion=both|tab|space|off]
```

## Parameters

### page

Specifies the number of lines to display at a time. When the off keyword or 0 is specified, the screen shows all lines once.

### *lines*

Specifies the number of lines to display. The range is 4 to 99 lines.

### *timeout*

Specifies time in seconds before the session ends when no commands are entered. The range is 0 to 3267 seconds. When 0 is specified, the session does not time out.

### completion

Specifies the way to expand a partially entered command at the prompt.

### both

Specifies the tab key and space bar to expand a partially entered command at the prompt. This is the default setting.

### tab

Specifies the tab key to expand a partially entered command at the prompt.

### space

Specifies the space bar to expand a partially entered command at the prompt.

### off

Specifies that commands are not expanded at the prompt.

## Description

Use this command to specify the number of lines to display, timeout, and command expansion setting for sessions through Telnet or from the Console port.

## Confirmation Command

“SHOW CONSOLE” on page 169

### **Example**

The following command specifies that sessions through Telnet and from the Console ports do not time out:

```
Manager > set console timeout=0
```

# SET TELNET

---

## Syntax

```
set telnet [limit=sessions] [listenport=port_number]
```

## Parameters

### *sessions*

Specifies the maximum number of Telnet sessions to access the switch at a time.

### *port\_number*

Specifies the TCP port for Telnet. The port number is from 1 to 65535. By default, the TCP port for Telnet is 23.

## Description

Use this command to specify the number of sessions to allow to access the switch at a time or change the UDP port for Telnet.

## Confirmation Command

“SHOW TELNET” on page 171

## Example

The following command changes the UDP port for Telnet to 120:

```
Manager > set telnet listenport=120
```

## SHOW ASYN

---

### Syntax

show asyn

### Parameters

None

### Description

Use this command to display the settings of the Console port.

An example of the command output is shown in Figure 26.

```
Serial Information
-----
Serial port
  Status ..... Enabled
  Data rate ..... 9600bps
-----
```

Figure 26. SHOW ASYN Command

### Example

The following command displays the settings of the Console port:

```
Manager> show asyn
```



## SHOW CONSOLE

---

### Syntax

```
show console
```

### Parameters

None

### Description

Use this command to display the settings of the Console port, Telnet, and the sessions through Telnet and the Console port.

An example of the command output is shown in Figure 27.

```

Console Information
-----
Console Password ..... Default
Page size ..... 22
Timeout ..... 300sec
Completion ..... Tab and Space

Serial port
Status ..... Enabled
Data rate ..... 9600bps

Telnet
Status ..... Enabled
TCP port ..... 23/tcp
Connection limit .... 4
-----

```

Figure 27. SHOW CONSOLE Command

The fields are described in Table 21.

Table 21. SHOW CONSOLE Command

Field	Description
Console Password	Displays the state of the login password. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> Default</li> <li><input type="checkbox"/> Configured - The password has been changed.</li> </ul>

Table 21. SHOW CONSOLE Command (Continued)

Field	Description
Page size	Displays the number of lines displayed at a time in the screen.
Timeout	Displays the time in seconds that the session ends after no commands are entered.
Completion	Displays the way that commands are expanded at the prompt. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> Tab and Space</li> <li><input type="checkbox"/> Tab only</li> <li><input type="checkbox"/> Space only</li> <li><input type="checkbox"/> Off</li> </ul>
Serial Port	Displays the information about the Console port.
Status	Displays whether logging in from the Console port is Enabled or Disabled.
Data rate	Displays the data rate from the Console port. It always shows 9600bps.
Telnet	Displays the information about Telnet.
Status	Displays whether logging in from Telnet is Enabled or Disabled.
TCP port	Displays the TCP port for the Telnet server.
Connection Limit	Displays the maximum number of Telnet sessions allowed.

**Example**

The following command displays the settings of the Console port, Telnet, and sessions from the console port and Telnet:

```
Manager> show console
```

# SHOW TELNET

---

## Syntax

```
show telnet
```

## Parameters

None

## Description

Use this command to display the settings of Telnet.

An example of the command output is shown in Figure 28.

```
TELNET Module Configuration:
-----
TELNET Server           : Enabled
TELNET Server Listen Port : 23
TELNET Connection Limit  : 4
-----
```

Figure 28. SHOW TELNET Command

The fields are described in Table 22.

Table 22. SHOW TELNET Command

Field	Description
Status	Displays whether logging in form Telnet is Enabled or Disabled.
TCP port	Displays the TCP port for the Telnet server.
Connection Limit	Displays the maximum number of Telnet sessions allowed.

## Example

The following command displays the settings of Telnet:

```
Manager> show telnet
```

## TELNET

---

### Syntax

```
telnet ip_address[:port_number]
```

### Parameters

*ip\_address*

Specifies the IPv4 address of the Telnet server.

*port\_number*

Specifies the TCP port for Telnet.

### Description

Use this command to start a Telnet session from the local management session through the Console port.

---

#### Note

You cannot start a Telnet session from the remote control session through Telnet.

---

### Example

The following command start a Telnet session from the session via the Cosole port:

```
Manager > telnet 192.168.1.240
```

## Chapter 10

# HTTP Commands

---

The HTTP commands are summarized in Table 23.

Table 23. HTTP Commands

Command	Description
“DISABLE HTTP SERVER” on page 174	Disables the HTTP server on the switch.
“ENABLE HTTP SERVER” on page 175	Enables the HTTP server on th switch.
“SET HTTP LISTENPORT” on page 176	Changes the TCP port for the HTTP server.
“SHOW HTTP SERVER” on page 177	Displays the settings of the HTTP server.

## DISABLE HTTP SERVER

---

### Syntax

```
disable http server
```

### Parameters

None

### Description

Use this command to disable the http server on the switch. By default, the HTTP server is disabled.

### Confirmation Command

“SHOW HTTP SERVER” on page 177

### Example

The following command disables the HTTP server:

```
Manager > disable http server
```

## ENABLE HTTP SERVER

---

### Syntax

```
enable http server
```

### Parameters

None

### Description

Use this command to enable the http server on the switch. By default, the Telnet server is disabled.

### Confirmation Command

“SHOW HTTP SERVER” on page 177

### Example

The following command enables the http server:

```
Manager > enable http server
```

## SET HTTP LISTENPORT

---

### Syntax

```
set http listenport=port_number
```

### Parameters

*port\_number*

Specifies the TCP port for HTTP. The port number is from 1 to 65535. By default, the TCP port for HTTP is 80.

### Description

Use this command to change the TCP port for HTTP.

### Confirmation Command

“SHOW HTTP SERVER” on page 177

### Example

The following command changes the TCP port for HTTP to 120:

```
Manager > set http listenport=120
```



## SHOW HTTP SERVER

---

### Syntax

```
show http server
```

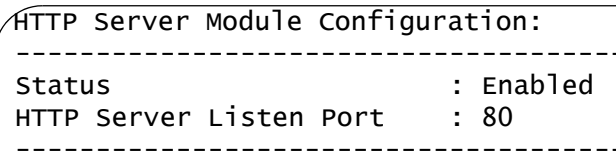
### Parameters

None

### Description

Use this command to display the settings of the HTTP server.

An example of the command output is shown in Figure 29.



```
HTTP Server Module Configuration:
-----
Status                : Enabled
HTTP Server Listen Port : 80
-----
```

Figure 29. SHOW HTTP SERVER Command

### Example

The following command displays the settings of the HTTP server:

```
Manager> show http server
```



## Chapter 11

# RADIUS Authentication Server Commands

---

The RADIUS server commands are summarized in Table 24.

Table 24. RADIUS Server Commands

Command	Description
“ADD RADIUSSERVER SERVER” on page 180	Adds a RADIUS server to the list.
“DELETE RADIUSSERVER SERVER” on page 181	Deletes the RADIUS server from the list.
“DISABLE RADIUSACCOUNTING” on page 182	Disables the accounting feature on RADIUS servers.
“ENABLE RADIUSACCOUNTING” on page 183	Enables the accounting feature on RADIUS servers.
“SET AUTHENTICATION” on page 184	Specifies the settings of RADIUS servers for authentication.
“SET RADIUS” on page 185	Specifies the settings of RADIUS servers for authentication.
“SET RADIUSACCOUNTING” on page 186	Specifies the settings of RADIUS servers for accounting.
“SHOW AUTHENTICATION” on page 188	Displays a list of RADIUS servers and their settings.
“SHOW RADIUS” on page 190	Displays a list of RADIUS servers and their settings.
“SHOW RADIUSACCOUNTING” on page 191	Displays the settings of RADIUS servers for accounting.

## ADD RADIUSSERVER SERVER

---

### Syntax

```
add radiusserver server=ip_address order=1|2 [secret=secret]  
[port=port_number] [accport=port_number]
```

### Parameters

*ip\_address*

Specifies the IPv4 address of the RADIUS server.

order

Specifies the priority for the RADIUS server, 1 or 2. The priority 1 is higher than the priority 2.

*secret*

Specifies the password to communicate with the RADIUS server.

port

Specifies the UDP port for the RADIUS server for authentication. By default, the port is 1812.

accport

Specifies the UDP port for the RADIUS server for accounting. By default, the port is 1813.

*port\_number*

Specifies the UDP port. The port number is from 1 to 65535.

### Description

Use this command to add a RADIUS server to the authentication server list.

### Confirmation Command

“SHOW AUTHENTICATION” on page 188

### Example

The following command adds a RADIUS server of 192.168.1.208, the priority 1, and the password radius:

```
Manager > add radiusserver server=192.168.1.208 order=1  
secret=radius
```

## DELETE RADIUS SERVER

---

### Syntax

```
delete radiusserver server=ip_address
```

### Parameters

*ip\_address*

Specifies the IPv4 address of the RADIUS server.

### Description

Use this command to delete a RADIUS server from the RADIUS server list.

### Confirmation Command

“SHOW AUTHENTICATION” on page 188

### Example

The following command deletes a RADIUS server of 192.168.1.208 from the RADIUS server list:

```
Manager > delete radiusserver server=192.168.1.208
```

## DISABLE RADIUSACCOUNTING

---

### Syntax

```
disable radiusaccounting
```

### Parameters

None

### Description

Use this command to disable the accounting feature on RADIUS servers. By default, RADIUS server for accounting is disabled.

### Confirmation Command

“SHOW RADIUSACCOUNTING” on page 191

### Example

The following command disables the accounting features on RADIUS servers:

```
Manager > disable radiusaccounting
```

## ENABLE RADIUSACCOUNTING

---

### Syntax

```
enable radiusaccounting
```

### Parameters

None

### Description

Use this command to enable the accounting feature on RADIUS servers. By default, RADIUS server for accounting is enabled.

### Confirmation Command

“SHOW RADIUSACCOUNTING” on page 191

### Example

The following command enables the accounting features on RADIUS servers:

```
Manager > enable radiusaccounting
```

## SET AUTHENTICATION

---

### Syntax

```
set authentication [timeout=timeout] [deadtime=deadtime]  
[retransmitcount=retransmitcount]  
[dead-action=deny | permit]
```

### Parameters

#### *timeout*

Specifies the maximum amount of time in seconds that the RADIUS client waits for a response from a RADIUS authentication server. The range is 1 to 15 seconds. The default setting is 6 seconds.

#### *deadtime*

Specifies the amount of time in minutes that the RADIUS client stops communicating with a RADIUS server after the RADIUS client resends requests to the RADIUS server for the number of times specified with the *retransmitcount* parameter. The default setting is 0 minutes.

#### *retransmitcount*

Specifies the maximum number of times that the RADIUS client resends requests to the same RADIUS server before it sends requests to the next RADIUS server on the list. The default setting is 3 times.

#### *dead-action*

Specifies deny or permit communication when a RADIUS server does not respond. The default setting is deny.

### Description

Use this command to specify the settings of RADIUS authentication servers.

### Confirmation Command

“SHOW AUTHENTICATION” on page 188

### Example

The following command specifies the RADIUS client to wait for a response from the RADIUS server for 15 seconds:

```
Manager > set authentication timeout=15
```



## SET RADIUS

---

### Syntax

```
set radius [timeout=timeout] [deadtime=deadtime]  
[retransmitcount=retransmitcount]  
[dead-action=deny | permit]
```

---

### Note

This command is identical to the SET AUTHENTICATION command. See “SET AUTHENTICATION” on page 184.

---

## SET RADIUSACCOUNTING

---

### Syntax

```
set radiusaccounting [status=enabled | disabled]
[serverport=port_number] [type=network]
[trigger=start_stop | stop_only]
[updateenable=enabled | disabled] [interval=interval]
```

### Parameters

#### status

Specifies the RADIUS accounting server to be enabled or disabled.

#### serverport

Specifies the UDP port for the RADIUS server for accounting. The default setting is 1813. You must specify the same port number that is specified by the ADD RADIUSSERVER SERVER command.

#### type

Specifies the place to send accounting information. This is always network.

#### trigger

Specifies when the RADIUS client sends accounting requests to the RADIUS accounting server. The default setting is start\_stop.

#### start\_stop

Specifies that the RADIUS client sends accounting requests when a supplicant logs in and logs out.

#### stop\_only

Specifies that the RADIUS client sends accounting requests when a supplicant logs out.

#### updateenable

Specifies that sending interim accounting messages to the RADIUS accounting server is enabled or disabled. By default, sending interim accounting messages is disabled.

#### *interval*

Specifies the interval in seconds of sending interim accounting messages. The range is 30 to 300 seconds. The default setting is 60 seconds.

**Description**

Use this command to specify the settings of RADIUS accounting servers.

**Confirmation Command**

“SHOW RADIUSACCOUNTING” on page 191

**Example**

The following command specifies:

```
Manager > set radiusaccounting status=enabled
```

# SHOW AUTHENTICATION

### Syntax

show authentication

### Parameters

None

### Description

Use this command to display a list of RADIUS servers and their settings. An example of the command output is shown in Figure 30.

```

RADIUS Server Parameters
-----
Server Retransmit Count..... 3
Server Timeout..... 6 sec
Server Dead Time..... 0 min
Server Dead Action..... Deny
-----

RADIUS Servers:
Server IP Address Auth Port Encryption Key Auth Req Auth Resp Status
-----
0.0.0.0           1812      <Not Defined> 0           0           Alive
0.0.0.0           1812      <Not Defined> 0           0           Alive
    
```

Figure 30. SHOW AUTHENTICATION Command

The fields are described in Table 25.

Table 25. SHOW AUTHENTICATION Command

Field	Description
Server Retransmit Count	Displays the maximum number of times that the RADIUS client resends requests to the same RADIUS server before it sends requests to next RADIUS server on the list.
Server Timeout	Displays the maximum amount time in seconds that the RADIUS client waits for a response from a RADIUS server.

Table 25. SHOW AUTHENTICATION Command (Continued)

Field	Description
Server Dead Time	Displays the amount of time in minutes that the RADIUS client stops communicating with a RADIUS server after the RADIUS client resent requests to the RADIUS server for the maximum time.
Server Dead Action	Displays the communication is denied or permitted to respond when the RADIUS server has no response. The options are: <input type="checkbox"/> Deny <input type="checkbox"/> Respond
Server IP Address	Displays the IPv4 address of a RADIUS server.
Auth Port	Displays the UDP port for RADIUS servers for authentication.
Encryption Key	Displays whether the encryption key is defined for the RADIUS server.
Auth Req	Displays the number of authentication requests sent to the RADIUS server.
Auth Resp	Displays the number of received user authentication responses from the RADIUS server.

**Example**

The following example displays a list of RADIUS servers and their settings:

```
Manager > show authentication
```

## SHOW RADIUS

---

### Syntax

```
show radius
```

---

### Note

This command is identical to the SHOW AUTHENTICATION command. See “SHOW AUTHENTICATION” on page 188.

---

## SHOW RADIUSACCOUNTING

### Syntax

```
show radiusaccounting
```

### Parameters

None

### Description

Use this command to display the settings for RADIUS servers for accounting. An example of the command output is shown in Figure 31.

```

Radius Accounting Configuration
-----
Radius Accounting Status .....: Disabled
Radius Accounting Port.....: 1813
Radius Accounting Type.....: Network
Radius Accounting Trigger Type.....: Start_Stop
Radius Accounting Update Status.....: Disabled
Radius Accounting Update Interval....: 60

```

Figure 31. SHOW RADIUSACCOUNTING Command

The fields are described in Table 26.

Table 26. SHOW RADIUSACCOUNTING Command

Field	Description
Radius Accounting Status	Displays the accounting feature for RADIUS servers is Enabled or Disabled.
Radius Accounting Port	Displays the UDP port for RADIUS servers for accounting.
Radius Accounting Type	Displays the type of RADIUS servers for accounting. It is always network.
Radius Accounting Trigger Type	Displays when the RADIUS client sends accounting requests to the server. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> start-stop</li> <li><input type="checkbox"/> stop-only</li> </ul>
Radius Accounting Update Status	Displays sending interim accounting messages to the RADIUS accounting server is enabled or disabled.

Table 26. SHOW RADIUSACCOUNTING Command (Continued)

<b>Field</b>	<b>Description</b>
Radius Accounting Update Interval	Displays the interval in seconds of sending interim accounting messages.

**Example**

The following example displays the settings for RADIUS server for accounting:

```
Manager > show radiusaccounting
```



## Section III

# Layer 2 Switching

---

This section contains the following chapters:

- ❑ Chapter 12, "IP Management Commands" on page 195
- ❑ Chapter 13, "VLAN Commands" on page 209
- ❑ Chapter 14, "Switching Commands" on page 219
- ❑ Chapter 15, "Ethernet Protected Switched Ring (EPSR) Commands" on page 279
- ❑ Chapter 16, "Forwarding Database (FDB) Commands" on page 291
- ❑ Chapter 17, "DHCP Snooping Commands" on page 303
- ❑ Chapter 18, "Power Over Ethernet (PoE) Commands" on page 333
- ❑ Chapter 19, "Power Saving Commands" on page 345
- ❑ Chapter 20, "Rapid Spanning Tree Protocol (RSTP) Commands" on page 361
- ❑ Chapter 21, "Multiple Spanning Tree Protocol (MSTP) Commands" on page 377



## Chapter 12

# IP Management Commands

The IP management commands are summarized in Table 27.

Table 27. IP Management Commands

Command	Description
“ADD IP IPADDRESS” on page 196	Assigns an IPv4 address to the switch and specifies whether the switch responds to ping.
“DELETE IP” on page 198	Deletes the IPv4 address assigned from the switch.
“DISABLE IP DHCP” on page 199	Disables the DHCP client.
“DISABLE IP REMOTEASSIGN” on page 200	Disables the DHCP client.
“ENABLE IP DHCP” on page 201	Enables the DHCP client.
“ENABLE IP REMOTEASSIGN” on page 202	Enables the DHCP client
“PING” on page 203	Tests the communication with the specified IP address.
“SET IP” on page 204	Changes the IPv4 address and settings on the switch.
“SHOW IP” on page 206	Displays the settings of IPv4 address on the switch.

## ADD IP IPADDRESS

---

### Syntax

```
add ip [interface=vlan_name|vlan_id]  
ipaddress=ip_address|dhcp [mask=subnet_mask]  
[gateway=ip_address] [directedbroadcast=yes|no|on|off]
```

### Parameters

**interface**

Specifies a VLAN interface with either a VLAN name or VLAN ID. The default is the default VLAN.

*vlan\_name*

Specifies a VLAN name.

*vlan\_id*

Specifies a VLAN ID. The range is 1 to 4094

**ipaddress**

Assigns an IPv4 address to the VLAN interface statically or dynamically.

*ip\_address*

Specifies an IPv4 address.

**dhcp**

Specifies DHCP to assign an IPv4 address dynamically.

**mask**

Specifies the subnet mask of the IPv4 address.

**gateway**

Specifies the IPv4 address of the gateway.

**directedbroadcast**

Specifies whether the VLAN interface responds to the directed broadcast ping. By default is no.

**yes, on**

Specifies the VLAN interface responds to the directed broadcast ping.

**no, off**

Specifies the VLAN interface does not respond to the directed broadcast ping.

## Description

Use this command to assign the IPv4 address to a VLAN interface and specify the action to respond to ping. You can assign only one IPv4 address to the switch.

## Confirmation Command

“SHOW IP” on page 206

## Example

The following command assigns the IPv4 address 192.168.1.5/24 to the default VLAN and 192.168.1.1 to the gateway:

```
Manager > add ip ipaddress=192.168.1.5 mask=255.255.255.0  
gateway=192.168.1.1
```

The following command specifies DHCP to assign an IPv4 address dynamically to the default VLAN:

```
Manager > add ip ipaddress=dhcp
```

## DELETE IP

---

### Syntax

```
delete ip
```

### Parameters

None

### Description

Use this command to delete the IPv4 address setting from the switch.

### Confirmation Command

“SHOW IP” on page 206

### Example

The following command deletes the IPv4 address setting from the switch:

```
Manager > delete ip
```

## DISABLE IP DHCP

---

### Syntax

```
disable ip dhcp
```

### Parameters

None

### Description

Use this command to disable the DHCP client on the switch. By default, The DHCP client is disabled.

### Confirmation Command

“SHOW IP” on page 206

### Example

The following command disables the DHCP client on the switch:

```
Manager > disable ip dhcp
```

## DISABLE IP REMOTEASSIGN

---

### Syntax

```
disable ip remoteassign
```

---

### Note

This command is identical to the DISABLE IP DHCP command. See “DISABLE IP DHCP” on page 199.

---



## ENABLE IP DHCP

---

### Syntax

```
enable ip dhcp
```

### Parameters

None

### Description

Use this command to enable the DHCP client on the switch. By default, the DHCP client is disabled.

### Confirmation Command

“SHOW IP” on page 206

### Example

The following command enables the DHCP client on the switch:

```
Manager > enable ip dhcp
```

## ENABLE IP REMOTEASSIGN

---

### Syntax

```
enable ip remoteassign
```

---

### Note

This command is identical to the ENABLE IP DHCP command. See “ENABLE IP DHCP” on page 201.

---

# PING

---

## Syntax

```
ping ipaddress=ip_address
```

## Parameters

*ip\_address*

Specifies an IPv4 address.

## Description

Use this command to ping the specified IP address. To stop the execution, enter Ctrl + c. An example of the command output is shown in Figure 32.

```
Manager > ping 192.168.1.1
PINGing 192.168.1.1 with 64 bytes of data:
Reply 1 from 192.168.1.1: bytes=64 times=114ms
Reply 2 from 192.168.1.1: bytes=64 times=41ms
Reply 3 from 192.168.1.1: bytes=64 times=42ms
Reply 4 from 192.168.1.1: bytes=64 times=42ms
Reply 5 from 192.168.1.1: bytes=64 times=71ms

Ping statistics for 192.168.1.1
    Packets: Sent = 5, Received = 5, Bad = 0, Lost = 0(0%loss)
Approximate round trip times in milliseconds:
    Minimum = 41ms, Maximum = 114ms, Average = 62ms
```

Figure 32. PING Command

## Confirmation Command

“SHOW IP” on page 206

## Example

The following command tests the communication with 192.168.1.10:

```
Manager > ping 192.168.1.10
```

## SET IP

---

### Syntax

```
set ip [ipaddress=ip_address|dhcp] [mask=subnet_mask]  
[gateway=ip_address] [directedbroadcast=yes|no|on|off]
```

### Parameters

#### ipaddress

Assigns an IPv4 address to the VLAN interface statically or dynamically.

#### dhcp

Specifies DHCP to assign an IPv4 address.

#### mask

Specifies the subnet mask of the IPv4 address.

#### gateway

Specifies the IPv4 address of the gateway.

#### *ip\_address*

Specifies an IPv4 address.

#### directedbroadcast

Specifies whether the interface responds to the directed broadcast ping. By default is no.

#### yes, on

Specifies the interface responds to the directed broadcast ping.

#### no, off

Specifies the interface does not respond to the directed broadcast ping.

### Description

Use this command to change the IP settings.

### Confirmation Command

“SHOW IP” on page 206

### Example

The following command changes the IP address to 192.168.1.6/24 and the gateway to 192.168.1.254:

```
Manager > set ip ipaddress=192.168.1.6 mask=255.255.255.0  
gateway=192.168.1.254
```

## SHOW IP

---

### Syntax

```
show ip
```

### Parameters

None

### Description

Use this command to display the settings of IP address on the switch. An example of the command output is shown in Figure 33.

```

IP Address Information
-----
Type ..... Static
Interface ..... default
IP address ..... 192.168.1.105
Subnet mask ..... 255.255.255.0
Gateway address ..... 0.0.0.0
MTU ..... 1500
DHCP Client ..... Disabled
Directed broadcast ..... No
-----

```

Figure 33. SHOW IP Command

The fields are described in Table 28.

Table 28. SHOW IP Command

Field	Description
Type	Displays the assignment type of the IP address. The options are: <ul style="list-style-type: none"> <li><input type="checkbox"/> Static</li> <li><input type="checkbox"/> Dynamic: assigned by DHCP</li> </ul>
Interface	Displays the VLAN interface that the IPv4 address is assigned to.
IP address	Displays the IPv4 address.
Subnet mask	Displays the subnet mask.
Gateway address	Displays the IPv4 address of the gateway.
MTU	Displays the maximum size of transmitting packets.

Table 28. SHOW IP Command (Continued)

<b>Field</b>	<b>Description</b>
DCHP client	Displays whether the DHCP client is Enabled or Disabled.
DHCP server	Displays the IPv4 address of the DHCP server. This is displayed only when the IPv4 address was assigned to the switch using the DHCP server.
Directed broadcast	Displays whether the switch responds to the directed broadcast ping.

**Example**

The following example displays the settings of the IP address on the switch:

```
Manager > show ip
```





## Chapter 13

# VLAN Commands

---

The VLAN commands are summarized in Table 29.

Table 29. VLAN Commands

Command	Description
“ADD VLAN PORT” on page 210	Assigns the VLAN to ports either tagged or untagged.
“CREATE VLAN” on page 212	Creates a VLAN.
“DELETE VLAN PORT” on page 213	Deletes a port from a VLAN.
“DESTROY VLAN” on page 214	Deletes a VLAN from the switch.
“SET VLAN PORT” on page 215	Changes tagged or untagged VLAN to the port.
“SHOW VLAN” on page 216	Displays information about the specified VLANs.

## ADD VLAN PORT

---

### Syntax

```
add vlan=vlan_name|vid port=port_list|all  
[frame=tagged|untagged] [group=uplink|auto|group_number]
```

### Parameters

*vlan*

Specifies a VLAN with either the VLAN name or VLAN ID.

*vlan\_name*

Specifies a VLAN name.

*vid*

Specifies a VLAN ID. The range is 2 to 4094.

*port\_list*

Specifies a list of ports to assign the VLAN to. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

frame

Assigns the port as tagged or untagged. The default setting is untagged.

tagged

Assigns the VLAN to the specified ports as tagged.

untagged

Assigns the VLAN to the specified ports as untagged. A port can belong to only one VLAN as a untagged port.

group

Specifies that the ports are for uplink or for clients.

uplink

Specifies the ports to uplink.

auto

A group is assigned automatically to each port.

*group\_number*

Specifies a group number. The range is 1 to 65535.

**Description**

Use this command to assign the VLAN to ports either tagged or untagged.

**Confirmation Command**

“SHOW VLAN” on page 216

**Example**

The following command assigns the VLAN test to ports 1 to 5:

```
Manager > add vlan=test port=1-5
```

## CREATE VLAN

---

### Syntax

```
create vlan=vlan_name vid=vlan_id [portprotected]
```

### Parameters

*vlan\_name*

Specifies the name of a new VLAN. The VLAN name can be from 1 to 20 alphanumeric characters including hyphen (-), underscore (\_), period (.), and parentheses (). The first letter must be an alphabet. The VLAN name is *not* case-sensitive; however, it is displayed as entered.

*vlan\_id*

Specifies a VLAN ID. The range is 2 to 4094.

portprotected

Specifies the new VLAN to the port-protected.

### Description

Use this command to create a VLAN. You can create up to 255 VLANs.

### Confirmation Command

“SHOW VLAN” on page 216

### Example

The following command creates a new VLAN called test with VLAN ID 10:

```
Manager > create vlan=test vid=10
```

## DELETE VLAN PORT

---

### Syntax

```
delete vlan=vlan_name|vlan_id] port=port_list|all
```

### Parameters

*vlan*

Specifies a VLAN with either the VLAN name or VLAN ID.

*vlan\_name*

Specifies a VLAN name.

*vlan\_id*

Specifies a VLAN ID. The range is 2 to 4094.

*port\_list*

Specifies a list of ports to assign to the VLAN. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to delete the specified ports from the VLAN:

### Confirmation Command

“SHOW VLAN” on page 216

### Example

The following command deletes ports 1 to 5 from the VLAN test:

```
Manager > delete vlan=test port=1-5
```

## DESTROY VLAN

---

### Syntax

```
destroy vlan=[vlan_name|vlan_id|all]
```

### Parameters

*vlan*

Specifies a VLAN with either the VLAN name or VLAN ID.

*vlan\_name*

Specifies a VLAN name.

*vlan\_id*

Specifies a VLAN ID. The range is 2 to 4094.

*all*

Specifies all VLANs.

### Description

Use this command to delete the specified VLAN from the switch.

### Confirmation Command

“SHOW VLAN” on page 216

### Example

The following command deletes VLAN 10 from the switch:

```
Manager > destroy vlan=10
```

## SET VLAN PORT

---

### Syntax

```
set vlan=vlan_name|vlan_id port=port_list|all
[frame=tagged|untagged]
```

### Parameters

*vlan*

Specifies a VLAN with either the VLAN name or VLAN ID.

*vlan\_name*

Specifies a VLAN name.

*vlan\_id*

Specifies a VLAN ID.

*port\_list*

Specifies a list of ports to assign to the VLAN. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

frame

Assigns the port as tagged or untagged.

tagged

Assigns the VLAN to the specified ports as tagged.

untagged

Assigns the VLAN to the specified ports as untagged. A port can belong to only one VLAN as a untagged port.

### Description

Use this command to change tagged or untagged VLAN to the ports.

### Confirmation Command

“SHOW VLAN” on page 216

### Example

The following command changes the untagged VLAN to tagged VLAN:

```
Manager > set vlan=20 port=5 frame=tagged
```

## SHOW VLAN

---

### Syntax

```
show vlan[=vlan_name|vlan_id|all]
```

### Parameters

*vlan*

Specifies a VLAN with either the VLAN name or VLAN ID.

*vlan\_name*

Specifies a VLAN name.

*vlan\_id*

Specifies a VLAN ID.

all

Specifies all VLANs. This is the default setting.

### Description

Use this command to display information about the specified VLANs. An example of the command output is shown in Figure 34.

```

VLAN Information
-----
Name ..... default
Identifier ..... 1
Status ..... Static
Protected Ports ..... None
Untagged Ports ..... All
Tagged Ports ..... None
Spanning Tree ..... default
Trunk Ports ..... None
Mirror Port ..... None
IP Interface ..... Yes
-----

```

Figure 34. SHOW VLAN Command

The fields are described in Table 30.

Table 30. SHOW VLAN Command

Field	Description
Name	Displays the name of a VLAN.
Identifier	Displays the VLAN ID.
Status	Displays the status. It is always Static.



Table 30. SHOW VLAN Command (Continued)

Field	Description
Protected Ports	Displays the setting of the VLAN ports. The options are: <input type="checkbox"/> Yes - Protected VLAN ports <input type="checkbox"/> None - Not protected VLAN ports
Configured	Displays a list of ports that are configured statically.
Actual	Displays a list of ports that belong to the VLAN.
Untagged Ports	Displays the port numbers of untagged ports.
Tagged Ports	Displays the port numbers of tagged ports.
Spanning Tree	Displays the name of STP domain.
Trunk Ports	Displays the port number of trunk.
Mirror Ports	Displays the port number of the mirror ports.
IP Interface	Display whether the VLAN has an IP address assigned.

**Example**

The following example displays information about all VLANs:

```
Manager > show vlan
```



## Chapter 14

# Switching Commands

The Switching commands are summarized in Table 31.

Table 31. Switching Commands

Command	Description
“ACTIVATE SWITCH PORT AUTONEGOTIATE” on page 222	Enables Auto-negotiation to ports.
“ADD SWITCH TRUNK” on page 223	Adds a list of ports to a trunk group.
“CREATE SWITCH TRUNK” on page 224	Creates a trunk group.
“DELETE SWITCH TRUNK” on page 226	Removes the ports from the trunk group.
“DESTROY SWITCH TRUNK” on page 227	Deletes a trunk group.
“DISABLE SWITCH BPDFORWARDING” on page 228	Disables Bridge Protocol Data Unit (BPDU) protection.
“DISABLE SWITCH EAPFORWARDING” on page 229	Disables Extensible Authentication Protocol (EAP) authentication.
“DISABLE SWITCH INFILTERING” on page 230	Disables the ingress filtering feature.
“DISABLE SWITCH LOOPDETECTION” on page 231	Disables Loop Detection.
“DISABLE SWITCH MIRROR” on page 232	Disables port mirroring.
“DISABLE SWITCH PORT” on page 233	Disables switch ports.
“DISABLE SWITCH PORT AUTOMDI” on page 234	Disables ports to automatically detect MDI or MDI-X.
“DISABLE SWITCH PORT FLOW” on page 235	Disables flow control on ports.

Table 31. Switching Commands (Continued)

Command	Description
"DISABLE SWITCH POWERSAVE" on page 236	Disables the power saving mode on the switch.
"DISABLE SWITCH STORMDETECTION" on page 237	Disables detecting the receiving rate.
"ENABLE SWITCH BPDFORWARDING" on page 238	Enables Bridge Protocol Data Unit (BPDU) protection.
"ENABLE SWITCH EAPFORWARDING" on page 239	Enables Extensible Authentication Protocol (EAP) authentication.
"ENABLE SWITCH INFILTERING" on page 240	Enables the ingress filtering feature.
"ENABLE SWITCH LOOPDETECTION" on page 241	Enables loop detection.
"ENABLE SWITCH MIRROR" on page 242	Enables port mirroring.
"ENABLE SWITCH PORT" on page 243	Enables switch ports.
"ENABLE SWITCH PORT AUTOMDI" on page 244	Enables ports to automatically detect MDI or MDI-X.
"ENABLE SWITCH PORT FLOW" on page 245	Enables Flow Control on ports.
"ENABLE SWITCH POWERSAVE" on page 246	Enables the power saving mode on the switch.
"ENABLE SWITCH STORMDETECTION" on page 247	Enables Storm Detection.
"RESET SWITCH" on page 248	Clears dynamically learned information, timers, and statistics counters.
"RESET SWITCH LOOPDETECTION COUNTER" on page 249	Clears counters for Loop Detection.
"RESET SWITCH PORT" on page 250	Resets ports by starting Auto-negotiation and clears statistics counters.

Table 31. Switching Commands (Continued)

Command	Description
"RESET SWITCH STORMDETECTION COUNTER" on page 251	Clears counters for Storm Detection.
"SET SWITCH LIMITATION" on page 252	Specifies the limitation of the receiving rate for Storm Detection.
"SET SWITCH LOOPDETECTION" on page 253	Specifies actions for Loop Detection.
"SET SWITCH MIRROR" on page 255	Specifies a port as the mirror port or disable port mirroring.
"SET SWITCH PORT" on page 257	Specifies the mirror port, communication mode, receiving frame type, security mode, or combo port.
"SET SWITCH STORMDETECTION" on page 263	Specifies actions for Storm Detection.
"SET SWITCH TRUNK" on page 266	Changes the settings of trunk groups.
"SHOW SWITCH" on page 267	Displays information about the switch.
"SHOW SWITCH COUNTER" on page 268	Displays statistics counters on the switch.
"SHOW SWITCH LOOPDETECTION" on page 269	Displays information about Loop Detection.
"SHOW SWITCH MIRROR" on page 271	Displays information about mirroring.
"SHOW SWITCH PORT" on page 272	Displays information about ports.
"SHOW SWITCH PORT COUNTER" on page 274	Displays statistics counters on ports.
"SHOW SWITCH STORMDETECTION" on page 276	Displays information about Storm Detection.
"SHOW SWITCH TRUNK" on page 278	Displays information about trunk groups.

## ACTIVATE SWITCH PORT AUTONEGOTIATE

---

### Syntax

```
activate switch port=port_list|all autonegotiate
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to enable Auto-negotiation to the specified ports.

### Confirmation Command

“SHOW SWITCH PORT” on page 272

### Example

The following command enables Auto-negotiation to all ports:

```
Manager > activate switch port=all autonegotiate
```

## ADD SWITCH TRUNK

---

### Syntax

```
add switch trunk=trunk_name port=port_list
```

### Parameters

*trunk\_name*

Specifies the name of a trunk group.

*port\_list*

Specifies a list of ports to add to the trunk group. One trunk can have up to 8 ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

### Description

Use this command to add a list of ports to a trunk group. For the guidelines for trunk groups, see page 224.

### Confirmation Command

“SHOW SWITCH TRUNK” on page 278

### Example

The following command adds port 1 to the trunk uplink:

```
Manager > add switch trunk=uplink port=1
```

## CREATE SWITCH TRUNK

---

### Syntax

```
create switch trunk=trunk_name [port=port_list]
[speed=1000m|100m|10m]
```

### Parameters

#### *trunk\_name*

Specifies the name of a trunk group. The trunk name can be from 1 to 20 alphanumeric characters including hyphen (-), underscore (\_), period (.), and parentheses (()). The name is not case-sensitive; however, it is displayed as entered.

#### *port\_list*

Specifies a list of ports to add to the trunk group. One trunk can have up to 8 ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### speed

Specifies the speed of the trunk port. The options are 1000M, 100M, and 10M. The default setting is 1000M. The combo ports have only 1000M option. All ports are in the full duplex mode.

### Description

Use this command to create a trunk group.

Here are the guidelines for creating a trunk group:

- One trunk group can have up to 8 trunk member ports.
- The GS908M V2 switch can have up to 4 trunk groups.
- The GS908M V2-4PS can have up to 5 trunk groups.
- The GS916M V2 and GS924M V2 switches can have up to 8 trunk groups.
- The port with the smallest port number is the master port of the trunk group.
- A port can belong to only one trunk group.
- A mirror port cannot be a trunk member.
- An authenticator and supplicant port for Port-based Authentication cannot be a trunk member.
- The member ports in the same trunk group must belong to the same VLAN.
- An STP-enabled port and an STP-disabled port cannot belong to



the same trunk group.

- ❑ A Loop Detection enabled port and a Loop Detection disabled port cannot belong to the same trunk group.
- ❑ A port that is set the security mode cannot be a trunk member.
- ❑ MDI/MDI-X automatic detection cannot be enabled on a trunk member port.
- ❑ Port 9 on the GS908M V2 switch cannot be a trunk member.
- ❑ The 100M SFP port cannot be a trunk member.
- ❑ Broadcast, multicast, and unlearned unicast frames are sent from the master port.

### **Confirmation Command**

“SHOW SWITCH TRUNK” on page 278

### **Example**

The following command creates a new trunk group of uplink:

```
Manager > create switch trunk=uplink
```

## DELETE SWITCH TRUNK

---

### Syntax

```
delete switch trunk=trunk_name port=port_list|all
```

### Parameters

*trunk\_name*

Specifies the name of a trunk group.

*port\_list*

Specifies a list of ports to delete. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to remove the specified ports from the trunk group.

### Confirmation Command

“SHOW SWITCH TRUNK” on page 278

### Example

The following command deletes port 1 from the trunk group uplink:

```
Manager > delete switch trunk=uplink port=1
```

## DESTROY SWITCH TRUNK

---

### Syntax

```
destroy switch trunk=trunk_name
```

### Parameters

*trunk\_name*

Specifies the name of a trunk group.

### Description

Use this command to delete the trunk group.

### Confirmation Command

“SHOW SWITCH TRUNK” on page 278

### Example

The following command deletes the trunk uplink:

```
Manager > destroy switch trunk=uplink
```

## DISABLE SWITCH BPDUFORWARDING

---

### Syntax

```
disable switch bpduforwarding
```

### Parameters

None

### Description

Use this command to disable Bridge Protocol Data Unit (BPDU) protection. By default, BPDU protection is disabled.

---

#### Note

When the switch has a port that STP is enabled on, BPDU cannot be enabled.

---

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command disables BPDU protection:

```
Manager > disable switch bpduforwarding
```

## DISABLE SWITCH EAPFORWARDING

---

### Syntax

```
disable switch eapforwarding
```

### Parameters

None

### Description

Use this command to disable Extensible Authentication Protocol (EAP) authentication. By default, EAP protection is disabled.

---

#### Note

When Port-based Authentication is enabled on the switch, EAP cannot be enabled.

---

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command disables EAP authentication:

```
Manager > disable switch eapforwarding
```

## DISABLE SWITCH INFILTERING

---

### Syntax

```
disable switch infiltering
```

### Parameters

None

### Description

Use this command to disable the ingress filtering feature. When the ingress filtering feature is enabled, a switch port accepts only frames that have the same VLAN ID with the port. By default, EAP protection is disabled.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command disables the ingress filtering feature on the switch:

```
Manager > disable switch infiltering
```

## DISABLE SWITCH LOOPDETECTION

---

### Syntax

```
disable switch loopdetection port=port_list|all
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to disable loop protection. By default, loop protection is disabled.

### Confirmation Command

“SHOW SWITCH LOOPDETECTION” on page 269

### Example

The following command disables loop protection on port 2:

```
Manager > disable switch loopdetection port=2
```

## DISABLE SWITCH MIRROR

---

### Syntax

```
disable switch mirror
```

### Parameters

None

### Description

Use this command to disable port mirroring on the switch. By default, port mirroring is disabled.

### Confirmation Command

“SHOW SWITCH MIRROR” on page 271

### Example

The following command disables port mirroring on the switch:

```
Manager > disable switch mirror
```



## DISABLE SWITCH PORT

---

### Syntax

```
disable switch port=port_list|all [link=enabled|disabled]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### link

Specifies the port to be physically enabled or disabled. Without this parameter, the port is physically enabled.

### Description

Use this command to disable switch ports.

---

#### Note

To enable the port physically after disabling it with the link parameter, use the ENABLE SWITCH PORT command. See “ENABLE SWITCH PORT” on page 243.

---

### Confirmation Command

“SHOW SWITCH PORT” on page 272

### Examples

The following command disables port 5 to port 10.

```
Manager > disable switch port=5-10
```

The following command physically disables port 5 to port 10.

```
Manager > disable switch port=5-10 link=disabled
```

## DISABLE SWITCH PORT AUTOMDI

---

### Syntax

```
disable switch port=port_list|all automdi
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports except SFP and combo ports.

### Description

Use this command to disable switch ports to automatically detect MDI or MDI-X. By default, the MDI auto-detection is enabled.

Here are guidelines for using MDI auto-detection on ports:

- ❑ The SFP and combo ports cannot be disabled the MDI auto-detection by this command.
- ❑ You cannot disable the MDI auto-detection on trunk member ports; however, you can add a port that the MDI auto-detection is disabled on to a trunk group.
- ❑ The port that is set the 100M speed cannot be disabled the MDI auto-detection by this command.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command disables the MDI auto-detection on port 3:

```
Manager > disable switch port=3 automdi
```

## DISABLE SWITCH PORT FLOW

---

### Syntax

```
disable switch port=port_list|all flow
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to disable flow control on switch ports. By default, flow control is enabled.

To disable flow control on a trunk port, you must specify all trunk ports in a trunk group.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command disables flow control on port 3:

```
Manager > disable switch port=3 flow
```

## DISABLE SWITCH POWERSAVE

---

### Syntax

```
disable switch powersave
```

### Parameters

None

### Description

Use this command to disable the power saving mode on the switch. By default, the power saving mode is disabled.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command disables the power saving mode:

```
Manager > disable switch powersave
```

## DISABLE SWITCH STORMDETECTION

---

### Syntax

```
disable switch stormdetection port=port_list|all
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to disable detecting the receiving rate. By default, detecting the receiving rate is disabled.

### Confirmation Command

“SHOW SWITCH STORMDETECTION” on page 276

### Example

The following command disables detecting the receiving rate:

```
Manager > disable switch stormdetection port=2
```

## ENABLE SWITCH BPDUFORWARDING

---

### Syntax

```
enable switch bpduforwarding
```

### Parameters

None

### Description

Use this command to enable Bridge Protocol Data Unit (BPDU) protection. By default, BPDU protection is disabled.

---

#### Note

When the switch has a port that STP is enabled on, BPDU cannot be enabled.

---

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command enables BPDU protection:

```
Manager > enable switch bpduforwarding
```

## ENABLE SWITCH EAPFORWARDING

---

### Syntax

```
enable switch eapforwarding
```

### Parameters

None

### Description

Use this command to enable Extensible Authentication Protocol (EAP) authentication. By default, EAP protection is disabled.

---

**Note**

When Port Authentication is enabled on the switch, EAP cannot be enabled.

---

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command enables EAP authentication:

```
Manager > enable switch eapforwarding
```

## ENABLE SWITCH INFILTERING

---

### Syntax

```
enable switch infiltering
```

### Parameters

None

### Description

Use this command to enable the ingress filtering feature. When the ingress filtering feature is enabled, a switch port accepts only frames that have the same VLAN ID with the port. By default, EAP protection is disabled.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command enables the ingress filtering feature on the switch:

```
Manager > enable switch infiltering
```



## ENABLE SWITCH LOOPDETECTION

---

### Syntax

```
enable switch loopdetection port=port_list|all
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to enable loop protection. By default, loop protection is disabled on the specified ports.

### Confirmation Command

“SHOW SWITCH LOOPDETECTION” on page 269

### Example

The following command enables loop protection on port 2:

```
Manager > enable switch loopdetection port=2
```

## ENABLE SWITCH MIRROR

---

### Syntax

```
enable switch mirror
```

### Parameters

None

### Description

Use this command to enable port mirroring on the switch. By default, port mirroring is disabled.

### Confirmation Command

“SHOW SWITCH MIRROR” on page 271

### Example

The following command enables port mirroring on the switch:

```
Manager > enable switch mirror
```

## ENABLE SWITCH PORT

---

### Syntax

```
enable switch port=port_list|all
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to enable switch ports.

### Confirmation Command

“SHOW SWITCH PORT” on page 272

### Example

The following command enables port 5 to port 10.

```
Manager > enable switch port=5-10
```

## ENABLE SWITCH PORT AUTOMDI

---

### Syntax

```
enable switch port=port_list|all automdi
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports except SFP and combo ports.

### Description

Use this command to enable switch ports to automatically detect MDI or MDI-X. By default, the MDI auto detection is enabled.

Here are guidelines for using this command:

- ❑ The SFP and combo ports cannot be disabled the MDI auto-detection by this command.
- ❑ You cannot disable the MDI auto-detection on trunk ports.
- ❑ You can add the ports that the MDI auto-detection is disabled to a trunk group.
- ❑ The port that is set the 100M speed cannot be disabled the MDI auto detection by this command.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command enables the MDI auto-detection on port 3:

```
Manager > enable switch port=3 automdi
```

## ENABLE SWITCH PORT FLOW

---

### Syntax

```
enable switch port=port_list|all flow
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to enable flow control on switch ports. By default, flow control is enabled. When flow control is enabled, the ports accept PAUSE frames, but does not send PAUSE frames.

To enable flow control on a trunk port, you must specify all trunk ports in the trunk group.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command enables flow control on port 3:

```
Manager > enable switch port=3 flow
```

## ENABLE SWITCH POWERSAVE

---

### Syntax

```
enable switch powersave
```

### Parameters

None

### Description

Use this command to enable the power saving mode on the switch. When the power saving mode is enabled, the switch saves power by limiting power on the ports with no link. By default, the power saving mode is disabled.

---

#### Note

When the power saving mode is enabled, the switch saves power by limiting power on ports with no link. The ports take up to 3 seconds to get the link up state.

---

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command enables the power saving mode:

```
Manager > enable switch powersave
```

## ENABLE SWITCH STORMDETECTION

---

### Syntax

```
enable switch stormdetection port=port_list|all
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to enable detecting the receiving rate. By default, detecting the receiving rate is disabled.

To enable detecting the receiving rate on a trunk port, you must specify all trunk ports in the trunk group.

### Confirmation Command

“SHOW SWITCH STORMDETECTION” on page 276

### Example

The following command enables detecting the receiving rate:

```
Manager > enable switch stormdetection port=2
```

## RESET SWITCH

---

### Syntax

```
reset switch [counter]
```

### Parameters

counter

Clears the counter of dynamic entries in the MAC table, timer, and static counters.

### Description

Use this command to reset the switch ports and clear the counter of dynamic entries in Forwarding Database (FDB), timer, and statistics counters.

### Confirmation Command

“SHOW SWITCH” on page 267

### Example

The following command resets the switch ports:

```
Manager > reset switch
```



## RESET SWITCH LOOPDETECTION COUNTER

---

### Syntax

```
reset switch loopdetection [port=port_list|all] counter
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports. This is the default setting.

### Description

Use this command to clear the counters of the loop detection feature on the specified ports.

### Confirmation Command

“SHOW SWITCH LOOPDETECTION” on page 269

### Example

The following command clears the counters of the loop detection feature on port 2:

```
Manager > reset switch loopdetection port=2 counter
```

## RESET SWITCH PORT

---

### Syntax

```
reset switch port[=port_list|all] [counter]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports. This is the default setting.

counter

Clears only statistics counters without physically resetting the ports.

### Description

Use this command to physically reset a switch port: starting Auto-negotiation and clearing the statistics counters on the port. With the keyword counter, the command does not reset the port physically.

### Confirmation Command

“SHOW SWITCH PORT” on page 272

### Examples

The following command physically resets port 1 to port 10:

```
Manager > reset switch port=1-10 counter
```

## RESET SWITCH STORMDETECTION COUNTER

---

### Syntax

```
reset switch stormdetection [port=port_list|all] counter
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports. This is the default setting.

### Description

Use this command to clear the counters of detecting the receiving rate.

### Confirmation Command

“SHOW SWITCH STORMDETECTION” on page 276

### Example

The following command clears the counters of detecting the receiving rate on port 2:

```
Manager > reset switch stormdetection port=2 counter
```

## SET SWITCH LIMITATION

---

### Syntax

```
set switch limitation[=none|0|receiving_rate]
```

### Parameters

none, 0

Disables the packet storm protection. The default value is 0.

*receiving\_rate*

Specifies the maximum receiving rate. The range is 1 to 1024000 Kbps.

### Description

Use this command to specify the maximum receiving rate for the packet storm protection. When the keyword none or 0 is specified, the packet storm protection is disabled. By default, the packet storm protection is disabled.

### Confirmation Command

“SHOW SWITCH STORMDETECTION” on page 276

### Example

The following command sets the maximum receiving rate to 10240 Kbps:

```
Manager > set switch limitation=10240
```

## SET SWITCH LOOPDETECTION

---

### Syntax

```
set switch loopdetection port[=port_list|all]
[action=portdisable|linkdown|bcdiscard|none]
[interval=interval] [secure=on|off]
[blocktimeout=timeout|none]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### action

Specifies an action when the port detects the loop. The port stops the action after the time specified by the blocktimeout parameter has passed.

#### portdisable

Specifies that the port is disabled when detecting the loop. This is the default setting.

#### linkdown

Specifies that the port is disconnected when detecting the loop.

#### bcdiscard

Specifies that the port stops receiving broadcast frames when detecting the loop.

#### none

Specifies that the port takes no action. However, the switch issues log messages.

#### *interval*

Specifies the interval of sending a Loop Detection Frame (LDF) in seconds. The default setting is 120 seconds.

#### secure

Specifies an action when the port receives an LDF.

#### on

Specifies that the port discards the LDF if the ID code in the LDF is different from the effective ID code. The ID code is effective during the specified interval. This is the default setting.

- off**  
Specifies that the port does not check the ID code in the LDF.
- blocktimeout**  
Specifies duration in seconds when the port takes the action specified by the action parameter.
- timeout**  
Specifies time in seconds. The default value is 300 seconds.
- none**  
Specifies that the port does not stop taking the action specified by the action parameter.

### Description

Use this command to specify the actions of Loop Detection.

Here are guidelines for Loop Detection:

- Allied Telesis recommends the linkdown action for trunk ports.
- You cannot specify the action of `bcdiscard` on the ports that the Packet Storm Protection is enabled.
- Allied Telesis recommends 1 second or longer for the interval parameter and 60 seconds or longer for the `blocktimeout` parameter when the action is set to linkdown.
- To cancel the action that the port took when the loop is detected:
  - Execute the `ENABLE SWITCH PORT` command.
  - Execute the `DISABLE SWITCH PORT` command
  - The port is disconnected.
  - Modify the power saving mode to `portoff`.

### Confirmation Command

“`SHOW SWITCH LOOPDETECTION`” on page 269

### Example

The following command sets port 2 to send a LDF every 60 seconds and to be disconnected for 3600 seconds when the loop is detected:

```
Manager > set switch loopdetection port=2 action=linkdown  
interval=60 blocktimeout=3600
```

## SET SWITCH MIRROR

---

### Syntax

```
set switch mirror=port_number|none
```

### Parameters

*port\_number*

Specifies a port as the mirror port.

none

Cancel the mirror port and disables port mirroring.

### Description

Use this command to specify a port as the mirror port or disable port mirroring. To specify a source port and target traffic, use the SET SWITCH PORT command.

Here are guidelines for port mirroring:

- The switch has only one mirror port.
- The following ports cannot be the mirror port:
  - Ports that belong to other than default VLAN
  - Ports that Port Security is enabled on
  - Authenticator and supplicant ports for Authentication
  - Trunk ports
  - Ports belong to other than default VLAN
- The mirror port does not function as a switch port even when Port Mirroring is disabled.
- STP cannot be enabled on the mirror port.

### Confirmation Command

“SHOW SWITCH MIRROR” on page 271

### Examples

The following command specifies port 1 as the mirror port:

```
Manager > set switch mirror=1
```

The following command disables port mirroring:

```
Manager > set switch mirror=none
```



## SET SWITCH PORT

---

### Syntax

```
set switch port[=port_list|all] [acceptable=all|vlan]
[description=string] [mirror=both|none|rx|tx]
[priority=priority]
[speed=autonetotiate|10mhalf|10mfull|10mhalfauto|10mfauto|
100mhalf|100mfull|100mhalfauto|100mfauto|1000mfull|1000mauto]
[securitymode=automatic|dynamic|limited|secured]
[learn=max_mac] [intrusionaction=discard|disable|log|trap]
[combo=fiberauto|copperauto|fiber|copper]
[polarity=mdi|mdix] [bclimit=on|off] [dlclimit=on|off]
[mclimit=on|off]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### acceptable

Specifies the frames that the port can accept.

#### vlan

Specifies the port to accept VLAN tagged frames. The port discards the frames in which the VID is 0. The ports that belong to only a tagged VLAN are always this setting.

#### all

Specifies the port to accept all frames. The ports that belong to an untagged VLAN are always this setting.

#### *string*

Specifies a port name up to 20 alphanumeric characters including hash (#), percent (%), question (?), and yen mark (¥). To include a space, place a double quote (") before and after the space.

#### mirror

Specifies the traffic type to be mirrored. Pause frames are also mirrored. You must specify the same traffic type on the switch.

#### rx

The receiving frames at the port are mirrored.

#### tx

The transmitting frames at the port are mirrored.

`both`  
Both receiving and transmitting frames at the port are mirrored.

`none`  
Specifies the port to be not mirrored.

`priority`  
Specifies a user priority. The range is 0 to 7. The default value is 0.

`speed`  
Specifies the port speed and duplex mode. When the port is a trunk port, the setting for the trunk overwrites the speed and duplex mode. The default setting is `autonegotiate`.

Here are guidelines for port speed settings:

- The speed for 100M SFP ports must be set to `100mfull`.
- SFP ports must be set to `1000mfull` except the SFP ports of the GS908M V2 switch, which have the `autonegotiate` and `1000mfull` options.
- The combo port of the GS916M V2 and GS924M V2 switches has the `autonegotiate` and `1000mfull` options.
- The `1000mfull` option is available only for combo ports.
- Combo ports cannot be set to the `1000mfull` and `fiberauto` options at the same time.
- SFP ports of the GS908M V2-4PS switch have the `autonegotiate`, `100mfull`, and `100mful` options.
- The port speed cannot to be set to `1000mfull` when the `combo` parameter is set to the `fiberauto` option.
- When 1000BASE-T ports are set to `1000mfull`, the Auto-negotiation is enabled.

`securitymode`  
Specifies the security mode.

`automatic`  
Specifies the security mode to automatic. The port disables port security and deletes the dynamic and static entries for the port in FDB. This is the default setting.

`dynamic`  
Specifies the security mode to dynamic. The port discards a packet with the source MAC address that is not in FDB when the number of the dynamic MAC addresses in FDB reaches the maximum number specified by the `learn` parameter.

**limited**

Specifies the security mode to limited. The port takes an action to a packet with the source MAC address that is not in FDB when the number of the dynamic MAC addresses in FDB reaches the maximum number specified by the learn parameter. The action is specified by the intrusionaction parameter.

**secured**

Specifies the security mode to secured. The port stops learning MAC addresses dynamically and changed the dynamic MAC addresses to static MAC addresses. The port takes the action specified by the intrusionaction parameter when receiving packets with the source MAC address that is not in FDB.

Here are guidelines for the security mode setting:

- When the security mode is dynamic, you must set the intrusionaction parameter.
- When the security mode is limited, the intrusionaction parameter is discarded.
- When the security mode is dynamic or limited, you must specify the learn parameter.
- Once the configuration is saved by the CREATE CONFIG command, when the security mode is set to secured, the static entires in FDB are not deleted due to aging or resetting the system. To delete the static entries in FDB, select the security modes other than secured, or execute the DELETE SWITCH FILTER command.
- When the port has static entires in FDB, the port cannot be set to the security mode dynamic. You must delete static entires using the DELETE SWITCH FILTER command.

**learn**

Specifies the learn parameter.

***max\_mac***

Specifies the maximum number of entires in FDB. The range is 0 to 256.

Here are guidelines for specifying the learn parameter:

- When the securitymode parameter is the default setting and the learn parameter is set to 0, the port disables learning dynamic MAC addresses.
- When the securitymode parameter is the default setting and the learn parameter is set to a number other than 0, the securitymode automatically becomes dynamic.

`intrusionaction`

Specifies the action when the port receives a packet with a MAC address that is not in FDB. This action is effective only when the `securitymode` is limited or secured.

`discard`

The port discards a packet with a MAC address that is not in FDB. This is the default setting.

`disable`

The port discards a packet, sends an SNMP trap, and disables the port itself when the MAC address of the packet is not in FDB. To enable the port, set the `securitymode` parameter to automatic to disable port security.

`log`

When the MAC address of a packet is not in FDB, the port discards the packet and issues a level 4 log message including the source MAC address, VID, and port number.

The switch stops logging after 150 log messages per port. The log messages are clear when:

- The `learn` parameter is changed when the `securitymode` is set to limited.
- The `intrusionaction` parameter is changed.
- The `securitymode` is changed.
- The VLAN membership for the port is changed.

`trap`

The port discards a packet and issues an SNMP trap including the source MAC address, VID, and port number when the MAC address of the packet is not in FDB.

`combo`

Specifies the redundancy to the combo port.

`fiberauto`

Fiber has the higher priority when both fiber and copper ports can be linked to the port.

`copperauto`

Copper has the higher priority when both fiber and copper ports can be linked to the port.

`fiber`

The port can be used as a fiber port only.

**copper**

The port can be used as a copper port only.

Here are guidelines for specifying the combo parameter:

- The combo parameter is not valid for the GS908M V2 and GS908M V2-4PS switches.
- The combo parameter is valid on ports 15 and 16 of the GS916M V2 switch and ports 15, 16, 23, and 24 of the GS924M V2 switch.
- 
- 

**polarity**

Specifies the polarity to mdi or mdix. The polarity is not valid for the SFP ports of the GS908M V2 and GS908M V2-4PS switches and combo ports. The default value is mdix.

**dlclimit**

Enables or disables storm protection for broadcast MAC addresses. By default, the storm protection for broadcast MAC addresses is disabled.

**dflimit**

Enables or disables storm protection for unlearned unicast MAC addresses. By default, the storm protection for unicast MAC addresses is disabled.

**mclimit**

Enables or disables storm protection for multicast MAC addresses. By default, the storm protection for multicast MAC addresses is disabled.

**Description**

Use this command to specify the mirror port, communication mode, receiving frame type, security mode, and combo port.

Here are guidelines for specifying port settings:

- The port that port security is enabled on cannot be a mirror port, the authenticator port for Port-based authentication, or a member of a trunk group.
- Port security and STP cannot be enabled on a port at the same time.
- Port security cannot be enabled on the combo port.
- Polarity cannot be changed on combo ports except when the

combo parameter is set to fiber or copper. When the combo parameter is fiber or copper on a combo port, you can set the speed to 1000mfull. Otherwise, the speed is always autonegotiated on combo ports.

- ❑ When the speed is set to 10mhalf, 10mfull, 100mhalf, or 100mfull, the polarity cannot be automatically set. When the speed is set to autonegotiate, 10mhauto, 10mfauto, 100mhauto, 100mfauto, or 100mfull, the polarity is automatically set.
- ❑ When LDF or receiving rate detection is enabled and the action parameter is bcdiscard on the port, the bclimit, dlflimit, and mclimit parameters cannot be set to on.
- ❑ Multicast MC addresses that is not specified by the ADD SWITCH FILTER command are not protected by storm protection.
- ❑ The reserved multicast MAC addresses, 01-80-c2-00-00-00 to 02-80-c2-00-00-2f, are not protected by storm protection.
- ❑ When the port was disabled by the disable action of the intrusionaction parameter, the port is still disabled after rebooting if the configuration is saved before rebooting. To enable the port, run the enable switch port command.
- ❑ 100M SFP ports cannot be a trunk member.

### Confirmation Command

“SHOW SWITCH PORT” on page 272

### Example

The following command sets port 1 to 100M speed and half duplex mode:

```
Manager > set switch port=1 speed=100mhalf
```

## SET SWITCH STORMDETECTION

---

### Syntax

```
set switch stormdetection port[=port_list|all]
[lowrateaction=portdisable|linkdown|bcdiscard|none]
[highrateaction=portdisable|linkdown|bcdiscard|none]
[lowratethreshold=rate] [highratethreshold=rate]
[blocktimeout=timeout|none]
[frametype=broadcast|multicast|all]
[framesize=framesize|auto]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### lowrateaction

Specifies an action when the port detects the loop. The port stops the action after the time specified by the blocktimeout parameter has passed.

#### portdisable

The port is disabled when the loop is detected. This is the default setting.

#### linkdown

Specifies that the port is disconnected when the loop is detected.

#### bcdiscard

Specifies that the port stops receiving broadcast frames when the loop is detected.

#### none

Specifies that the port takes no action. However, the switch issues log messages.

#### *interval*

Specifies the interval of sending a Loop Detection Frame (LDF) in seconds. The default setting is 120 seconds.

#### secure

Specifies an action when the port receives an LDF.

- on**  
Specifies that the port discards the LDF if the ID code in the LDF is different from the valid ID code. The ID code is valid during the specified interval. This is the default setting.
- off**  
Specifies that the port does not check the ID code in the LDF.
- blocktimeout**  
Specifies duration in seconds when the port takes the action specified by the `lowrateaction` or `highrateaction` parameter.
- timeout**  
Specifies time in seconds. The default value is 300 seconds.
- none**  
Specifies that the port does not stop taking the action specified by the action parameter.

### Description

Use this command to specify the actions of Loop Detection.

Here are guidelines for Loop Detection:

- Allied Telesis recommends the linkdown option for trunk ports.
- You cannot specify the `bcdiscard` option on the ports that the Packet Storm Protection is enabled.
- Allied Telesis recommends 1 second or longer for the interval and 60 seconds or longer for the `blocktimeout` parameter when the linkdown option is specified.
- To cancel the action that the port took when the loop is detected:
  - Execute the `ENABLE SWITCH PORT` command.
  - Execute the `DISABLE SWITCH PORT` command
  - Disconnect the port.
  - Modify the power saving mode to `portoff`.

### Confirmation Command

“`SHOW SWITCH STORMDETECTION`” on page 276

### Example

The following command sets port 2 to send an LDF every 60 seconds and to be disconnected for 3600 seconds when the loop is detected:



```
Manager > set switch loopdetection port=2 action=linkdown  
interval=60 blocktimeout=3600
```

## SET SWITCH TRUNK

---

### Syntax

```
set switch trunk=trunk_name speed=1000m|100m|10m
```

### Parameters

*trunk\_name*

Specifies a trunk name.

speed

Specifies port speed.

1000m

The port is set to 1000M speed, the full duplex, and Auto-negotiation. Combo ports must be set to 1000m. This is the default setting.

100m

The port is set to 100M speed, the full duplex, and Auto-negotiation.

10m

The port is set to 10M speed, the full duplex, and Auto-negotiation.

### Description

Use this command to change the trunk settings.

### Confirmation Command

“SHOW SWITCH TRUNK” on page 278

### Example

The following command changes the trunk name to uplink and the speed to 1000m:

```
Manager > set switch trunk=uplink speed=1000m
```

## SHOW SWITCH

---

### Syntax

```
show switch
```

### Parameters

None

### Description

Use this command to display information about the switch settings. An example of the command output is shown in Figure 35.

```

Switch Configuration
-----
Switch Address ..... 00-09-16-00-00-02
Ageingtimer ..... On
Number of Fixed Ports ..... 16
Mirroring ..... Disabled
Mirror port ..... None
Ports mirroring on Rx ..... None
Ports mirroring on Tx ..... None
Ports mirroring on Both ... None
BPDU Forwarding ..... Disabled
EAP Forwarding ..... Disabled
Powersaving ..... Disabled
Ageingtime ..... 300
UpTime ..... 00:34:57
-----

```

Figure 35. SHOW SWITCH Command

### Example

The following example displays information about the switch:

```
Manager > show switch
```

## SHOW SWITCH COUNTER

---

### Syntax

```
show switch counter
```

### Parameters

None

### Description

Use this command to display statistics on the switch. An example of the command output is shown in Figure 36.

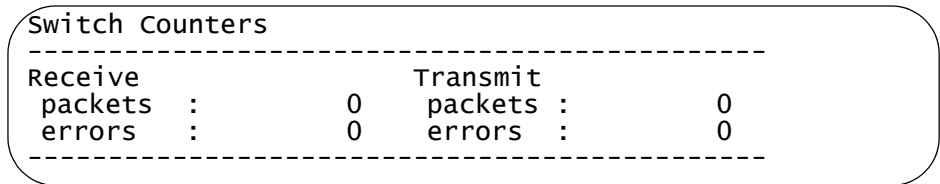


Figure 36. SHOW SWITCH COUNTER Command

### Example

The following example displays statistics on the switch:

```
Manager > show switch counter
```

## SHOW SWITCH LOOPDETECTION

---

### Syntax

```
show switch loopdetection [port=port_list|all]  
[config|status|counter]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### config

Displays the configurations of Loop Detection.

#### status

Displays the status of Loop Detection.

#### counter

Displays the counters of Loop Detection.

### Description

Use this command to display information about Loop Detection. An example of the command output is shown in Figure 37 on page 270.

```

Switch Loop Detection configuration
-----
Port ..... 1
Status ..... Disabled
Frame Action ..... PortDisable
Frame Interval ..... 120 sec
Secure Frame ..... On
Blocking Timeout ..... 300 sec

Port ..... 2
Status ..... Enabled
Frame Action ..... Linkdown
Frame Interval ..... 1 (sec)
Secure Frame ..... Off
Blocking Timeout ..... 3600 (sec)

Switch Loop Detection Status
-----
Port Loop      Expiry Port Status      Link Status      B/C Status
-----
1   Blocking 115   Disabled(Act)    Up                Discard
2   Normal  --    Disabled(User)  Up                Forward
3   Detected 32    Enabled         Up                Forward
4   Blocking 192   Disabled(Act)   Down(Act)         Forward
5   --        --    Enabled         Down              Forward
6   --        --    Enabled         Down              Forward
7   --        --    Disabled(User)  Down(User)        Forward
8   --        --    Enabled         Down              Forward

Switch Loop Detection Counter
-----
Port Frame Tx      Frame Rx      Action      Frame Rx Discards
-----
1   0                0             0           0
2   67295            1             1           0
3   0                0             0           0
4   0                0             0           0
5   0                0             0           0
6   0                0             0           0
7   0                0             0           0
8   0                0             0           0

```

Figure 37. SHOW SWITCH LOOPDETECTION Command

**Example**

The following example displays Loop Detection information on port 1 and 2:

```
Manager > show switch loopdetection port=1,2
```

## SHOW SWITCH MIRROR

---

### Syntax

```
show switch mirror
```

### Parameters

None

### Description

Use this command to display the settings of mirroring. An example of the command output is shown in Figure 38.

```
Port Mirroring Information
-----
Mirror Port ..... 1
Status ..... Disabled
Port Mirroring on Rx ..... None
Port Mirroring on Tx ..... None
Port Mirroring on Both .... None
-----
```

Figure 38. SHOW SWITCH MIRROR Command

### Example

The following example displays the settings of mirroring:

```
Manager > show switch mirror
```

## SHOW SWITCH PORT

---

### Syntax

```
show switch port[=port_list|all] [summary|security]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

summary

Displays the summary of port settings.

security

Displays security settings on ports.

### Description

Use this command to display port settings and security settings. An example of the command output is shown in Figure 39 on page 273.



```

Manager > show switch port=1

Switch Port Information
-----
Port ..... 1
Description ..... -
Status ..... Enabled
Link State ..... Down
UpTime ..... -
Port Media Type ..... Ethernet CSMA/CD
Port Type ..... 10/100/1000Base-T
Configured speed/duplex ..... Autonegotiate
Actual speed/duplex ..... -
MDI Configuration (Polarity) .. Automatic (-)
Acceptable Frame Types ..... Acceptable All Frames
Broadcast rate limit ..... -
Multicast rate limit ..... -
DLF rate limit ..... -
Security Mode ..... Automatic
Learn Limit ..... -
Intrusion Action ..... Discard
Mirroring ..... None
Is this port mirror port ..... No
Enabled flow control(s) ..... -
Send tagged pkts for VLAN(s)... -
Port-based VLAN ..... vlan2(2)
Ingress Filtering ..... Off
Trunk Group ..... -
Port Priority ..... 0
STP ..... default
-----

Manager > show switch port=all security

Port                Security Mode   Learn Learned Locked IntrusionAction
-----
1:                  Secured        -      -      ON      Log
2:                  Secured        -      -      ON      Discard
3:                  Secured        -      -      ON      Disable
4:                  Dynamic Limited 10     0     OFF     Discard
5:                  Limited        2      2     ON      Trap
6:                  Secured        -      -      ON      Discard
7:                  Automatic      -      -      OFF     Discard
8:                  Automatic      -      -      OFF     Discard
9:                  Automatic      -      -      OFF     Discard
-----

```

Figure 39. SHOW SWITCH PORT Command

**Example**

The following example displays the detailed port settings on port 1:

```
Manager > show switch port=1
```

## SHOW SWITCH PORT COUNTER

### Syntax

```
show switch port[=port_list|all] counter
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to display statistics counters on ports. An example of the command output is shown in Figure 40.

```
Switch Port Counters
-----
Port 1. Counters:
Combined receive/transmit packets counters:
 64          :          1757    1024-1518  :          0
 65-127      :          314    1519-1522(T) :          0
 128-255     :          485    1519-2047     :          0
 256-511     :          113    2048-4095     :          0
 512-1023    :           0    4096-9216     :    2503749

General Counters:
Receive
Octets      :    21341360956
UnicastPkts :          1
MulticastPkts:         12
BroadcastPkts:        2656
Discards    :    2506241
Errors      :    13839360
PauseFrames :           0

Transmit
Octets      :          0
UnicastPkts :          0
MulticastPkts:          0
BroadcastPkts:          0
Discards    :          0
Errors      :          0
PauseFrames :          0

AlignmentErrors :          0
FCSErrors       :          0
LateCollisions  :          0
ExcessiveCollisions :          0
CarrierSenseErrors :          0
FrameTooLongs  :          0
SymbolErrors    :          0
UndersizePkts   :    13839360
Fragments       :          0
Jabbers         :          0
SingleCollisionFrames :          0
MultipleCollisionFrames :          0
DeferredTransmissions :          0
```

Figure 40. SHOW SWITCH PORT COUNTER Command

**Example**

The following example displays statics counters on port 1:

```
Manager > show switch port=1 counter
```

## SHOW SWITCH STORMDETECTION

---

### Syntax

```
show switch loopdetection [port=port_list|all]  
[config|status|counter]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

config

Displays the configurations of Storm Detection.

status

Displays the status of Storm Detection.

counter

Displays the counters of Storm Detection.

### Description

Use this command to display information about Storm Detection. An example of the command output is shown in Figure 41 on page 277.

```

Switch Storm Detection configuration
-----
Port ..... 1
Status ..... Disabled
High Rate Action ..... PortDisable
Low Rate Action ..... None
High Rate Threshold ..... 81940 Kbps
Low Rate Threshold ..... 51200 Kbps
Blocking Timeout ..... 300 sec
Frame Type ..... ALL
Frame Size ..... AUTO

Switch Storm Detection Status
-----
Port Threshold Storm Expiry Port Status Link Status B/C Status
-----
1 High Blocking 115 Disabled(Act) Up Discard
  Low Blocking 115
2 High Normal -- Disabled(User) Up Forward
  Low Blocking 115
3 High Detected 32 Enabled Up Forward
  Low Detected 32
4 -- -- -- Disabled(Act) Down(Act) Forward
5 -- -- -- Enabled Down Forward
6 -- -- -- Enabled Down Forward
7 -- -- -- Disabled(User) Down(User) Forward
8 -- -- -- Enabled Down Forward

Switch Storm Detection Counter
-----
Port Detected(High) Action(High) Detected(Low) Action(Low) RxRate(Kbps)
-----
1 1 1 1 0 1000230
2 0 0 1 1 0
3 0 0 0 0 0
4 0 0 0 0 0
5 0 0 0 0 0
6 0 0 0 0 0
7 0 0 0 0 0
8 0 0 0 0 0

```

Figure 41. SHOW SWITCH STORMDETECTION Command

**Example**

The following example displays Storm Detection information on port 1:

```
Manager > show switch stormdetection port=1
```

## SHOW SWITCH TRUNK

---

### Syntax

```
show switch trunk=trunk
```

### Parameters

*trunk*

Specifies a trunk group to display its information.

### Description

Use this command to display information about trunk groups. An example of the command output is shown in Figure 42.

```
Switch Trunk Group
-----
Trunk group name ... uplink
Speed ..... 1000 Mbps
Ports ..... 1-8
-----
```

Figure 42. SHOW SWITCH TRUNK Command

### Example

The following example displays information about trunk groups:

```
Manager > show switch trunk
```

## Chapter 15

# Ethernet Protected Switched Ring (EPSR) Commands

---

The EPSR commands are summarized in Table 32.

Table 32. EPSR Commands

Command	Description
“ADD EPSR DATAVLAN” on page 280	Adds a data VLAN to the EPSR domain.
“CREATE EPSR” on page 281	Create an EPSR domain.
“DELETE EPSR DATAVLAN” on page 283	Removes a data VLAN from the EPSR domain.
“DESTROY EPSR” on page 284	Deletes an EPSR domain.
“DISABLE EPSR” on page 285	Disables an EPSR domain.
“ENABLE EPSR” on page 286	Enables an EPSR domain.
“PURGE EPSR” on page 287	Initializes EPSR and deletes all EPSR domains on the switch.
“SHOW EPSR” on page 288	Displays information about EPSR domains on the switch.
“SHOW EPSR COUNTER” on page 289	Displays statistics counters for the EPSR domain.

## ADD EPSR DATA VLAN

---

### Syntax

```
add epsr=epsr_name datavlan=[vlan_name|vlan_id]
```

### Parameters

*epsr\_name*

Specifies an EPSR domain.

*datavlan*

Specifies a data VLAN with a VLAN name or VLAN ID.

### Description

Use this command to add a data VLAN to the Ethernet Protected Switched Ring (EPSR) domain. Data VLANs carry data traffic that EPSR protects from looping.

Here are guidelines for data VLAN:

- ❑ One EPSR domain can have up to 255 data VLANs.
- ❑ A data VLAN to an EPSR domain can be added as a data VLAN to another EPSR domain if the EPSR domains are not connected to the same ports.
- ❑ A control VLAN that is assigned to an EPSR domain cannot be added as a data VLAN.
- ❑ A VLAN associated to an MST instance of Multiple Spanning Tree Protocol (MSTP) cannot be added as a data VLAN.

### Confirmation Command

“SHOW EPSR” on page 288

### Example

The following command adds VLAN 50 to the EPSR domain “epsr1:”

```
Manager > add epsr=epsr1 datavlan=50
```



## CREATE EPSR

---

### Syntax

```
create epsr=epsr_name mode=aware|transit
controlvlan=vlan_name|vlan_id [deletemcast]
```

### Parameters

*epsr\_name*

Specifies an Ethernet Protected Switched Ring (EPSR) domain name.

aware

Specifies the role of the EPSR domain to the aware mode, which the switch is a transit node with the aware function. See Table 33 on page 282.

transit

Specifies the role of the EPSR domain to the transit mode, which the switch is a transit node with the full function. See Table 33 on page 282.

controlvlan

Specifies a tagged VLAN that handles control messages for the EPSR domain. Specifies a VLAN with a VLAN name or VLAN ID.

Here are guidelines for control VLAN:

- The control VLAN must have two member ports. Ports belong to the same trunk group are considered as one port.
- The control VLAN cannot be a data VLAN or control VLAN for another EPSR domain.
- A port on which STP, port security, or Port-based authentication is enabled cannot be a member port of a control VLAN.

deletemcast

When the deletemcast keyword is specified, the switch deletes the multicast addresses for IGMP Snooping and MLD Snooping from the FDB. Static MLD multicast addresses are not deleted.

### Description

Use this command to create an Ethernet Protected Switched Ring (EPSR) domain. You can create up to 8 EPSR domains per switch. EPSR protects loops in Layer 2 and recovers switching in a ring topology. The master node polls by sending health check messages to transit nodes; the transit

nodes send linkdown notices. The switch is able to function as a transit node.

The functions as a transit node are described in Table 33.

Table 33. Aware and Transit Modes

Function	Aware mode	Transit mode
Displaying the status of the EPSR domain	Yes	Yes
Clearing the FDB and APR table when requested by the master node	Yes	Yes
Generating port link down notice	Yes	Yes
Recovering from double failure	Yes	Yes
Blocking the recovery port in the forwarding state	No	Yes
Sending traps	No	Yes
Logging	Yes	Yes

### Confirmation Command

“SHOW EPSR” on page 288

### Example

The following command creates the EPSR domain “epsr1” that the switch functions in the aware mode and uses VLAN 10 as a control VLAN:

```
Manager > create epsr=epsr1 mode=aware controlvlan=10
```

## DELETE EPSR DATAVLAN

---

### Syntax

```
delete epsr=epsr_name datavlan=[vlan_name|vlan_id|all]
```

### Parameters

*epsr\_name*

Specifies an Ethernet Protected Switched Ring (EPSR) domain.

*datavlan*

Specifies a data VLAN with a VLAN name or VLAN ID. With the keyword all, all data VLANs are specified.

### Description

Use this command to remove a data VLAN from the specified EPSR domain.

### Confirmation Command

“SHOW EPSR” on page 288

### Example

The following command deletes VLAN 50 from the EPSR domain “epsr1:”

```
Manager > delete epsr=epsr1 datavlan=50
```

## DESTROY EPSR

---

### Syntax

```
destroy epsr=epsr_name|all
```

### Parameters

*epsr\_name*

Specifies an EPSR domain.

all

Specifies all EPSR domains.

### Description

Use this command to delete EPSR domains on the switch.

### Confirmation Command

“SHOW EPSR” on page 288

### Example

The following command deletes all EPSR domains on the switch:

```
Manager > destroy epsr=all
```

## DISABLE EPSR

---

### Syntax

```
disable epsr=epsr_name|all
```

### Parameters

*epsr\_name*

Specifies an EPSR domain.

all

Specifies all EPSR domains.

### Description

Use this command to disable an EPSR domain.

---

#### Note

Before executing this command, you must disable the port for the ring either by running the DISABLE SWITCH PORT command or unplugging the cable.

---

### Confirmation Command

“SHOW EPSR” on page 288

### Example

The following command disables the EPSR domain “espr1:”

```
Manager > disable epsr=espr1
```

## ENABLE EPSR

---

### Syntax

```
enable epsr=epsr_name|all
```

### Parameters

*epsr\_name*

Specifies an EPSR domain.

all

Specifies all EPSR domains.

### Description

Use this command to enable an EPSR domain.

### Confirmation Command

“SHOW EPSR” on page 288

### Example

The following command enables all EPSR domains on the switch:

```
Manager > enable epsr=all
```

## PURGE EPSR

---

### Syntax

```
purge epsr
```

### Parameters

None

### Description

Use this command to initialize EPSR and delete all EPSR domains.

### Confirmation Command

“SHOW EPSR” on page 288

### Example

The following command initializes EPSR and deletes all EPSR domains:

```
Manager > purge epsr
```

## SHOW EPSR

---

### Syntax

```
show epsr[=epsr_name|all]
```

### Parameters

*epsr\_name*

Specifies an EPSR domain.

all

Specifies all EPSR domains.

### Description

Use this command to display information about the EPSR domain. An example of the command output is shown in Figure 43.

```

-----
EPSR Information
-----
Name ..... blue
Mode ..... AWARE
Status ..... Enabled
State ..... Links-Up
Delete Multicast Entry ..... Disabled
Control Vlan ..... control (2)
Data VLAN(s) ..... data (100)
First Port ..... 1
First Port Status ..... Up
First Port Direction ..... Downstream
Second Port ..... 2
Second Port Status ..... Up
Second Port Direction ..... Upstream
Master Node ..... 00-00-cd-24-03-4e
-----

```

Figure 43. SHOW EPSR Command

### Example

The following example displays information about the EPSR domains on the switch:

```
Manager > show epsr
```



## SHOW EPSR COUNTER

### Syntax

```
show epsr[=epsr_name|all] counter
```

### Parameters

*epsr\_name*

Specifies an EPSR domain.

all

Specifies all EPSR domains.

### Description

Use this command to display statistics counters for the EPSR domain. An example of the command output is shown in Figure 44.

```

-----
EPSR Counters
-----
Name: domain_two
Receive:
Total EPSR Packets      4674
Health                  4671
Ring Up                  2
Ring Down                0
Link Down                1
Invalid EPSR Packets    0
Transmit:
Total EPSR Packets 2
Health                  0
Ring Up                 2
Ring Down               0
Link Down               0

Name: domain_one
Receive:
Total EPSR Packets      1609
Health                  1603
Ring Up                  3
Ring Down                3
Link Down                0
Invalid EPSR Packets    0
Transmit:
Total EPSR Packets 3
Health                  0
Ring Up                 0
Ring Down               0
Link Down               3
-----

```

Figure 44. SHOW EPSR COUNTER Command

### Example

The following example displays statistics counters for the the EPSR domains:

```
Manager > show epsr=all counter
```



## Chapter 16

# Forwarding Database (FDB) Commands

The FDB commands are summarized in Table 34.

Table 34. FDB Commands

Command	Description
“ADD SWITCH FILTER” on page 292	Adds a static entry to the FDB.
“DELETE SWITCH FILTER” on page 294	Deletes a static entry from the FDB.
“DISABLE SWITCH AGEINGTIMER” on page 295	Disables the FDB aging timer.
“ENABLE SWITCH AGEINGTIMER” on page 296	Enables the FDB aging timer.
“RESET SWITCH FDB” on page 297	Deletes all dynamic entries from the FDB.
“SET SWITCH AGEINGTIMER” on page 298	Changes the FDB aging timer.
“SHOW SWITCH FDB” on page 299	Displays the entries of the FDB.
“SHOW SWITCH FILTER” on page 301	Displays the static entries for the FDB.

## ADD SWITCH FILTER

---

### Syntax

```
add switch filter destaddress=unicast_mac_add  
port=port_number [vlan=vlan_name|vid]
```

```
add switch filter destaddress=multicast_mac_add  
vlan=vlan_name|vid
```

### Parameters

*destaddress*

Specifies the a data VLAN with a VLAN name or VLAN ID.

*unicast\_mac\_add*

Specifies a unicast MAC address in the format: *ff-ff-ff-ff-ff-ff*. The first octet of a unicast MAC address is an even number.

*multicast\_mac\_add*

Specifies a multicast MAC address in the format: *ff-ff-ff-ff-ff-ff*. The first octet of a multicast MAC address is an odd number.

*port\_number*

Specifies the port number.

*vlan*

Specifies a tagged VLAN that the port belongs to. Do not specify this parameter if the port is only a member of untagged VLAN. You must specify this parameter when adding a multicast MAC address.

### Description

Use this command to add a static entry to the Forwarding Database (FDB). FDB is a database to store MAC addresses that the switch uses to determine a port to forward frames.

You can add up to 2048 static entries to the Forwarding Database.

### Confirmation Command

“SHOW SWITCH FDB” on page 299

**Example**

The following command adds a static entry of the MAC address 00-00-f4-12-34-56 to FDB:

```
Manager > add switch filter destaddress=00-00-f4-12-34-56  
port=1
```

## DELETE SWITCH FILTER

---

### Syntax

```
delete switch filter port=port_number
[destaddress=unicast_mac_add] [vlan=vlan_name|vid]
```

```
delete switch filter destaddress=multicast_mac_add
vlan=vlan_name|vid
```

### Parameters

*destaddress*

Specifies the a data VLAN with a VLAN name or VLAN ID.

*unicast\_mac\_add*

Specifies a unicast MAC address in the format: *ff-ff-ff-ff-ff-ff*. The first octet of a unicast MAC address is an even number.

*multicast\_mac\_add*

Specifies a multicast MAC address in the format: *ff-ff-ff-ff-ff-ff*. The first octet of a multicast MAC address is an odd number.

*port\_number*

Specifies the number of port.

*vlan*

Specifies a tagged VLAN that the port belongs to. Do not specify this parameter if the port is only a member of untagged VLAN. You must specify this parameter when adding a multicast MAC address.

### Description

Use this command to delete a static entry from the Forwarding Database (FDB). Confirmation Command

“SHOW SWITCH FDB” on page 299

### Example

The following command deletes a static entry of the MAC address 00-00-f4-12-34-56 from FDB:

```
Manager > delete switch filter port=1 destaddress=00-00-f4-12-34-56
```

## DISABLE SWITCH AGEINGTIMER

---

### Syntax

```
disable switch agingtimer
```

### Parameters

None

### Description

Use this command to disable the FDB aging timer. When the FDB aging timer is disabled, the dynamic entries of FDB are not expired and deleted. By default, the FDB aging timer is enabled.

### Confirmation Command

“SHOW SWITCH FDB” on page 299

### Example

The following command disables the FDB aging timer:

```
Manager > disable switch agingtimer
```

## ENABLE SWITCH AGEINGTIMER

---

### Syntax

```
enable switch agingtimer
```

### Parameters

None

### Description

Use this command to enable the FDB aging timer. When the FDB aging timer is enabled, the dynamic entries of FDB are expired and deleted. By default, the FDB aging timer is enabled.

### Confirmation Command

“SHOW SWITCH FDB” on page 299

### Example

The following command enables the FDB aging timer:

```
Manager > enable switch agingtimer
```



## RESET SWITCH FDB

---

### Syntax

```
reset switch fdb
```

### Parameters

None

### Description

Use this command to delete all of the dynamic entries from FDB. The static entries are not deleted.

### Confirmation Command

“SHOW SWITCH FDB” on page 299

### Example

The following command deletes all dynamic entries from FDB:

```
Manager > reset switch fdb
```

## SET SWITCH AGEINGTIMER

---

### Syntax

```
set switch agingtimer=time
```

### Parameters

*time*

Specifies time in seconds that the dynamic entries in FDB are expired. The range is 1 to 1,000,000 seconds. The default setting is 300 seconds.

### Description

Use this command to change timer for the dynamic entries in FDB to be expired. A dynamic entry is deleted from FDB when any frame with the destination MAC address of the dynamic entry has not been received for the period of the specified time.

### Confirmation Command

“SHOW SWITCH FDB” on page 299

### Example

The following command changes the aging timer to 500 seconds:

```
Manager > set switch agingtimer=500
```

## SHOW SWITCH FDB

---

### Syntax

```
show switch fdb [address=mac_add] [port=port_list|all]
[status=static|dynamic|discard] [vlan=vlan_name|vid]
[trunk=trunk]
```

### Parameters

*mac\_add*

Specifies a unicast MAC address in the format: *ff-ff-ff-ff-ff*.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all switch ports.

status

Specifies the entry type to display information about.

vlan

Specifies a VLAN with either the VLAN name or VLAN ID.

*trunk*

Specifies the name of a trunk group. Displays only entries that belong to the trunk group.

### Description

Use this command to display entries of FDB. An example of the command output is shown in Figure 45.

```
Manager > show switch fdb
```

```
Switch Forwarding Database (Software)
```

VLAN	MAC Address	Status	Port
1	d4-be-d9-6b-16-d5	Dynamic	7

Figure 45. SHOW SWITCH FDB Command

**Example**

The following example displays the entries of FDB:

```
Manager > show switch fdb
```

## SHOW SWITCH FILTER

---

### Syntax

```
show switch filter [port=port_list|all]
[destaddress=mac_add] [vlan=vlan_name|vid]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all switch ports.

#### *mac\_add*

Specifies a destination MAC address in the format: *ff-ff-ff-ff-ff*.

#### vlan

Specifies a VLAN with either the VLAN name or VLAN ID.

### Description

Use this command to display the static entries of FDB. An example of the command output is shown in Figure 46.

Switch Filters					
Entry	VLAN	Destination Address	Port	Action	Source
1	blue (30)	00-00-f4-12-12-13	8	Forward	Static
2	orange (20)	00-00-f4-01-01-01	5	Forward	Static
3	white (10)	00-00-f4-12-12-14	8	Forward	Static

Figure 46. SHOW SWITCH FILTER Command

### Example

The following example displays the static entries of FDB:

```
Manager > show switch filter
```



## Chapter 17

# DHCP Snooping Commands

The DHCP Snooping commands are summarized in Table 35.

Table 35. DHCP Snooping Commands

Command	Description
“ADD DHCP Snooping” on page 305	Adds a static entry to the DHCP Snooping table.
“CREATE DHCP Snooping MACFILTER” on page 306	Creates a MAC address filtering entry.
“DELETE DHCP Snooping” on page 308	Deletes a static entry from the DHCP Snooping table.
“DESTROY DHCP Snooping MACFILTER” on page 309	Deletes MAC address filtering entries.
“DISABLE DHCP Snooping” on page 310	Disables DHCP Snooping on the switch.
“DISABLE DHCP Snooping ARPSECURITY” on page 311	Disables ARP security on the switch.
“DISABLE DHCP Snooping LOG” on page 312	Disables the DHCP Snooping log function on ARP security or MAC filtering.
“DISABLE DHCP Snooping OPTION82” on page 313	Disables the function to handle relay agent option 82.
“ENABLE DHCP Snooping” on page 314	Enables DHCP Snooping on the switch.
“ENABLE DHCP Snooping ARPSECURITY” on page 316	Enables ARP security on the switch.
“ENABLE DHCP Snooping LOG” on page 317	Enables the DHCP Snooping log function on ARP security or MAC filtering.
“ENABLE DHCP Snooping OPTION82” on page 318	Enables handling Relay Agent Information Option 82.
“PURGE DHCP Snooping” on page 319	Disables DHCP Snooping and deletes the settings.
“RESET DHCP Snooping COUNTER” on page 320	Resets the statistics counters for DHCP Snooping.

Table 35. DHCP Snooping Commands (Continued)

Command	Description
"RESET DHCP Snooping DATABASE" on page 321	Deletes dynamic entries for the specified port from the DHCP Snooping table.
"SET DHCP Snooping CHECKINTERVAL" on page 322	Changes an interval to check the DHCP Snooping table.
"SET DHCP Snooping CHECKOPTION" on page 323	Specifies the conditions to delete entries from the DHCP Snooping table.
"SET DHCP Snooping MACFILTER" on page 324	Changes a MAC address filtering entry.
"SET DHCP Snooping PORT" on page 326	Changes port settings for DHCP Snooping.
"SHOW DHCP Snooping" on page 328	Displays information about DHCP Snooping.
"SHOW DHCP Snooping COUNTER" on page 329	Displays statistics information for DHCP Snooping.
"SHOW DHCP Snooping DATABASE" on page 330	Displays the DHCP Snooping table.
"SHOW DHCP Snooping MACFILTER" on page 331	Displays MAC address filters.
"SHOW DHCP Snooping PORT" on page 332	Displays the settings of DHCP Snooping for the specified port.



## ADD DHCPSNOOPING

---

### Syntax

```
add dhcpsnooping binding=mac_address
interface=vlan_interface ip=ip_address port=port_number
```

### Parameters

*mac\_address*

Specifies the MAC address of the client.

*vlan\_interface*

Specifies the VLAN name or VLAN ID that the client belong to.

*ip\_address*

Specifies the IP address of the client.

*port\_number*

Specifies the port number that the client is connected to.

### Description

Use this command to add a static entry to the DHCP Snooping table.

Here are guidelines for DHCP Snooping:

- By default, one port can be only one static entry. To add more than one entry per port, use the SET DHCPSNOOPING PORT command to change the maxlease value.
- A trusted port cannot be a static entry to the DCHP Snooping table.
- An IP address in the DCHP range cannot be added to the DHCP Snooping table.

### Confirmation Command

“SHOW DHCPSNOOPING DATABASE” on page 330

### Example

The following command adds a static entry to the DCHP Snooping table:

```
Manager > add dhcpsnooping binding=00-00-00-00-00-01
intervace=vlan2 ip=192.168.10.5 port=5
```

## CREATE DHCP Snooping MACFILTER

---

### Syntax

```
create dhcp snooping macfilter=entry_id
[address=mac_address|any] [mask=mac_mask]
[vlan=vlan_name|vlan_id|any] [port=port_list|all|none]
[action=deny|permit]
```

### Parameters

*entry\_id*

Specifies the ID of a MAC address filtering entry. The range is 1 to 999.

*mac\_address*

Specifies the MAC address of the device to be filtered.

any

Specifies all MAC addresses. This is the default setting.

*mac\_mask*

Specifies the mask of the MAC address to be filtered.

*vlan\_name*

Specifies a VLAN name.

*vlan\_id*

Specifies a VLAN ID. The range is 1 to 4094.

any

Specifies all VLANs.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

none

Specifies no switch ports.

deny

When matching the filtering criteria, the client is denied.

permit

When matching the filtering criteria, the client is permitted.

**Description**

Use this command to create a MAC address filtering entry.

**Confirmation Command**

“SHOW DHCP Snooping MACFILTER” on page 331

**Example**

The following command creates a MAC address filtering entry:

```
Manager > create dhcp snooping macfilter=1  
address=00-09-41-00-00-00 mask=ff-ff-ff-00-00-00 port=all  
action=permit
```

## DELETE DHCPSNOOPING

---

### Syntax

```
delete dhcp snooping binding=mac_address [ip=ip_address]
```

### Parameters

*mac\_address*

Specifies the MAC address of the client entry.

*ip\_address*

Specifies the IP address of the client entry.

### Description

Use this command to delete a static entry from the DHCP Snooping table.

### Confirmation Command

“SHOW DHCPSNOOPING DATABASE” on page 330

### Example

The following command delete the client entry:

```
Manager > delete dhcp snooping binding=00-00-00-00-00-01  
ip=192.168.10.5
```

## DESTROY DHCP Snooping MACFILTER

---

### Syntax

```
destroy dhcp snooping macfilter=entry_id_list|all
```

### Parameters

*entry\_id\_list*

Specifies a list of client entries. To specify multiple entries, use a comma (,) to separate them. To specify a range of entries, use a hyphen (-).

all

Specifies all client entries.

### Description

Use this command to delete MAC address filtering entries.

### Confirmation Command

“SHOW DHCP Snooping MACFILTER” on page 331

### Example

The following command delete the client entry IDs 2, 3, and 4:

```
Manager > destroy dhcp snooping macfilter=2,3,4
```

## DISABLE DHCPSNOOPING

---

### Syntax

```
disable dhcpsnooping
```

### Parameters

None

### Description

Use this command to disable DHCP Snooping. By default, DHCP Snooping is disabled.

### Confirmation Command

“SHOW DHCPSNOOPING” on page 328

### Example

The following command disables DHCP Snooping:

```
Manager > disable dhcpsnooping
```

## DISABLE DHCPSNOOPING ARPSECURITY

---

### Syntax

```
disable dhcpsnooping arpsecurity
```

### Parameters

None

### Description

Use this command to disable ARP security. By default, ARP security is disabled.

### Confirmation Command

“SHOW DHCPSNOOPING” on page 328

### Example

The following command disables ARP security:

```
Manager > disable dhcpsnooping arpsecurity
```

## DISABLE DHCPSNOOPING LOG

---

### Syntax

```
disable dhcpsnooping log=arpsecurity|macfilter
```

### Parameters

log

Specifies a log event. To specify multiple log events, use a comma to separate them.

arpsecurity

Specifies the ARP security log. Log messages are issued when an ARP packet is discarded because the source address is not in the DHCP Snooping table.

macfilter

Specifies the MAC filter log. Log messages are issued when a DHCP packet is discarded due to MAC filtering.

### Description

Use this command to disable logging for DHCP Snooping. By default, logging for DHCP Snooping is disabled.

### Confirmation Command

“SHOW DHCPSNOOPING” on page 328

### Example

The following command disables ARP security logging:

```
Manager > disable dhcpsnooping log=arpsecurity
```



## DISABLE DHCP Snooping Option 82

---

### Syntax

```
disable dhcp snooping option 82
```

### Parameters

None

### Description

Use this command to disable Relay Agent option 82. By default, Relay Agent option 82 is disabled.

### Confirmation Command

“SHOW DHCP SNOOPING” on page 328

### Example

The following command disables Relay Agent option 82:

```
Manager > disable dhcp snooping option 82
```

## ENABLE DHCPSNOOPING

---

### Syntax

```
enable dhcpsnooping
```

### Parameters

None

### Description

Use this command to enable DHCP Snooping and start snooping DHCP messages between DHCP servers and clients. By default, DHCP Snooping is disabled.

When DHCP Snooping is enabled:

- ❑ When the DHCP server assigns an IP address to a client, the switch adds the client connected to an untrusted port to the DHCP Snooping table.
- ❑ Untrusted ports permit IP packets from the clients listed in the DHCP Snooping table and discard the rest of the packets.

Here are the guidelines for DHCP Snooping:

- ❑ The switch writes client information in NVS into the DHCP Snooping table when starts DHCP Snooping.
- ❑ The switch filters DHCP messages between the DHCP server and DHCP clients connected to the untrusted port.
- ❑ DHCP Snooping and STP cannot be enabled at the same time.
- ❑ DHCP Snooping and Policy-based QoS cannot be enabled at the same time.
- ❑ Untrusted ports cannot be trunk ports, Web authenticated, EPCSR aware, or port security enabled port.
- ❑ One port can have up to 5 DHCP clients.
- ❑ The GS908M V2 switch can have up to 40 DHCP clients.
- ❑ The GS908M V2-4PS switch can have up to 45 DHCP clients.
- ❑ The GS916M V2 switch can have up to 75 DHCP clients.
- ❑ The GS924M V2 switch can have up to 115 DHCP clients.

### Confirmation Command

“SHOW DHCPSNOOPING” on page 328

**Example**

The following command enables DHCP Snooping:

```
Manager > enable dhcpsnooping
```

## ENABLE DHCP Snooping ARPSECURITY

---

### Syntax

```
enable dhcp snooping arpsecurity
```

### Parameters

None

### Description

Use this command to set ARP security enabled. ARP security is enabled when DHCP Snooping is enabled. When ARP security is enabled, the switch forwards ARP packets from DHCP clients and discards the rest. By default, ARP security is disabled.

### Confirmation Command

“SHOW DHCP Snooping” on page 328

### Example

The following command sets ARP security enabled:

```
Manager > enable dhcp snooping arpsecurity
```

## ENABLE DHCP Snooping LOG

---

### Syntax

```
enable dhcp snooping log=arpsecurity|macfilter
```

### Parameters

#### log

Specifies a log event. To specify multiple log events, use a comma to separate them.

#### arpsecurity

Specifies the ARP security log event. A log is issued when an ARP packet is discarded because the source address is not in the DHCP Snooping table.

#### macfilter

Specifies the MAC filter log event. A log is issued when a DHCP packet is discarded due to the MAC filtering.

### Description

Use this command to enable logging for DHCP Snooping. By default, logging for DHCP Snooping is disabled.

### Confirmation Command

“SHOW DHCP SNOOPING” on page 328

### Example

The following command enables ARP security logging for DHCP Snooping:

```
Manager > enable dhcp snooping log=arpsecurity
```

## ENABLE DHCP Snooping Option 82

---

### Syntax

```
enable dhcp snooping option82
```

### Parameters

None

### Description

Use this command to set handling Relay Agent Information Option 82 enabled. Relay Agent Information Option 82 is enabled when DHCP Snooping is enabled. When Relay Agent Information Option 82 is enabled, the switch inserts the Relay Agent Information Option into DHCP and BOOTP packets before forwarding them.

The Relay Agent Information Option 82 includes:

- ❑ Remote-ID: the MAC address of the switch
- ❑ Circuit-ID: the switch port that receives client packets and VLAN ID of the port
- ❑ Subscriber-ID: the value of the subscriberid parameter specified by the SET DHCP Snooping PORT command

Here are the guidelines for Relay Agent Information Option 82:

- ❑ Untrusted ports discard the DHCP and BOOTP packets that include the Relay Agent Information Option.
- ❑ Trusted ports forward the DHCP and BOOTP packets including the Relay Agent Information Option.
- ❑ When Relay Agent Information Option 82 is enabled, the switch deletes the Relay Agent Information Option and forwards packets back from the server to a client if the client is directly connected to an untrusted port.

### Confirmation Command

“SHOW DHCP Snooping” on page 328

### Example

The following command sets Relay Agent Information Option 82 enabled:

```
Manager > enable dhcp snooping option82
```

# PURGE DHCP Snooping

---

## Syntax

```
purge dhcp snooping
```

## Parameters

None

## Description

Use this command to disable DHCP Snooping and delete the settings.

## Confirmation Command

“SHOW DHCP Snooping” on page 328

## Example

The following command disables DHCP Snooping and deletes the settings:

```
Manager > purge dhcp snooping
```

## RESET DHCPSNOOPING COUNTER

---

### Syntax

```
reset dhcpsnooping counter
```

### Parameters

None

### Description

Use this command to reset the statistics counters for DHCP Snooping.

### Confirmation Command

“SHOW DHCPSNOOPING COUNTER” on page 329

### Example

The following command resets the statistics counters for DHCP Snooping:

```
Manager > reset dhcpsnooping counter
```



## RESET DHCP Snooping Database

---

### Syntax

```
reset dhcp snooping database [port=port_list|all]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to delete dynamic entries for the specified port from the DHCP Snooping table.

### Confirmation Command

“SHOW DHCP SNOOPING DATABASE” on page 330

### Example

The following command delete dynamic entries on port 1 and 2 from the DHCP Snooping table:

```
Manager > reset dhcp snooping database port=1-2
```

## SET DHCP Snooping CHECKINTERVAL

---

### Syntax

```
set dhcp snooping checkinterval=time
```

### Parameters

*time*

Specifies time in seconds. The range is 1 to 3600. The default value is 60 seconds.

### Description

Use this command to change the interval to check the DHCP Snooping table. The switch checks dynamic entries at the specified intervals and deletes the dynamic entries that the IP address is expired in.

### Confirmation Command

“SHOW DHCP Snooping” on page 328

### Example

The following command changes the interval to 40 seconds:

```
Manager > reset dhcp snooping checkinterval=40
```

## SET DHCP Snooping Checkoption

---

### Syntax

```
set dhcp snooping checkoption=none|dhcprelease|linkdown
```

### Parameters

#### checkoption

Specifies one or more conditions to delete client entries from the DHCP Snooping table. To specify multiple conditions, use a comma (,) to separate them. The keyword none cannot be specified with other keywords.

#### none

Deletes a client entry when the maxlease exceeds. This is the default setting.

#### dhcprelease

Deletes a client entry when the maxlease exceeds or the DHCP release packet for the client is received.

#### linkdown

Deletes a client entry when the maxlease exceeds or the port connected to the client is disconnected.

### Description

Use this command to specify the conditions to delete entries from the DHCP Snooping table.

### Confirmation Command

“SHOW DHCP Snooping DATABASE” on page 330

### Example

The following command deletes a client entry when the maxlease exceeds and the port connected to a client is disconnected:

```
Manager > reset dhcp snooping checkoption=linkdown
```

## SET DHCP Snooping MACFILTER

---

### Syntax

```
set dhcp snooping macfilter=entry_id
[address=mac_address|any] [mask=mac_mask]
[vlan=vlan_name|vlan_id|any] [port=port_list|all|none]
[action=deny|permit]
```

### Parameters

*entry\_id*

Specifies the ID of a MAC address filtering entry.

*mac\_address*

Specifies the MAC address of the device to be filtered.

any

Specifies all MAC addresses. This is the default setting.

*mac\_mask*

Specifies the mask of the MAC address to be filtered.

*vlan\_name*

Specifies a VLAN name.

*vlan\_id*

Specifies a VLAN ID. The range is 1 to 4094.

any

Specifies all VLANs.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

none

Specifies no switch ports.

deny

When matching the filtering criteria, the client is denied.

permit

When matching the filtering criteria, the client is permitted.

**Description**

Use this command to change a MAC address filtering entry.

**Confirmation Command**

“SHOW DHCP Snooping MACFILTER” on page 331

**Example**

The following command changes the MAC address filtering entry:

```
Manager > set dhcp snooping macfilter=2  
address=00-44-56-77-88-00 mask=ff-ff-ff-ff-ff-ff
```

## SET DHCP Snooping PORT

---

### Syntax

```
set dhcp snooping port=port_list|all
[trusted=yes|no|on|off|true|false] [max lease=lease]
[subscriber id=subscriber_id|none]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### trusted

Specifies the port is either a trusted port or untrusted port.

#### yes, on, true

The port is a trusted port. This is the default setting.

#### no, off, false

The port is an untrusted port.

#### *lease*

Specifies the maximum number of clients to permit IP packets through the port. This number includes the number of both dynamic and static DHCP clients. The range is 0 to 5. When 0 is specified, any IP packets through the port is denied. The default value is 1.

#### *subscriber*

Specifies the subscriber ID using up to 50 alphanumeric characters. Use quotes (") when including a space. When DHCP Snooping option 82 is enabled, the subscriber ID is included in the relay agent information option.

#### none

The subscriber ID is not included in the relay agent information option.

### Description

Use this command to change port settings for DHCP Snooping.

**Confirmation Command**

“SHOW DHCP Snooping PORT” on page 332

**Example**

The following command changes the settings on port 4 for DHCP Snooping:

```
Manager > set dhcpsnooping port=4 trusted=true
```

## SHOW DHCPSNOOPING

---

### Syntax

```
show dhcpsnooping
```

### Parameters

None

### Description

Use this command to display information about DHCP Snooping. An example of the command output is shown in Figure 47.

```
-----  
DHCP Snooping Information  
-----  
DHCP Snooping ..... Enabled  
Option 82 status ..... Enabled  
ARP security ..... Enabled  
Logging enabled ..... None  
  
DHCP Snooping Database:  
Full Leases/Max Leases ... 2/260  
Check Interval ..... 60 seconds  
Check Options ..... None  
-----
```

Figure 47. SHOW DHCPSNOOPING Command

### Example

The following example displays information for DHCP Snooping:

```
Manager > show dhcpsnooping
```



## SHOW DHCP Snooping Counter

---

### Syntax

```
show dhcp snooping counter
```

### Parameters

None

### Description

Use this command to display statistics information for DHCP Snooping. An example of the command output is shown in Figure 48.

```

DHCP Snooping Counters
-----
DHCP Snooping
  InPackets ..... 16
  InBootpRequests ..... 14
  InBootpReplies ..... 2
  InDiscards ..... 0

ARP Security
  InPackets ..... 6
  InDiscards ..... 3
  NoLease ..... 3
  Invalid ..... 0
  
```

Figure 48. SHOW DHCP SNOOPING COUNTER Command

### Example

The following example displays statistics for DHCP Snooping:

```
Manager > show dhcp snooping counter
```

## SHOW DHCP Snooping DATABASE

### Syntax

```
show dhcpsnooping database
```

### Parameters

None

### Description

Use this command to display the DHCP Snooping table. An example of the command output is shown in Figure 49.

```

DHCP Snooping Binding Database
-----
Full Leases/Max Leases ... 2/24
Check Interval ..... 60 seconds
Check Options ..... None

Current valid entries
MAC Address          IP Address          Expires(s)  VLAN  Port  ID  Source
-----
00-00-00-00-00-01   192.168.10.5       Static      1     5     4   User
00-0a-79-34-06-12   192.168.10.200    2231       1     11    1   Dynamic
-----

Entries with client lease but no listeners
MAC Address          IP Address          Expires(s)  VLAN  Port  ID  Source
-----
None...

Entries with no client lease and no listeners
MAC Address          IP Address          Expires(s)  VLAN  Port  ID  Source
-----
None...

```

Figure 49. SHOW DHCP Snooping DATABASE Command

### Example

The following example displays the DHCP Snooping table:

```
Manager > show dhcpsnooping database
```

## SHOW DHCP Snooping MACFILTER

---

### Syntax

```
show dhcp snooping macfilter[=entry_id|all]
[port=port_list|all]
```

### Parameters

*entry\_id*

Specifies the ID of a MAC address filtering entry.

all

Specifies all the switch ports.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to display MAC address filters. An example of the command output is shown in Figure 50.

```

DHCP Snooping MAC Filter ( 1 entry )
-----
Filter ID ..... 1
VLAN ID ..... 1
Port ..... ALL
Action ..... Permit
Is Active ..... No
-----

```

Figure 50. SHOW DHCP Snooping MACFILTER Command

### Example

The following example displays MAC address filters:

```
Manager > show dhcp snooping macfilter
```

## SHOW DHCPSNOOPING PORT

---

### Syntax

```
show dhcpsnooping port[=port_list|all]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to display the settings of DHCP Snooping for the specified port. An example of the command output is shown in Figure 51.

```

DHCP Snooping Port Information:
-----
Port ..... 11
Trusted ..... No
Full Leases/Max Leases ... 1/1
Subscriber-ID ..... None
-----

```

Figure 51. SHOW DHCPSNOOPING PORT Command

### Example

The following example displays the settings of DHCP Snooping on port 1:

```
Manager > show dhcpsnooping port=1
```

## Chapter 18

# Power Over Ethernet (PoE) Commands

The PoE commands are summarized in Table 36.

Table 36. PoE Commands

Command	Description
“DISABLE POE PORT” on page 334	Disables Power of Ethernet (PoE) on ports.
“ENABLE POE PORT” on page 335	Enables PoE on ports.
“SET POE DETECT” on page 336	Detects IEEE compliant and legacy PDs.
“SET POE GUARDBAND” on page 337	Specifies guard power in watts.
“SET POE MANAGEMENT” on page 338	Specifies the power management mode to the switch.
“SET POE PORT” on page 339	Specifies the power supply priority and power limit on the ports.
“SET POE THRESHOLD” on page 341	Specifies the threshold that the switch supplies to the connected PDs.
“SHOW POE” on page 342	Displays information about PoE settings and ports.
“SHOW POE PORT” on page 343	Displays information about PoE ports.

## DISABLE POE PORT

---

### Syntax

```
disable poe port[=port_list|all]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to disable Power of Ethernet (PoE) on the specified ports. By default, PoE is enabled on all ports.

---

#### Note

The PoE commands are available only for the GS908M V2-4PS switch.

---

### Confirmation Command

“SHOW POE” on page 342

### Example

The following command disables PoE on port 1 to port 3:

```
Manager > disable poe port=1-3
```

## ENABLE POE PORT

---

### Syntax

```
enable poe port[=port_list|all]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to enable Power of Ethernet (PoE) on the specified ports. By default, PoE is enabled on all ports.

---

#### Note

The PoE commands are available only for the GS908M V2-4PS switch.

---

### Confirmation Command

“SHOW POE” on page 342

### Example

The following command enables PoE on port 1 to port 2:

```
Manager > enable poe port=1-2
```

## SET POE DETECT

---

### Syntax

```
set poe detect[=ieee|legacy]
```

### Parameters

ieee

Detects IEEE compliant PDs. This is the default setting.

legacy

Detects IEEE compliant PDs and legacy PDs.

### Description

Use this command to specify the detect method of powered devices (PDs).

---

#### Note

The PoE commands are available only for the GS908M V2-4PS switch.

---

### Confirmation Command

“SHOW POE” on page 342

### Example

The following command specifies IEEE compliant PDs:

```
Manager > set poe detect=ieee
```



## SET POE GUARDBAND

---

### Syntax

```
set poe guardband=guard_band
```

### Parameters

*guard\_band*

Specifies the guard band in watts. The range is 2 to 70 watts. The default setting is 10 watts.

### Description

Use this command to specify guard power in watts. The switch does not supply power to a PD that is newly connected to the port when the switch is supplying power to the other PDs exceeding the power threshold. The power threshold is the maximum power 75 watts minus the specified guard band. For example, when the guard band is 25 watts, the switch does not supply power to a new PD if the switch is supplying power to other PDs exceeding 50 (75 minus 25) watts.

---

#### Note

The PoE commands are available only for the GS908M V2-4PS switch.

---

### Confirmation Command

“SHOW POE” on page 342

### Example

The following command specifies 25 watts to the guard band:

```
Manager > set poe guardband=25
```

## SET POE MANAGEMENT

---

### Syntax

```
set poe management[=class|actual]
```

### Parameters

`class`

Specifies the class power management mode. The switch assigns power to ports based on the class of the PD connected to the port.

`actual`

Specifies the actual power management mode. The switch assigns power to ports based on power usage of the PD connected to the port.

### Description

Use this command to specify the power management mode to the switch.

---

#### Note

The PoE commands are available only for the GS908M V2-4PS switch.

---

### Confirmation Command

“SHOW POE” on page 342

### Example

The following command specifies the switch to assign power to ports based on the class of the PD connected to the port:

```
Manager > set poe management=class
```

## SET POE PORT

---

### Syntax

```
set poe port[=port_list|all] [priority=low|high|critical]
[powerlimit=power_limit]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### priority

Specifies the power supply priority to the port. The options are low, high, and critical. The critical is the highest priority. The default setting is low. When ports have the same priority, the port with the smaller port number has a higher priority.

#### *power\_limit*

Specifies the power limit in mili-watts. The default setting is 30000 mili-watts. The switch does not supply power to a PD that consumes more than the power limit.

### Description

Use this command to specify the power supply priority and power limit on the ports.

---

#### Note

The PoE commands are available only for the GS908M V2-4PS switch.

---

Here are the guidelines for using the SET POE PORT command:

- ❑ You can use this command only on PoE ports, port 1 to 4.
- ❑ When the power management mode is class, the maximum power supplied to the port is the power level of the PD class if the power level of the PD is larger than the power limit.
- ❑ When the power management mode is class, the maximum power is the power limit specified by this command if the power level of the PD is smaller than the power limit.

- ❑ When the power management mode is actual, the maximum power supplied to the port is 15400 mili-watts on the port connected to the PD whose class is 0 to 3 even if the power limit is set to larger than 15400mili-watts.

### **Confirmation Command**

“SHOW POE” on page 342

### **Example**

The following command specifies the priority high and power limit 5000 mili-watts on port 1 and port 2:

```
Manager > set poe port=1-2 priority=high powerlimit=5000
```

## SET POE THRESHOLD

---

### Syntax

```
set poe threshold=threshold
```

### Parameters

*threshold*

Specifies the percentage of the maximum power that the switch supplies to the PDs.

### Description

Use this command to specify the threshold that the switch supplies to the connected PDs. The switch sends SNMP traps when the power supply to the PDs exceeds or falls below the threshold. For example, when the threshold is set to 80%, the switch sends SNMP traps when the power supply to the PDs exceeds 80% of the maximum power or falls below 80% of the maximum power.

---

#### Note

The PoE commands are available only for the GS908M V2-4PS switch.

---

### Confirmation Command

“SHOW POE” on page 342

### Example

The following command specifies the threshold 80% of the maximum power supply :

```
Manager > set poe threshold=80
```

## SHOW POE

---

### Syntax

```
show POE
```

### Parameters

None

### Description

Use this command to display information about PoE settings and ports. An example of the command output is shown in Figure 52.

```
PoE Global Power Status:
-----
Power Management Mode ..... Actual
Power Detect Mode ..... IEEE
PoE Limit ..... 75 W
Guard Band ..... 10 W
PoE No Connect ..... 65 W
Total Allocated Power ..... 0 W
Consumed Power ..... 0 W
Available Power ..... 75 W
Consumed Power Usage ..... 0 percent
Consumed Power Threshold ..... 95 percent

PoE All Ports Power Status Summary:
-----
Port  PoE Status  Class  Consumed(mW)  Power State
-----
1     Enabled      -      0             OFF - Detection in process
2     Enabled      -      0             OFF - Detection in process
3     Enabled      -      0             OFF - Detection in process
4     Enabled      -      0             OFF - Detection in process
-----
```

Figure 52. SHOW POE Command

### Example

The following example displays information about PoE settings and ports:

```
Manager > show poe
```

## SHOW POE PORT

---

### Syntax

```
show POE port[=port_list|all]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to display information about PoE ports. An example of the command output is shown in Figure 53.

```

PoE Port Information
-----
Port ..... 1
PoE Status ..... Enabled
Power Limit ..... 30000mw
Power Priority ..... LOW
Power State ..... ON - valid PD detected
Consumed Power ..... 1900 mw
Power Class ..... 1
-----

```

Figure 53. SHOW POE PORT Command

### Example

The following example displays information about PoE settings and ports:

```
Manager > show poe port=1
```





## Chapter 19

# Power Saving Commands

The Power Saving commands are summarized in Table 37.

Table 37. Power Saving Commands

Command	Description
“CREATE TRIGGER” on page 346	Creates a power saving trigger.
“DESTROY TRIGGER” on page 349	Deletes a power saving trigger.
“DISABLE TRIGGER” on page 350	Disables a power saving trigger.
“ENABLE TRIGGER” on page 351	Enables a power saving trigger.
“PURGE TRIGGER” on page 352	Disables and deletes all power saving triggers.
“SET LED MODE” on page 353	Specifies the global port LED mode.
“SET LED PORT” on page 354	Specifies the port LED settings on ports.
“SET TRIGGER” on page 356	Modifies a power saving trigger.
“SHOW LED” on page 359	Displays the LED settings.
“SHOW TRIGGER” on page 360	Displays information about triggers.

## CREATE TRIGGER

---

### Syntax

```
create trigger=trigger_id
psmode[=sleep|ledoff|portoff|poeoff] starttime=time
[endtime=time] [startdate=date] [enddate=date]
[days=day_list] port[=port_list|all] [name=string]
[poetarget=alliedtelesis-ap|other] [state=enabled|disabled]
[test=yes|no|on|off]
```

### Parameters

*trigger\_id*

Specifies a power saving trigger ID. The range is 1 to 10.

psmode

Specifies the power saving mode.

sleep

The switch is turned off and in the standby mode.

ledoff

The switch turns off the led.

portoff

The switch shuts down the port.

poeoff

The switch stops supplying power to a PoE PD.

starttime

Specifies the time to start the trigger.

endtime

Specifies the time to end the trigger.

*time*

Specifies time in the hh:mm format.

startdate

Specifies the start date that the trigger becomes effective.

enddate

Specifies the end date that the trigger becomes effective.

*date*

Specifies a date in the yyy-mm-dd format.

*days*

Specifies days that the trigger is effective.

*day\_list*

The options are mon, tue, wed, thu, fri, sat, sun, weekday, weekend, or any combination. The weekday is mon, tue, wed, thu, and fri. The weekend is san and sun. To specify multiple options, use comma (,) to separate them.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

*all*

Specifies all the switch ports.

*name*

Specifies a trigger name up to 40 alphanumeric characters. Use double quotes (") to specify a space.

*poetarget*

Specifies a type of PD. This parameter is used when the psmode is set to poeoff.

*alliedtelesis-ap*

When the PD is a Allied Telesis wireless access point, the link relay function is enabled. When the trigger becomes effective, the switch disconnect the link and stops supplying power to the connected wireless access point. The wireless access point can disconnect its clients before shutting down.

*other*

When the PD is other than Allied Telesis access point. When the trigger becomes effective, the switch stops supplying power to PDs. This is the default setting.

*state*

Enables or disables the trigger. The options are enabled and disabled. By default, the trigger is enabled.

*test*

Specifies the trigger to the test mode. When the trigger starts, no action is taken, but log messages are issued. The default setting is no.

*yes, on*

The trigger is in the test mode.

*no, off*

The trigger is not in the test mode.

## Description

Use this command to create a power saving trigger.

Here are the guidelines for power saving triggers:

- ❑ To start the switch in the sleep mode due to the trigger, you must power on the switch or press the reset button.
- ❑ To start the switch in the sleep mode right after the trigger starts, you must wait at least one minute to restart the switch.
- ❑ A log messages is issued when the trigger ends and the switch is released from the sleep mode.
- ❑ The maximum days is 28 days for a trigger with the sleep mode. You must power on or reset the switch to be released from the sleep mode if the days parameter is set to longer than 28 days.
- ❑ When the trigger effective time is less than 3 minutes, the switch does not stop supplying power to PoE devices even if the psmode is set to poeoff.

## Confirmation Command

“SHOW TRIGGER” on page 360

## Example

The following command creates a trigger to set the switch in the sleep mode starting at 23:00 and ending at 6:00:

```
Manager > create trigger=1 psmode=sleep starttime=23:00  
endtime=6:00
```

## DESTROY TRIGGER

---

### Syntax

```
create trigger=trigger_id
```

### Parameters

*trigger\_id*

Specifies a power saving trigger ID.

### Description

Use this command to delete a power saving trigger.

### Confirmation Command

“SHOW TRIGGER” on page 360

### Example

The following command deletes trigger 10:

```
Manager > destroy trigger=10
```

## DISABLE TRIGGER

---

### Syntax

```
disable trigger=trigger_id
```

### Parameters

*trigger\_id*

Specifies a power saving trigger ID.

### Description

Use this command to disable a power saving trigger. Right after the trigger is created, the trigger is enabled except the state parameter is set to disabled.

### Confirmation Command

“SHOW TRIGGER” on page 360

### Example

The following command disables trigger 10:

```
Manager > disable trigger=10
```

## ENABLE TRIGGER

---

### Syntax

```
enable trigger=trigger_id
```

### Parameters

*trigger\_id*

Specifies a power saving trigger ID.

### Description

Use this command to enable a power saving trigger. Right after the trigger is created, the trigger is enabled except the state parameter is set to disabled.

### Confirmation Command

“SHOW TRIGGER” on page 360

### Example

The following command enables trigger 10:

```
Manager > enable trigger=10
```

## PURGE TRIGGER

---

### Syntax

```
purge trigger
```

### Parameters

*trigger\_id*  
Specifies a power saving trigger ID.

### Description

Use this command to disable and delete all power saving triggers.

### Confirmation Command

“SHOW TRIGGER” on page 360

### Example

The following command disables and deletes all power saving triggers:

```
Manager > purge trigger
```



## SET LED MODE

---

### Syntax

```
set led mode=speed|duplex|off
```

### Parameters

#### speed

Sets the LED mode to speed. The LINK/ACT LED's are on and the SPD/DPX LED's indicate the speed.

#### duplex

Sets the LED mode to duplex. The LINK/ACT LED's are on and the SPD/DPX LED's indicate the duplex mode.

#### duplex

Turns off the port LED's.

### Description

Use this command to set the global port LED mode. When the port LED mode is speed or duplex, the port LED's are on.

Here are guidelines for the global port LED mode:

- ❑ When the global port LED mode is off, the port LED settings on ports specified by the SET LED PORT command have priority over the global port LED mode.
- ❑ The operations of the MODE button on the switch panel have priority over the global port LED mode.

### Confirmation Command

“SHOW LED” on page 359

### Example

The following command sets the LED mode to off:

```
Manager > set led mode=off
```

## SET LED PORT

---

### Syntax

```
set led port=port_list|all [action=on|off] [rate=rate|none]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### action

Specifies the action of the LINK/ACT LED on a port.

#### on

The LINK/ACT LED on a port is on.

#### off

The LINK/ACT LED on a port is on. This is the default setting.

#### rate

Specifies the threshold of the receiving rate. When the action parameter is on, this parameter is set to none.

#### *rate*

Specifies the threshold in Kbps. The range is 1 to 1024000 Kbps. When the receiving rate at a port exceeds the threshold, the port LED flashes.

#### none

Specifies no threshold. The port LED is off. This is the default setting.

### Description

Use this command to set the port LED settings on ports. The settings are effective on LINK/ACT LED's when the global port LED mode is off.

**Confirmation Command**

“SHOW LED” on page 359

**Example**

The following command sets the LED on port 1 to be off when the receiving rate is less than 1 Kbps:

```
Manager > set led port=1 action=off rate=1
```

## SET TRIGGER

---

### Syntax

```
set trigger=trigger_id psmode=sleep|ledoff|portoff|poeoff
starttime=time [endtime=time] [startdate=date]
[enddate=date] [days=day_list] [port=port_list|all]
[name=string] [poetarget=alliedtelesis-ap|other]
[state=enabled|disabled] [test=yes|no|on|off]
```

### Parameters

*trigger\_id*

Specifies a power saving trigger ID.

psmode

Specifies the power saving mode.

sleep

The switch turns off and is in the standby mode.

ledoff

The switch turns off the led.

portoff

The switch shuts down the port.

poeoff

The switch stops supplying power to a PoE PD.

starttime

Specifies the time to start the trigger.

endtime

Specifies the time to end the trigger.

*time*

Specifies time in the hh:mm format.

startdate

Specifies the start date that the trigger becomes effective.

enddate

Specifies the end date that the trigger becomes effective.

*date*

Specifies a date in the yyy-mm-dd format.

days

Specifies days that the trigger is effective.

*day\_list*

The options are mon, tue, wed, thu, fri, sat, sun, weekday, weekend, or any combination. The weekday is mon, tue, wed, thu, and fri. The weekend is san and sun. To specify multiple options, use comma (,) to separate them.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

## all

Specifies all the switch ports.

## name

Specifies a trigger name up to 40 alphanumeric characters. Use double quotes (") to specify a space.

## poetarget

Specifies a type of PD. This parameter is used when the psmode is set to poeoff.

## alliedtelesis-ap

When the PD is a Allied Telesis wireless access point, the link relay function is enabled. When the trigger becomes effective, the switch disconnect the link and stops supplying power to the connected wireless access point. The wireless access point can disconnect its clients before shutting down.

## other

When the PD is other than Allied Telesis access point. When the trigger becomes effective, the switch stops supplying power to PDs. This is the default setting.

## state

Enables or disables the trigger. The options are enabled and disabled. By default, the trigger is enabled.

## test

Specifies the trigger to the test mode. When the trigger starts, no action is taken, but log messages are issued. The default setting is no.

## yes, on

The trigger is in the test mode.

## no, off

The trigger is not in the test mode.

### **Description**

Use this command to modify a power saving trigger. See “CREATE TRIGGER” on page 346 for the guidelines for power saving triggers.

### **Confirmation Command**

“SHOW TRIGGER” on page 360

### **Example**

The following command changes trigger ID 1 to set the switch in the sleep mode starting at 24:00 and ending at 7:00:

```
Manager > set trigger=1 psmode=sleep starttime=24:00  
endtime=7:00
```

## SHOW LED

---

### Syntax

```
show led
```

### Parameters

None

### Description

Use this command to display information about port LED settings. An example of the command output is shown in Figure 54.

```
Switch LED Information
-----
Configured LED Mode ..... LED Off
Actual LED Mode ..... LED Off

Port Action Threshold RxRate Link PowerSave LEDState
-----
1 Off - - Up Yes Off
2 On 1 - Up No On
3 On 1024000 - Up Yes Off
4 On 1024000 - Down Yes Off
5 Off - - Up Yes Off
6 Off - - Up Yes Off
7 Off - - Up Yes Off
8 Off - - Down Yes Off
9 Off - - Down Yes Off
```

Figure 54. SHOW LED Command

### Example

The following example displays information about port LED settings:

```
Manager > show led
```

## SHOW TRIGGER

---

### Syntax

```
show trigger=trigger_id [full|status|summary]
```

### Parameters

*trigger\_id*

Specifies a power saving trigger ID.

full

Displays the detailed information about the trigger.

status

Displays the status of the trigger module.

summary

Displays the summary of all triggers. This is the default setting.

### Description

Use this command to display information about PoE ports. An example of the command output is shown in Figure 55.

```

Manager > show trigger=2 full
Trigger ..... 2
Name ..... SLEEP Trigger start at 18:00
Type and details ..... Time-SLEEP (18:00-23:59)
Days ..... Daily
Start Time ..... 18:00
End Time ..... 23:59
Port ..... 1,3,5-10
PoE Target ..... ALLIEDTELEESIS-AP
Enabled ..... Enabled
Test ..... No
Repeat ..... Yes
Created/Modified ..... 2011-05-11 16:16:02
Number of Activations ..... 0
Last Activation ..... ****_**_** **:**:**
Number of scripts ..... 0

```

Figure 55. SHOW TRIGGER Command

### Example

The following example displays the status of the trigger module:

```
Manager > show trigger status
```



## Chapter 20

# Rapid Spanning Tree Protocol (RSTP) Commands

---

This Rapid Spanning Tree Protocol commands are summarized in Table 38 and described in this chapter.

Table 38. Rapid Spanning Tree Protocol Commands

Command	Description
“DISABLE STP” on page 362	Disables RSTP on individual ports or the switch.
“ENABLE STP” on page 363	Enables RSTP on individual ports or the switch.
“PURGE STP” on page 364	Resets all RSTP parameter settings to their default values.
“SET STP” on page 365	Sets the RSTP bridge settings.
“SET STP PORT” on page 368	Sets the RSTP port settings.
“SHOW STP” on page 371	Displays the RSTP bridge settings.
“SHOW STP PORTCONFIG” on page 374	Displays the RSTP port settings.
“SHOW STP PORTSTATE” on page 375	Displays the RSTP status of the ports.

## DISABLE STP

---

### Syntax

```
disable stp [port=port_list|all]
```

### Parameters

*port\_list*

Specifies one or more ports. To specify multiple ports, use commas to separate nonconsecutive numbers (for example 5,7,9) or a dash to specify consecutive numbers (for example 1-4).

### Description

This command is used to disable the Rapid Spanning Tree Protocol (RSTP) on selected ports or the switch. By default, RSTP is disabled. To view the current status of RSTP, use “SHOW STP” on page 371.

### Examples

The following command disables RSTP on ports 5 and 6:

```
disable stp port=5-6
```

The following command disables RSTP on the switch:

```
disable stp
```

## ENABLE STP

---

### Syntax

```
enable stp [port=port_list|all]
```

### Parameters

*port\_list*

Specifies one or more ports. To specify multiple ports, use commas to separate nonconsecutive numbers (for example 5,7,9) or a dash to specify consecutive numbers (for example 1-4).

### Description

This command is used to enable the Rapid Spanning Tree Protocol on selected ports or the switch. By default, RSTP is disabled. To view the current status of RSTP, use “SHOW STP” on page 371. The default setting for RSTP is disabled.

### Examples

The following command enables RSTP on ports 1 and 4:

```
enable stp port=1,4
```

The following command enables RSTP on the switch:

```
enable stp
```

## PURGE STP

---

### Syntax

```
purge stp
```

### Parameters

None

### Description

This command returns all the RSTP bridge and port parameters to the default settings. RSTP must be disabled before you can use this command. To disable RSTP, refer to “DISABLE STP” on page 362.

### Example

The following command resets the RSTP parameters to their default settings:

```
purge stp
```

### Equivalent Command

```
set stp default
```

For information, refer to “SET STP” on page 365.

## SET STP

---

### Syntax

```
set stp [rstptype=normal|stpcompatible] [priority=priority]
[maxage=maxage] [hellotime=hellotime]
[forwarddelay=forwarddelay] [default]
```

### Parameters

#### *rstptype*

Sets the RSTP mode. The options are:

*normal*: The bridge uses RSTP. It transmits RSTP BPDU packets, except on ports connected to bridges running STP. This is the default setting.

*stpcompatible*: The bridge uses the RSTP parameter settings, but transmits only STP BPDU packets from the ports. These options are equivalent.

#### *priority*

Specifies the priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. The range is 0 to 61,440 in increments of 4,096, as shown in Table 39. The default value is 32,768. If you enter a value that is not an increment of 4096, the switch rounds the value down to the previous increment.

Table 39. Bridge Priority Values

Bridge Priority	Bridge Priority
0	32768
4096	36864
8192	40960
12288	45056
16384	49152
20480	53248
24576	57344
28672	61440

**maxage**

Specifies the length of time, in seconds, after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

---

**Note**

The value for the maxage parameter must be greater than  $(2 \times (\text{hellotime} + 1))$  and less than  $(2 \times (\text{forwarddelay} - 1))$ .

---

**hellotime**

Specifies the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

**forwarddelay**

Specifies the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds. This parameter effects only those ports operating in the STP compatible mode.

**default**

Returns all bridge and port RSTP settings to the default values. This parameter cannot be used with any other command parameter and only when RSTP is disabled. (This parameter performs the same function as the PURGE STP command.)

**Description**

This command configures the following RSTP parameter settings.

- Bridge priority
- Hello time
- Forwarding delay
- Maximum age time
- Force version of STP or normal RSTP

This command can also return the RSTP parameters to their default settings.

## Examples

The following command sets the bridge priority to 20480, the hello time to 5 seconds, and the forwarding delay to 20 seconds:

```
set stp priority=20480 hellotime=5 forwarddelay=20
```

The following command uses the RSTPTYPE parameter to configure the bridge to use the RSTP parameters but to transmit only STP BPDU packets:

```
set stp rstptype=stpcompatible
```

The following command returns all RSTP parameter settings to their default values:

```
set stp default
```

## Equivalent Command

```
purge stp
```

For information, see “PURGE STP” on page 364.

## SET STP PORT

---

### Syntax

```
set stp port=port_list [portpriority=portpriority]
[pathcost=cost|auto] [edgeport=yes|no|on|off|true|false]
[ptp=auto|yes|no|on|off|true|false]
[migrationcheck=on|yes|true]
```

### Parameters

#### *port\_list*

Specifies one or more ports. To specify multiple ports, use commas to separate nonconsecutive numbers (for example 5,7,9) or a dash to specify consecutive numbers (for example (1-4)).

#### portpriority

Specifies the port's priority. This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16, for a total of 16 increments, as shown in Table 40. The default is 128. If you enter a value that is not an increment of 16, the switch rounds the value down to the previous increment.

Table 40. Port Priority Values

Bridge Priority	Bridge Priority
0	128
16	144
32	160
48	176
64	192
80	208
96	224
112	240

#### pathcost

Specifies the port's cost. The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The options are:

**cost:** A value for the port cost. The range is 1 to 200,000,000.



auto: Automatically sets the port cost according to the speed of the port. This is the default. Table 41 lists the port costs with auto-detect.

Table 41. RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	200,000 to 2,000,000
100 Mbps	20,000 to 200,000
1000 Mbps	2,000 to 20,000

The port cost for a port that is part of a trunk is always 2,000, regardless of port speed.

#### edgeport

Defines whether the port is functioning as an edge port. An edge port is connected to a device operating at half-duplex mode and is not connected to any device running STP or RSTP. The options are:

yes, on, true: The port is an edge port. The options are equivalent.

no, off, false: The port is not an edge port. The options are equivalent. This is the default.

#### ptp

Defines whether the port is functioning as a point-to-point port. The parameters are equivalent. This type of port is connected to a device operating at full-duplex mode. The options are:

yes, on, true: The port is an point-to-point port. The options are equivalent.

no, off, false: The port is not an point-to-point port. The parameters are equivalent. are equivalent.

auto: The port's status is determined automatically. This is the default.

#### migrationcheck

Enables migration check. The purpose of this feature is to return a port to the RSTP mode from the STP compatible mode. The port remains in the RSTP mode until the port receives STP BPDU packets. The keywords, yes, on, true are equivalent and all enable migration check.

This parameter is not saved in the configuration file on the switch.

### **Description**

This command sets a port's RSTP settings.

### **Examples**

The following command sets the port cost to 1,000,000 and port priority to 224 (increment 14) on port 4:

```
set stp port=4 portcost=1000000 portpriority=14
```

The following command changes ports 6 to 8 so they are not considered edge ports:

```
set stp port=6-8 edgeport=no
```

## SHOW STP

### Syntax

```
show stp
```

### Parameters

None.

### Description

You use this command to display the RSTP parameter settings. An example of the command is shown in Figure 56.

```

STP Information
-----
RSTP Type ..... Normal
Number of Ports ..... 16
  Number Enabled ..... 4
  Number Disabled ..... 12
Enable Port List ..... 1-4
Bridge Identifier ..... 32768 : 00:21:46:A7:B4:11
Bridge Priority ..... 32768
Root Bridge ..... 32768 : 00:21:46:A7:B4:11
Root Port ..... (n/a)
Root Path Cost ..... 0
Max Age ..... 20
Hello Time ..... 2
Forward Delay ..... 15/15
Switch Max Age ..... 20
Switch Hello Time ..... 2
Switch Forward Delay ..... 15/15
Hold Time ..... 1

```

Figure 56. SHOW STP Command

The fields are described in Table 42.

Table 42. SHOW STP Command

Column	Description
RSTP Type	Indicates whether the switch is operating in the normal RSTP mode or STP compatible mode.
Number of Ports	Indicates the number of ports on the switch.
Number Enabled	Displays the number of ports on which RSTP is enabled.

Table 42. SHOW STP Command (Continued)

Column	Description
Number Disabled	Displays the number of ports on which RSTP is disabled.
Enable Port List	Displays the port numbers of the ports with RSTP is enabled.
Bridge Identifier	Displays the bridge Identifier parameter consists of the switch's bridge priority value and MAC address, separated by a colon (:). To change the switch's priority value, refer to "SET STP" on page 365. The MAC address of the switch cannot be changed.
Bridge Priority	Displays the switch's bridge priority.
Root Bridge	Displays the bridge priority value and MAC address of the root switch of the spanning tree domain. The values are separated by a colon (:).
Root Port	Displays the port that leads to the root bridge. This value displays n/a if the switch is the root bridge.
Root Path Cost	Displays the path cost of the port that leads to the root bridge. This value displays 0 if the switch is the root bridge.
Max Age	Displays the maximum age value on the root bridge of the spanning tree domain.
Hello Time	Displays the hello time value on the root bridge of the spanning tree domain.
Forward Delay	Displays the forward delay value on the root bridge of the spanning tree domain.
Switch Max Age	Displays the maximum age value on the switch.
Switch Hello Time	Displays the hello time value on the switch.

Table 42. SHOW STP Command (Continued)

<b>Column</b>	<b>Description</b>
Switch Forward Delay	Displays the forward delay value on the switch.
Hold Time	Displays the minimum transmission interval when the root bridge sends a confirmation BPDU.

**Examples**

The following command displays the RSTP parameter settings:

```
show stp
```

## SHOW STP PORTCONFIG

---

### Syntax

```
show stp portconfig[=port_list|all]
```

### Parameters

*port\_list*

Specifies one or more ports. To specify multiple ports, use commas to separate nonconsecutive numbers (for example 5,7,9) or a dash to specify consecutive numbers (for example (1-4)).

### Description

You use this command to display the RSTP settings of the ports on the switch. The parameters are defined in “SET STP PORT” on page 368. An example of the command is shown in Figure 57.

Port	Edge-Port	Point-to-Point	Cost	Priority
1	Yes	Auto Update	Auto Update	128
2	Yes	Auto Update	Auto Update	128
3	Yes	Auto Update	Auto Update	128
4	Yes	Auto Update	Auto Update	128
5	Yes	Auto Update	Auto Update	128
6	Yes	Auto Update	Auto Update	128
7	Yes	Auto Update	Auto Update	128
8	Yes	Auto Update	Auto Update	128

Figure 57. SHOW STP PORTCONFIG Command

### Examples

The following command displays the RSTP parameter settings for port 1:

```
show stp portconfig=1
```

The following command displays the RSTP parameter settings for all of the ports:

```
show stp portconfig=all
```

## SHOW STP PORTSTATE

### Syntax

```
show stp portstate[=port_list|all]
```

### Parameters

*port\_list* Specifies one or more ports. To specify multiple ports, use commas to separate nonconsecutive numbers (for example 5,7,9) or a dash to specify consecutive numbers (for example (1-4)).

### Description

You use this command to display the current operating status of the ports. An example is shown in Figure 58.

Port	Enable	State	Role	Edge	P2P	Version	Port Cost
1	Enabled	Forwarding	Designated	No	Yes	RSTP	200000
2	Enabled	Forwarding	Designated	No	Yes	RSTP	200000
3	Enabled	Forwarding	Designated	No	Yes	RSTP	200000
4	Enabled	Forwarding	Designated	No	Yes	RSTP	200000
5	Enabled	Forwarding	Designated	No	Yes	RSTP	200000
6	Enabled	Forwarding	Designated	No	Yes	RSTP	200000
7	Enabled	Forwarding	Designated	No	Yes	RSTP	200000
8	Enabled	Forwarding	Designated	No	Yes	RSTP	200000

Figure 58. SHOW STP PORTSTATE Command

The columns are described in Table 43.

Table 43. SHOW STP PORTSTATE Command

Column	Description
Port	The port number.
Enabled	Whether STP is enabled or disabled on the port.

Table 43. SHOW STP PORTSTATE Command (Continued)

Column	Description
State	<p>The RSTP state of the port. The possible states for a port connected to another device running RSTP are Discarding and Forwarding.</p> <p>The possible states for a port connected to a device running STP are Listening, Learning, Forwarding, and Discarding.</p> <p>The possible states for a port not being used or where spanning tree is not activated is Disabled.</p>
Role	<p>The RSTP role of the port. Possible roles are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Root - The port is connected to the root switch, directly or through other switches, with the least path cost.</li> <li><input type="checkbox"/> Alternate - The port offers an alternate path to the root switch.</li> <li><input type="checkbox"/> Backup - The port on a designated switch that provides a backup for the path provided by the designated port.</li> <li><input type="checkbox"/> Designated - The port has the least cost path to the root switch.</li> </ul>
Edge	Whether the port is functioning as an edge port.
P2P	Whether or not the port is functioning as a point-to-point port. The possible settings are Yes and No.
Version	Whether the port is operating in RSTP mode or STP-compatible mode.
Port Cost	The current operating cost of the port.

### Examples

The following command displays the status of RSTP for port 3:

```
show stp portstate=3
```

The following command displays the status of RSTP for all of the ports:

```
show stp portstate=all
```



## Chapter 21

# Multiple Spanning Tree Protocol (MSTP) Commands

---

The MSTP commands are summarized in Table 44 and described in this chapter.

Table 44. Multiple Spanning Tree Protocol Commands

Command	Description
“ADD MSTP MSTI VLAN” on page 379	Associates VLANs to MST instances.
“CREATE MSTP MSTI” on page 380	Creates an MST instance.
“DELETE MSTP MSTI VLAN” on page 381	Releases a VLAN from the associated MST instance.
“DESTROY MSTP MSTI” on page 382	Deletes an MST instance.
“DISABLE MSTP” on page 383	Disables MSTP on the selected ports or the switch.
“DISABLE MSTP DEBUG MSTI” on page 384	Disables the debug option on an MST instance.
“ENABLE MSTP” on page 385	Enables MSTP on the selected ports or the switch.
“ENABLE MSTP DEBUG MSTI” on page 387	Enables the debug option on an MST instance.
“PURGE MSTP” on page 389	Sets all the MSTP parameters to the default settings.
“RESET MSTP COUNTER PORT” on page 390	Clears MSTP counters on the specified port.
“SET MSTP” on page 391	Specifies the MSTP settings of the switch.
“SET MSTP CIST” on page 393	Specifies the bridge priority for Common and Internal Spanning Tree (CIST).
“SET MSTP CIST PORT” on page 394	Specifies the MSTP settings for CIST.

Table 44. Multiple Spanning Tree Protocol Commands (Continued)

<b>Command</b>	<b>Description</b>
"SET MSTP MSTI" on page 397	Specifies the bridge priority to the specified MST instance.
"SET MSTP MSTI PORT" on page 398	Specifies the port priority for an MST instance.
"SHOW MSTP" on page 399	Displays the settings and state of MSTP and CIST.
"SHOW MSTP COUNTER PORT" on page 401	Displays the MST counters on the specified ports.
"SHOW MSTP DEBUG MSTI" on page 402	Displays the debug options on the specified MST instance.

## ADD MSTP MSTI VLAN

---

### Syntax

```
add mstp msti=instance vlan=vlan_list|all
```

### Parameters

*instance*

Specifies MST instance ID. The range is 1 to 15.

*vlan\_list*

Specifies a list of VLANs. To specify multiple VLANs, use a comma (,) to separate them. To specify a range of VLANs, use a hyphen (-).

### Description

Use this command to associate VLANs to MST instances. By default, all VLANs are associated to Common and Internal Spanning Tree (CIST).

When associated to a MST instance, the VLAN is not associated to CIST any more. A VLAN can be associated to only one MST instance. To change a MST instance for a VLAN, you must delete a MST instance from a VLAN using the DELETE MSTP MSTI VLAN command before using the ADD MSTP MSTI VLAN command.

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command associates VLAN 10 to MST instance 1:

```
add mstp msti=1 vlan=10
```

## CREATE MSTP MSTI

---

### Syntax

```
create mstp msti=instance priority=priority
```

### Parameters

#### *instance*

Specifies MST instance ID. The range is 1 to 15.

#### *priority*

Specifies bridge priority for the MST instance. The range is 0 to 65535. The default value is 32768. The smaller number has higher priority to be a root bridge. The switch converts the specified number into an increment of 4096, which is close to and smaller than the specified number. For example, when you specifies 10,000, the switch sets the priority to 8192.

### Description

Use this command to create a MST instance. One switch or one region can have up to 15 MST instances.

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command creates MST instance 1:

```
create mstp msti=1
```

## DELETE MSTP MSTI VLAN

---

### Syntax

```
delete mstp msti=instance vlan=vlan_list|all
```

### Parameters

*msti*

Specifies an MST instance that the debug option is enabled for.

*instance*

Specifies MST instance ID. The range is 1 to 15.

*vlan\_list*

Specifies a list of VLANs. To specify multiple VLANs, use a comma (,) to separate them. To specify a range of VLANs, use a hyphen (-).

### Description

Use this command to release a VLAN from association with a MST instance. When a VLAN is released from the associated MST instance, the VLAN is automatically returned to Common and Internal Spanning Tree (CIST).

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command releases VLAN 10 from the associated MST instance 1:

```
delete mstp msti=1 vlan=10
```

## DESTROY MSTP MSTI

---

### Syntax

```
disable mstp msti=instance
```

### Parameters

*instance*

Specifies a MST instance ID. The range is 1 to 15.

### Description

Use this command to delete a MST instance. The MSTP instance associated with a VLAN cannot be deleted. To delete a MSTP instance, release the VLAN from the MSTP instance using the DELETE MSTP MSTI VLAN command before using the DESTROY MSTP MSTI command.

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command deletes the MSTP instance 1:

```
destroy mstp msti=1
```

## DISABLE MSTP

---

### Syntax

```
disable mstp [port=port_list|all]
```

### Parameters

*port*

Specifies one or more ports that MSTP is disabled on. To disable MSTP on a trunk port, you must specify all members in the trunk group.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

This command is used to disable the Multiple Spanning Tree Protocol (MSTP) on the selected ports or the switch. By default MSTP is disabled.

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command disables MSTP on ports 5 and 6:

```
disable mstp port=5-6
```

The following command disables MSTP on the switch:

```
disable mstp
```

## DISABLE MSTP DEBUG MSTI

---

### Syntax

```
disable mstp debug=msg|pkt|state|all msti=cist|instance|all
[port=port_list|all]
```

### Parameters

**debug**

Specifies a debug option to disable.

**msg**

Specifies the msg option to decode and display BPDU.

**pkt**

Specifies the pkt option to display BPDU for an ASCII value.

**state**

Specifies the state option to display the state of ports.

**msti**

Specifies an MST instance that the debug option is disabled for.

**csti**

Common and Internal Spanning Tree (CIST) instance.

*instance*

Specifies MST instance ID. The range is 1 to 15.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

### Description

This command is used to disable the debug option on the specified MSTP instance. By default, MSTP debugging is disabled.

### Confirmation Command

“SHOW MSTP DEBUG MSTI” on page 402

### Examples

The following command disables all MSTP debug options on all MSTP instances:

```
disable mstp debug=all msti=all
```



## ENABLE MSTP

---

### Syntax

```
enable mstp [port=port_list |all]
```

### Parameters

*port*

Specifies one or more ports that MSTP is enabled on. To enable MSTP on a trunk port, you must specify all member ports in the trunk group.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

*all*

Specifies all the switch ports.

### Description

This command is used to enable the Multiple Spanning Tree Protocol (MSTP) on the selected ports or the switch. By default, MSTP is disabled.

Here are the guidelines for MSTP:

- When MSTP is enabled on a port, the port cannot be a mirror port, authenticator or supplicant port for Port-based authentication.
- When MSTP is enabled on a port, the port-security feature on the port is disabled.
- When MSTP is enabled, Bridge Protocol Data Unit (BPDU) protection is disabled.
- To enable MSTP on a trunk port, you must specify all member ports in the trunk group.

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command enables MSTP on ports 5 and 6:

```
enable mstp port=5-6
```

The following command enables MSTP on the switch:

```
enable mstp
```

## ENABLE MSTP DEBUG MSTI

---

### Syntax

```
enable mstp debug=msg|pkt|state|all msti=cist|instance|all
[port=port_list|all]
[statemachine=ptm|prx|ppm|pim|ptx|prs|prt|pst|tcm|all]
[output=console] [timeout=timeout|none]
```

### Parameters

**debug**

Specifies a debug option to enable.

**msg**

Specifies the msg option to decode and display BPDU.

**pkt**

Specifies the pkt option to display BPDUs in ASCII code.

**state**

Specifies the state option to display the state of ports.

**msti**

Specifies an MST instance that the debug option is enabled for.

**csti**

Common and Internal Spanning Tree (CIST) instance.

***instance***

Specifies MST instance ID. The range is 1 to 15.

***port\_list***

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

**statemachine**

Specifies the state machine to display the state when the debug option is specified state or all.

**ptm**

Port timer state machine.

**prx**

Port receive state machine.

**ppm**

Port protocol migration state machine.

<code>pim</code>	Port information state machine.
<code>ptx</code>	Port transmit state machine.
<code>prs</code>	Port role selection state machine.
<code>prt</code>	Port role transition state machine.
<code>pst</code>	Port state transition state machine.
<code>tcn</code>	Topology change state machine.
<code>output</code>	Specifies the output to display debug information. The option is console only.
<code>timeout</code>	Specifies time in seconds when the debug option is enabled. The range is 1 to 4,000,000,000 seconds.

### **Description**

Use this command to enable the debug option on the specified MSTP instance. By default, MSTP debugging is disabled.

### **Confirmation Command**

“SHOW MSTP” on page 399

### **Examples**

The following command enables all MSTP debug options on all MSTP instances:

```
enable mstp debug=all msti=all
```

## PURGE MSTP

---

### Syntax

```
purge mstp
```

### Parameters

None.

### Description

Use this command to set all the MSTP parameters to the default settings. The command deletes all MSTP instances that the user created, resets all VLANs to belong to Common and Internal Spanning Tree (CIST), and disable MSTP.

### Confirmation Command

“SHOW MSTP” on page 399

### Example

The following command resets the MSTP parameters to their default settings:

```
purge mstp
```

## RESET MSTP COUNTER PORT

---

### Syntax

```
reset mstp counter port[=port_list|all]
```

### Parameters

*port*

Specifies one or more ports that MSTP counters are reset on.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to clear MSTP counters on the specified port.

### Confirmation Command

“SHOW MSTP COUNTER PORT” on page 401

### Examples

The following command clears MSTP counters on ports 5 and 6:

```
reset mstp counter port=5-6
```

## SET MSTP

---

### Syntax

```
set mstp [configname=name] [revisionlevel=revisionlevel]
[maxhops=maxhops] [maxage=maxage] [hellotime=hellotime]
[forwarddelay=forwarddelay]
[protocolversion=mstp|stpcompatible]
```

### Parameters

#### configname

Specifies the name of the MST region that the switch belongs to. The name must be up to 32 alphanumeric characters including an underscore (\_). The default value is the MAC address of the switch.

#### revisionlevel

Specifies the revision of the MST region that the switch belongs to. The range is 0 to 65535. The default value is 0.

#### maxhops

Specifies the maximum number of hops for a BPDU to be forwarded in the MST region before a BPDU is discarded. The default value is 20.

#### maxage

Specifies the maximum aging time of BPDUs in seconds. The maxage is the length of time the switch holds a configuration BPDU before discarding it and attempting a reconfiguration. The range is 6 to 40 seconds. The default is 20 seconds.

---

#### Note

The value for the maxage parameter must be greater than  $(2 \times (\text{hellotime} + 1))$  and less than  $(2 \times (\text{forwarddelay} - 1))$ .

---

#### hellotime

Specifies the time interval, in seconds, between configuration messages the root bridge sends. The range is 1 to 10 seconds. The default is 2 seconds.

#### forwarddelay

Specifies the forward delay time in seconds. The forward delay time is the length of time that a port waits before changing the STP state from learning and listening to forwarding. The range is 4 to 30 seconds. The default is 15 seconds. This parameter effects only the ports operating in the STP compatible mode.

`protocolversion`  
Specifies the protocol version.

`mstp`  
Specifies MSTP version.

`stpcompatible`  
Specifies MSTP version using STP BPDUs.

### **Description**

Use this command to change the following MSTP parameters of the switch:

- MST region
- Revision of the MST region
- Maximum hops
- Maximum age time
- Hello time
- Forwarding delay
- Protocol version

### **Confirmation Command**

“SHOW MSTP” on page 399

### **Examples**

The following command changes the revision of the MST region:

```
set mstp revisionlevel=2
```



## SET MSTP CIST

---

### Syntax

```
set mstp cist priority=priority
```

### Parameters

#### *priority*

Specifies the bridge priority for CIST. The smaller number has higher priority to be a root bridge. The range is 0 to 65535. The default value is 32768. The switch converts the specified number into an increment of 4096, which is close to and smaller than the specified number. For example, when you specifies 10,000, the switch sets the priority to 8192.

### Description

Use this command to set the bridge priority for Common and Internal Spanning Tree (CIST).

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command sets the bridge priority for CIST to 4096:

```
set mstp cist priority=4096
```

## SET MSTP CIST PORT

---

### Syntax

```
set mstp cist port[=port_list|all] priority=priority
[inpathcost=inpathcost|default|auto]
[expathcost=expathcost|default|auto]
[edgeport=yes|no|on|off|true|false]
[pointtopoint=yes|no|off|true|false|auto]
[migrationchech=yes|on|true]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### *priority*

Specifies the port priority for CIST. The smaller number has higher priority to be a root port. The range is 0 to 255. The default value is 128. The switch converts the specified number into an increment of 16, which is lose to and smaller than the specified number. For example, when you specifies 70, the switch sets the priority to 64.

#### *inpathcost*

Specifies the cost of the path to the CIST root bridge in the MST region.

#### *inpathcost*

Specifies the inpathcost. The range is 1 to 200,000,000. See Table 45 for the recommended cost and default costs per speed.

Table 45. In-Path Costs

Port Speed	Recommended Cost	Default Cost
10 Mbps	200,000 to 2,000,000	2,000,000
100 Mbps	20,000 to 200,000	200,000
1000 Mbps	2,000 to 20,000	20,000
Trunk Ports (10/100/1000 Mbps)	None (The past cost is always 2,000.)	2,000

#### default

Returns the setting to the default value.

- auto**  
Detects the port speed automatically and specifies the port cost according to the speed. This is the default setting.
- expathcost**  
Specifies the cost for the path to the region of the CIST root bridge.
- expathcost*  
Specifies the expathcost. The range is 1 to 200,000,000. See Table 45, "In-Path Costs" on page 394 for the recommended cost and default costs per speed.
- edgeport**  
Specifies whether the port is an edge port. The edge port is a port connected to a host, which does not have a bridge on this end.
- yes, on, true**  
Specifies the port as an edge port.
- no, off, false**  
Specifies that the port is not an edge port. This is the default setting. Even when the port is specified as an edge port, the port is no longer an edge port once receiving a BPDU.
- pointtopoint**  
Specifies the port is connected to another bridge on a point-to-point link.
- auto**  
Detects whether the port is connected to another bridge on a point-to-point link. This is the default setting.
- pointtopoint**  
Specifies the port is connected to another bridge on a point-to-point link.
- migrationcheck**  
Returns the port setting to the MSTP mode from the standard mode.
- yes, on, true**  
Specifies the port setting to the MSTP mode. This setting is not saved in the configuration file.

### **Description**

Use this command to specify the MSTP parameters for Common and Internal Spanning Tree (CIST).

### **Confirmation Command**

“SHOW MSTP” on page 399

### **Examples**

The following command sets port 10 to port 20 as edge ports:

```
set mstp cist port=10-20 edgeport=yes
```

## SET MSTP MSTI

---

### Syntax

```
set mstp msti=instance priority=priority
```

### Parameters

*instance*

Specifies MST instance ID.

*priority*

Specifies the bridge priority for the MST instance. The smaller number has higher priority to be a root bridge. The range is 0 to 65535. The default value is 32768. The switch converts the specified number into an increment of 4096, which is close to and smaller than the specified number. For example, when you specifies 10,000, the switch sets the priority to 8192.

### Description

Use this command to set the bridge priority to the specified MST instance.

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command sets the bridge priority of MST instance 5 to 8192:

```
set mstp cist priority=8192
```

## SET MSTP MSTI PORT

---

### Syntax

```
set mstp msti=instance port[=port_list|all]
priority=priority [pathcost=pathcost|default|auto]
```

### Parameters

#### *instance*

Specifies MST instance ID.

#### *priority*

Specifies the port priority. The smaller number has higher priority to be a root port. The range is 0 to 255. The default value is 128. The switch converts the specified number into an increment of 16, which is close to and smaller than the specified number. For example, when you specifies 70, the switch sets the priority to 64.

#### pathcost

Specifies the cost for the path to the root bridge of the MST instance.

#### *pathcost*

Specifies the pathcost. The range is 1 to 200,000,000. See Table 45 on page 394 for the recommended cost and default costs per speed.

#### default

Returns the setting to the default value.

#### auto

Detects the port speed automatically and specifies the past cost according to the speed. This is the default setting.

### Description

Use this command to set the port priority for an MST instance.

### Confirmation Command

“SHOW MSTP” on page 399

### Examples

The following command sets the port priority for port 10 for MST instance 5 to 64:

```
set mstp msti port=10 priority=64
```

## SHOW MSTP

---

### Syntax

```
show mstp [portconfig=port_list|all]  
[portstate=port_list|all] [mstistate=instance] [cist]  
[mstivlanassoc]
```

### Parameters

**portconfig**

Displays the settings of the specified port.

**portstate**

Displays the state of the specified port.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

**all**

Specifies all the switch ports.

**mstistate**

Displays the state of the specified MST instance.

**cist**

Displays the state of CIST.

**mstivlanassoc**

Displays the mapping table of MST instances and VLANs.

### Description

Use this command to display the settings and state of MSTP and CIST. See Figure 59 on page 400 for an example.

```
Manager > show mstp

Switch MSTP Config Information:

The current protocol version is: MSTP
Switch MSTP Config Information:

Status ..... Enabled
Force Version ..... NormalMSTP
Hello Time ..... 2/2 (Configured/Actual)
Forwarding Delay ..... 15/15 (Configured/Actual)
Max Age ..... 20/20 (Configured/Actual)
Max Hops ..... 20
Configuration Name ..... 00-00-F4-27-2D-81
Revision Level ..... 0
Bridge Identifier ..... 32768/00:00:F4:27:2D:81
Root Identifier ..... 32768/00:00:F4:27:2D:81
Root Path Cost ..... 0
```

Figure 59. SHOW MSTP Command

### Examples

The following command displays the MSTP configuration:

```
show mstp
```



## SHOW MSTP COUNTER PORT

### Syntax

```
show mstp counter port[=port_list|all]
```

### Parameters

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

all

Specifies all the switch ports.

### Description

Use this command to display the MSTP counters on the specified ports. See Figure 60 for an example.

MSTP Port Counters			
-----			
Port Number	5		
Receive:		Transmit:	
Total BPDUs	581	Total BPDUs	579
MSTP BPDUs	581	MSTP BPDUs	579
RSTP BPDUs	0	RSTP BPDUs	0
STP BPDUs	0	STP BPDUs	0
Invalid BPDUs	0		
Discarded:			
Port Disabled	0		
Invalid Protocol	0		
Invalid Type	0		
Invalid BPDUs length	0		
-----			

Figure 60. SHOW MSTP COUNTER PORT Command

### Examples

The following command displays the MSTP counters of port 5:

```
show mstp counter port=5
```

## SHOW MSTP DEBUG MSTI

---

### Syntax

```
show mstp debug msti=cist|instance|all]
```

### Parameters

*msti*

Specifies the MST instance to display the MSTP debug options.

*cist*

Displays the debug options on CIST.

*instance*

Specifies the MST instance ID to displays the debug options.

*all*

Displays the debug options on all the MST instances.

### Description

Use this command to display the debug options on the specified MST instance. See Figure 61 for an example.

```
Manager > show mstp debug msti=cist
```

MSTP Instance	Port	Debug Modes State Machine	Debug Modes	Output	Timeout
CIST	1	STATE		Asyn 0 (16)	None
		PTX			
	2	STATE		Asyn 0 (16)	None
		PTX			
	3	STATE		Asyn 0 (16)	None
		PTX			
	4	STATE		Asyn 0 (16)	None
		PTX			
	5	STATE		Asyn 0 (16)	None
		PTX			
...					

Figure 61. SHOW MSTP DEBUG MSTI Command

### Examples

The following command displays the debug options on CIST:

```
show mstp debug msti=cist
```

## Section IV

# Security and Traffic Control

---

This section contains the following chapters:

- ❑ Chapter 22, “Access Filter Commands” on page 405
- ❑ Chapter 23, “Internet Group Management Protocol (IGMP) Snooping Commands” on page 417
- ❑ Chapter 24, “Multicast Listener Discovery (MLD) Snooping Commands” on page 429
- ❑ Chapter 25, “Quality of Service (QoS) Commands” on page 441
- ❑ Chapter 26, “Policy-Based QoS Commands” on page 455
- ❑ Chapter 27, “Port-Based Authentication Commands” on page 497



## Chapter 22

# Access Filter Commands

The access filter commands are summarized in Table 46.

Table 46. Access Filter Commands

Command	Description
“ADD ACCESS FILTER” on page 406	Adds an access filter entry to the specified access filter group.
“DELETE ACCESS FILTER ENTRY” on page 408	Deletes an access filter entry from the access filter group.
“DISABLE ACCESS FILTER” on page 410	Disables the access filter function on the specified access filter group.
“ENABLE ACCESS FILTER” on page 411	Enables the access filter function on the specified access filter group.
“SET ACCESS FILTER” on page 412	Specifies the default action on the specified access filter group.
“SET ACCESS FILTER ENTRY” on page 413	Changes the settings of the specified access filter entry.
“SHOW ACCESS FILTER” on page 415	Displays the default action and status of the access filter groups or the settings of the specified access filter group.

## ADD ACCESS FILTER

---

### Syntax

```
add access filter=snmp|ftp|telnet|http|icmp|global
ipaddress=ip_address mask=mask action=pass|discard
port=port_list|all
```

### Parameters

*filter*

Specifies one of the access filter groups to the access filter entry.

*snmp*

Specifies the entry to add to the group snmp.

*ftp*

Specifies the entry to add to the group ftp.

*telnet*

Specifies the entry to add to the group telnet.

*http*

Specifies the entry to add to the group http.

*icmp*

Specifies the entry to add to the group icmp.

*global*

Specifies the entry to add to all the groups.

*ip\_address*

Specifies the IPv4 address of the target.

*mask*

Specifies the mask to filter the IPv4 address.

*action*

Specifies the action when a packet matches the access filter.

*pass*

Passes the packet when it matches the access filter.

*discard*

Discard the packet when it matches the access filter.

*port\_list*

Specifies a switch port number or list of port numbers. To specify multiple port numbers, separate port numbers using a comma or use a hyphen to specify the range of port numbers.

`all`  
Specifies all the switch ports.

### **Description**

Use this command to create an access filter entry. The switch can have up to 512 entries.

### **Confirmation Command**

“SHOW ACCESS FILTER” on page 415

### **Example**

The following command adds an access filter to deny Telnet on all the ports from the 192.168.1.2 device:

```
Manager > add access filter=telnet ipaddress=192.168.1.2  
mask=255.255.255.255 action discard port=all
```

## DELETE ACCESS FILTER ENTRY

---

### Syntax

```
delete access filter=snmp|ftp|telnet|http|icmp|global  
entry=entry_number
```

### Parameters

*filter*

Specifies the access filter group of the access filter. See “ADD ACCESS FILTER” on page 406.

*filter*

Specifies one of the access filter groups.

*snmp*

Specifies the group snmp.

*ftp*

Specifies the group ftp.

*telnet*

Specifies the group telnet.

*http*

Specifies the http.

*icmp*

Specifies the group icmp.

*global*

Specifies all the groups.

*entry\_number*

Specifies the number of the access filter entry. The entry number of an access filter is shown on the list. See “SHOW ACCESS FILTER” on page 415.

### Description

Use this command to delete the specified access filter entry.

### Confirmation Command

“SHOW ACCESS FILTER” on page 415



**Example**

The following command deletes an access filter 1 for Telnet:

```
Manager > delete access filter=telnet entry=1
```

## DISABLE ACCESS FILTER

---

### Syntax

```
disable access filter=snmp|ftp|telnet|http|icmp|global|all
```

### Parameters

`filter`

Specifies an access filter group. See “ADD ACCESS FILTER” on page 406.

`global`

Specifies all the access filter groups.

`all`

Specifies the access filter entries: snmp, ftp, telnet, http, and icmp.

### Description

Use this command to disable the access filter feature on the specified access filter group or all the access filter entries.

### Confirmation Command

“SHOW ACCESS FILTER” on page 415

### Example

The following command disables the access filter features for TFTP service:

```
Manager > disable access filter=tftp
```

## ENABLE ACCESS FILTER

---

### Syntax

```
enable access filter=snmp|ftp|telnet|http|icmp|global|all
```

### Parameters

`filter`

Specifies an access filter group. See “ADD ACCESS FILTER” on page 406.

`global`

Specifies all the access filter groups.

`all`

Specifies the access filter entries: snmp, ftp, telnet, http, and icmp.

### Description

Use this command to enable the access filter feature on the specified access filter group or all the access filter entries.

### Confirmation Command

“SHOW ACCESS FILTER” on page 415

### Example

The following command enables the access filter features for SNMP service:

```
Manager > enable access filter=snmp
```

## SET ACCESS FILTER

---

### Syntax

```
set access filter=snmp|ftp|telnet|http|icmp|global|all  
default=pass|discard
```

### Parameters

`filter`

Specifies an access filter group. See “ADD ACCESS FILTER” on page 406.

`global`

Specifies all the access filter groups.

`all`

Specifies the access filter entries: snmp, ftp, telnet, http, and icmp.

`default`

Specifies the default action.

`pass`

Passes the packet when it matches the access filter.

`discard`

Discard the packet when it matches the access filter.

### Description

Use this command to change the default action of an access filter group.

### Confirmation Command

“SHOW ACCESS FILTER” on page 415

### Example

The following command changes the default action to discard for the access filter group snmp:

```
Manager > set access filter=snmp default=discard
```

## SET ACCESS FILTER ENTRY

---

### Syntax

```
set access filter=snmp|ftp|telnet|http|icmp|global  
entry=entry_number [ipaddress=ip_address] [mask=mask]  
[action=pass|discard] [port=port_list|all]
```

### Parameters

**filter**

Specifies one of the access filter groups to the access filter entry.

**snmp**

Specifies the entry to add to the group snmp.

**ftp**

Specifies the entry to add to the group ftp.

**telnet**

Specifies the entry to add to the group telnet.

**http**

Specifies the entry to add to the group http.

**icmp**

Specifies the entry to add to the group icmp.

**global**

Specifies the entry to add to all the groups.

***entry\_number***

Specifies the number of the access filter entry.

***ip\_address***

Specifies the IPv4 address of the target.

***mask***

Specifies the mask to filter the IPv4 address.

**action**

Specifies the action when a packet matches the access filter.

**pass**

Passes the packet when it matches the access filter.

**discard**

Discard the packet when it matches the access filter.

*port\_list*

Specifies a switch port number or list of port numbers. To specify multiple port numbers, separate port numbers using a comma or use a hyphen to specify the range of port numbers.

all

Specifies all the switch ports.

### **Description**

Use this command to change the settings of the specified access filter entry.

### **Confirmation Command**

“SHOW ACCESS FILTER” on page 415

### **Example**

The following command changes the access filter entry 1 of the access filter group Telnet:

```
Manager > set access filter=telnet entry=1  
ipaddress=192.168.1.2 mask=255.255.255.255 action=pass  
port1-7
```

## SHOW ACCESS FILTER

---

### Syntax

```
show access filter=snmp|ftp|telnet|http|icmp|global|all
```

### Parameters

**filter**

Specifies an access filter group. See “ADD ACCESS FILTER” on page 406.

**global**

Specifies all the access filter groups.

**all**

Specifies the access filter entries: snmp, ftp, telnet, http, and icmp.

### Description

Use this command to display the default action and status of access filter groups or the settings of the specified access group. An example of the command output is shown in Figure 62.

```
Manager > show access filter
```

Filter	Default	Status
SNMP	Discard	Disabled
FTP	Pass	Disabled
TELNET	Discard	Disabled
HTTP	Pass	Disabled
ICMP	Pass	Disabled
GLOBAL	Pass	Disabled

Figure 62. SHOW ACCESS FILTER Command

Another example of the command output is shown in Figure 63.

```

Manager > show access filter=telnet

TELNET:
Access Filtering ..... Enabled
Port ..... 23
Default..... Discard

Entry      IP                MASK                ACTION  PORT
-----
1          192.168.1.2       255.255.255.0     Pass    ALL
2          192.168.8.5       255.255.255.0     Pass    1-7
3          192.168.40.5     255.255.0.0       Pass    2
-----

```

Figure 63. SHOW ACCESS FILTER Command with Parameter

The fields are described in Table 47.

Table 47. SHOW ACCESS FILTER Command

Field	Description
Filter	Displays the name of the access filter group.
Default	Displays the default action. The options are: <input type="checkbox"/> Pass <input type="checkbox"/> Discard
Status	Displays the feature is Enabled or Disabled.
Access Filtering	Displays the feature is Enabled Disabled.
Port	Displays the target switch ports.
Entry	Displays the entry number of the access filter.
IP	Displays the IPv4 address of the target.
MASK	Displays the mask to filter the IPv4 addresses.
ACTION	Displays the action at matching. The options are: <input type="checkbox"/> Pass <input type="checkbox"/> Discard
PORT	Displays the target switch ports.

### Example

The following example displays the settings of the access filter group Telnet:

```

Manager > show access filter=telnet

```



## Chapter 23

# Internet Group Management Protocol (IGMP) Snooping Commands

---

The IGMP Snooping commands are summarized in Table 48.

Table 48. IGMP Snooping Commands

Command	Description
“ADD IGMP SNOOPING MCGROUP” on page 418	Add a multicast group for IGMP Snooping.
“DELETE IGMP SNOOPING” on page 421	Deletes a static multicast group address.
“DISABLE IGMP SNOOPING” on page 422	Disables IGMP Snooping.
“ENABLE IGMP SNOOPING” on page 423	Enables IGMP Snooping.
“SET IGMP SNOOPING” on page 424	Specifies the timeout and changes the settings of the multicast group.
“SET IGMP SNOOPING MCGROUP” on page 426	Changes the router ports for the multicast group.
“SHOW IGMP SNOOPING” on page 427	Displays the settings and status of IGMP Snooping.

## ADD IGMPSNOOPING MCGROUP

---

### Syntax

```
add igmpsnooping mcgroup=ip_address [number=number]  
[routerport=port_list|all]
```

### Parameters

#### *mcgroup*

Specifies a multicast group IP address for IGMP Snooping. This IP address is the name of the multicast group and the starting IP address if you specify more than one IP address to the multicast group.

#### *ip\_address*

Specifies an IPv4 address.

#### *number*

Specifies the number of multicast addresses to add to the group. The range is 1 to 255 addresses. The default value is 1 address.

#### *routerport*

Specifies router ports. The router port is a port connected to the multicast router. When the port is on this port list, the switch adds a port as a router port when the port receives a Query packet.

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### *all*

Specifies all the switch ports.

### Description

Use this command to add a multicast group and specify router ports for the multicast group. The switch forwards traffic addressed to a multicast group only to the router port for the multicast group.

Here are the guidelines for adding a multicast group:

- ❑ The switch supports IGMP Versions 1, 2, and 3 Snooping except IGMP Version 3 Snooping Source Filtering.
- ❑ When an existing multicast group address is added, the command issues an error.
- ❑ The IP addresses mapped to the reserved MAC address 01-00-5e-00-00-*nn* cannot be used as multicast group addresses. For a list of the unavailable IP addresses, see Table 49 on page 419.

- ❑ The multicast group includes the specified number of IP addresses, starting from the IP address of the mcgroup and the sequence going up by 1.

A list of IP addresses unavailable to multicast groups is shown in Table 49.

Table 49. Unavailable IP Addresses for Multicast Groups

IP Address	Mapped MAC Address
224.0.0.0/24	01-00-5e-00-00- <i>nn</i>
224.128.0.0/24	
225.0.0.0/24	
225.128.0.0/24	
226.0.0.0/24	
226.128.0.0/24	
227.0.0.0/24	
227.128.0.0/24	
228.0.0.0/24	
228.128.0.0/24	
229.0.0.0/24	
229.128.0.0/24	
230.0.0.0/24	
230.128.0.0/24	
231.0.0.0/24	
231.128.0.0/24	
232.0.0.0/24	
232.128.0.0/24	
233.0.0.0/24	
233.128.0.0/24	
234.0.0.0/24	
234.128.0.0/24	
235.0.0.0/24	
235.128.0.0/24	

Table 49. Unavailable IP Addresses for Multicast Groups

IP Address	Mapped MAC Address
236.0.0.0/24	
236.128.0.0/24	
237.0.0.0/24	
237.128.0.0/24	
238.0.0.0/24	
238.128.0.0/24	
239.0.0.0/24	
239.128.0.0/24	

**Confirmation Command**

“SHOW IGMP Snooping” on page 427

**Example**

The following command creates a multicast group of 224.1.1.1 for IGMP Snooping:

```
Manager > add igmpsnooping mcgroup=224.1.1.1
```

## DELETE IGMPSNOOPING

---

### Syntax

```
delete igmpsnooping mcgroup=ip_add
```

### Parameters

mcgroup

Specifies an IP multicast group address.

### Description

Use this command to delete a static multicast group.

### Confirmation Command

“SHOW IGMPSNOOPING” on page 427

### Example

The following command deletes a multicast group, 224.1.1.1:

```
Manager > delete igmpsnooping mcgroup=224.1.1.1
```

## DISABLE IGMPSNOOPING

---

### Syntax

```
disable igmpsnooping
```

### Parameters

None

### Description

Use this command to disable IGMP Snooping. By default, IGMP Snooping is disabled.

### Confirmation Command

“SHOW IGMPSNOOPING” on page 427

### Example

The following command disables IGMP Snooping:

```
Manager > disable igmpsnooping
```

## ENABLE IGMPSNOOPING

---

### Syntax

```
enable igmpsnooping
```

### Parameters

None

### Description

Use this command to enable IGMP Snooping on the switch. By default, IGMP Snooping is disabled.

By default, the switch forwards multicast traffic to all ports belong to the same VLAN if any of the ports is a member of the multicast group. When IGMP Snooping is enabled, the switch snoops IGMP messages and forwards multicast traffic only to multicast member ports.

---

### Note

The switch does not support the source filtering function of IGMP version 3 Snooping.

---

### Confirmation Command

“SHOW IGMPSNOOPING” on page 427

### Example

The following command enables IGMP Snooping:

```
Manager > enable igmpsnooping
```

## SET IGMPSNOOPING

---

### Syntax

```
set igmpsnooping [timeout=timeout]  
[numbermulticastgroups=numbermulticastgroups]  
[routerport=port_list|all|none|auto] [force]
```

### Parameters

#### *timeout*

Specifies time in seconds. When the time passes since the last membership report, the switch deletes the multicast group. The range is 0 to 86400 seconds. The default value is 260 seconds.

#### *numbermulticastgroups*

Specifies the number of multicast groups that the switch can learn by IGMP Snooping. The range is 1 to 255. The default value is 64.

#### routerport

Specifies router ports or the method to determine router ports. The router port is a port connected to the multicast router. The switch adds a port as a router port when the port receives a Query packet only if the port is on this port list.

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### none

The switch discards query packets from the multicast router.

#### auto

The switch determines a port that receives a Query packet as a port for the multicast router. This is the default setting.

#### force

The setting of the routerport parameter affects all the multicast groups specified by the ADD IGMPSNOOPING MCGROUP command.

### Description

Use this command to specify the timeout and changes the settings of the multicast group.



By default, the switch forwards multicast traffic to all ports belong to the same VLAN if any of the ports is a member of the multicast group. When IGMP Snooping is enabled, the switch snoops IGMP messages and forwards multicast traffic only to multicast member ports.

Here are the guidelines for router ports:

- ❑ A router port is canceled when the port does not receive a query packet for the certain period of time; however, a router port is not canceled if the multicast group was added by the ADD IGMP Snooping MCGROUP command.
- ❑ When the routerport parameter is specified to none or auto, all multicast groups specified by the ADD IGMP Snooping MCGROUP command are deleted.

### **Confirmation Command**

“SHOW IGMP Snooping” on page 427

### **Example**

The following command sets the timeout for IGMP Snooping:

```
Manager > set igmpsnoping timeout=300
```

## SET IGMPSNOOPING MCGROUP

---

### Syntax

```
set igmpsnooping mcgroup=ip_address  
routerport=port_list|all
```

### Parameters

*mcgroup*

Specifies an IP multicast group address.

*routerport*

Specifies ports for router ports.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

*ip\_address*

Specifies an IPv4 address.

all

Specifies all the switch ports.

### Description

Use this command to change the router ports for multicast groups. You can change the router ports only for the multicast groups added statically by the ADD IGMPSNOOPING MCGROUP command.

### Confirmation Command

“SHOW IGMPSNOOPING” on page 427

### Example

The following command changes the router ports for the multicast group 224.1.1.1:

```
Manager > set igmpsnooping mcgroup=224.1.1.1 routerport=1
```

## SHOW IGMP Snooping

### Syntax

```
show igmpsnooping
```

### Parameters

None

### Description

Use this command to display the settings and status of IGMP Snooping. An example of the command output is shown in Figure 64.

```
IGMP Snooping Configuration:
IGMP Snooping Status ..... Enabled
Host/Router Timeout Interval ..... 260 seconds
Maximum IGMP Multicast Groups ..... 64 (2)
Router Port(s) ..... 1-3

IP Multicast Group Address ..... 224.1.1.1
Multicast MAC Address ..... 01-00-5e-01-01-01
Router Port(s) ..... 3

Host List:
Number of IGMP Multicast Groups: 2

MulticastGroup      VLAN  Port/      IGMP Exp.
                    ID      TrunkID   HostIP    Ver  Time
-----
01:00:5e:7f:ff:fa  1      Port 13   192.168.1.101    v2   187

Router List:
VLAN ID      Port/TrunkID      RouterIP
-----
1            Port 1            192.168.1.254
1            Port 3            192.168.2.200
```

Figure 64. SHOW IGMP Snooping Command

### Example

The following example displays the settings and status of IGMP Snooping:

```
Manager > show igmpsnooping
```



## Chapter 24

# Multicast Listener Discovery (MLD) Snooping Commands

---

The MLD Snooping commands are summarized in Table 50.

Table 50. MLD Snooping Commands

Command	Description
“ADD MLDSNOOPING MCGROUP” on page 430	Adds an IPv6 multicast group for MLD Snooping.
“DELETE MLDSNOOPING” on page 432	Deletes a static IPv6 multicast group address.
“DISABLE MLDSNOOPING” on page 433	Disables MLD Snooping.
“ENABLE MLDSNOOPING” on page 434	Enables MLD Snooping.
“SET MLDSNOOPING” on page 435	Specifies the timeout and changes the settings of the IPv6 multicast group.
“SET MLDSNOOPING MCGROUP” on page 437	Changes the router ports for the IPv6 multicast group.
“SHOW MLDSNOOPING” on page 439	Displays the settings and status of MLD Snooping.

## ADD MLDSNOOPING MCGROUP

---

### Syntax

```
add igmpsnooping mcgroup=ipv6_address
[routerport=port_list|all]
```

### Parameters

*mcgroup*

Specifies a multicast group IPv6 address for MLD Snooping. This IPv6 address is the name of the multicast group.

*ipv6\_address*

Specifies the IPv6 address of the multicast group.

Here are the guidelines for IPv6 multicast addresses.

- Specify an IPv6 address in the full format `ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` or the zero compressed format.

For example, an IPv6 address of

`ff05:0000:0001:0000:0000:0000:0000:0101` in the full format is `ff05:0:1::101` in the zero compressed format.

- The first two most significant bits must be “ff” to be a multicast address.
- The range of 112-bit group IDs for the IPv6 address is shown in Table 51 on page 431.

*routerport*

Specifies router ports. The router port is a port connected to the IPv6 multicast router. The switch adds a port as a router port when the port receives a Query packet only if the port is on this port list.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

*all*

Specifies all the switch ports.

### Description

Use this command to add a multicast group for MLD Snooping. The switch forwards traffic addressed to an IPv6 multicast group only to the router port for the multicast group.

Here are the guidelines for adding a multicast group:

- ❑ When an existing multicast group IPv6 address is added, the command issues an error.
- ❑ The destination MAC address for the IPv6 multicast traffic is copied from the least significant 32 bits of the IPv6 multicast address.
- ❑ The range of available group IDs are shown in Table 51.

Table 51. Unavailable Group ID for Multicast Group

<b>Group ID (ffff:ffff:ffff:ffff:ffff:ffff:WWXX:YYZZ)</b>	<b>Available Group ID</b>
<i>WW</i>	00 to fe
<i>XX</i>	03 to ff
<i>YY</i>	00 to ff
<i>ZZ</i>	00 to ff

- ❑ When a port with the smallest port number in a trunk group is disabled by the DISABLE SWITCH PORT command, the other ports in the trunk group do not forward multicast traffic. You can work around this issue by running the DISABLE SWITCH PORT command specifying the link parameter with the disable option.
- ❑ To specify a trunk port as a router port, you must specify all the member ports of the trunk group as router ports.

### Confirmation Command

“SHOW MLDSNOOPING” on page 439

### Example

The following command adds an IPv6 multicast group for MLD Snooping:

```
Manager > add mldsnooping
mcgroup=ff02:2310:1020:3131:4312:5515:fe11:ffff
```

## DELETE MLDSNOOPING

---

### Syntax

```
delete mld Snooping mcgroup=ip6_address
```

### Parameters

*mcgroup*

Specifies an IPv6 multicast group address.

*ip6\_address*

Specifies the IPv6 address of the multicast group.

Here is the guidelines for IPv6 multicast addresses.

- Specify an IPv6 address in the full format *ff ff: ffff: ffff: ffff: ffff: ffff: ffff: ffff* or the zero compressed format.

For example, an IPv6 address of

*ff05:0000:0001:0000:0000:0000:0101* in the full format is *ff05:0:1::101* in the zero compressed format.

- The first two most significant bits must be “ff” to be a multicast address.
- The range of 112-bit group IDs for the IPv6 address is shown in Table 51 on page 431.

### Description

Use this command to delete a static IPv6 multicast group address.

### Confirmation Command

“SHOW MLDSNOOPING” on page 439

### Example

The following command deletes an IPv6 multicast group address, *ff05:0:1::101*:

```
Manager > delete mld Snooping mcgroup=ff05:0:1::101
```



## DISABLE MLDSNOOPING

---

### Syntax

```
disable mld Snooping
```

### Parameters

None

### Description

Use this command to disable MLD Snooping. By default, MLD Snooping is disabled.

### Confirmation Command

“SHOW MLDSNOOPING” on page 439

### Example

The following command disables MLD Snooping:

```
Manager > disable mld Snooping
```

## ENABLE MLDSNOOPING

---

### Syntax

```
enable mldsnooping
```

### Parameters

None

### Description

Use this command to enable Multicast Listener Discovery (MLD) Snooping on the switch. The switch supports MLD versions 1 and 2 Snooping. By default, MLD Snooping is disabled.

When MLD Snooping is disabled, the switch forwards IPv6 multicast traffic to all ports belong to the same VLAN if any of the ports is a member of the multicast group. When MLD Snooping is enabled, the switch snoops MLD messages and forwards IPv6 multicast traffic only to multicast member ports.

---

### Note

The switch does not support the source filtering function of MLD version 2 Snooping.

---

### Confirmation Command

“SHOW MLDSNOOPING” on page 439

### Example

The following command enables MLD Snooping:

```
Manager > enable mldsnooping
```

## SET MLDSNOOPING

---

### Syntax

```
set mld Snooping [timeout=timeout]
[numbermulticastgroups=numbermulticastgroups]
[routerport=port_list|all|none|auto] [force]
```

### Parameters

#### *timeout*

Specifies time in seconds. When the time passes since the last membership report, the switch deletes the multicast group. The range is 0 to 86400 seconds. The default value is 260 seconds.

#### *numbermulticastgroups*

Specifies the number of multicast groups that the switch can learn by MLD Snooping. The range is 1 to 255. The default value is 64.

The switch can learn total 255 multicast groups both for MLD Snooping and IGMP Snooping.

#### *routerport*

Specifies router ports or the method to determine router ports. The router port is a port connected to the multicast router. When a list of ports are specified, the switch does not add a port that receives a Query packets as a port for the multicast port if the port is not on the specified list.

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies all the switch ports.

#### none

Specifies none. The switch discards query packets from the multicast router.

#### auto

Specifies auto. The switch determines a port that receives a Query packet as a port for the multicast router. This is the default setting.

#### force

The setting of the routerport parameter affects all the multicast groups specified by the ADD MLDSNOOPING MCGROUP command.

## Description

Use this command to specify the timeout and changes the settings of the multicast group for MLD Snooping.

By default, the switch forwards multicast traffic to all ports belong to the same VLAN if any of the ports is a member of the multicast group. When MLD Snooping is enabled, the switch snoops MLD messages and forwards multicast traffic only to multicast member ports.

Here are the guidelines for router ports:

- ❑ A router port is canceled when the port does not receive a query packet for the certain period of time; however, a router port is not canceled if the multicast group was added by the ADD MLD SNOOPING MCGROUP command.
- ❑ When the routerport paramter is specified to none or auto, all multicast groups specified by the ADD MLDSNOOPING MCGROUP command are deleted.

## Confirmation Command

“SHOW MLDSNOOPING” on page 439

## Example

The following command sets the timeout for MLD Snooping:

```
Manager > set mld Snooping timeout=300
```

## SET MLDSNOOPING MCGROUP

---

### Syntax

```
set mld Snooping mcgroup=ip_add routerport=port_list|all
```

### Parameters

*mcgroup*

Specifies an IPv6 multicast group address.

*ipv6\_address*

Specifies the IPv6 address of the multicast group.

Here are the guidelines for IPv6 multicast addresses.

- Specify an IPv6 address in the full format *ff ff: ffff: ffff: ffff: ffff: ffff: ffff: ffff* or the zero compressed format.

For example, an IPv6 address of

*ff05:0000:0001:0000:0000:0000:0000:0101* in the full format is *ff05:0:1::101* in the zero compressed format.

- The first two most significant bits must be “ff” to be a multicast address.
- The range of 112-bit group IDs for the IPv6 address is shown in Table 51 on page 431.

*routerport*

Specifies ports for router ports.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

*all*

Specifies all the switch ports.

### Description

Use this command to change the router ports for IPv6 multicast groups. You can change the router ports only for the multicast groups added statically by the ADD MLDSNOOPING MCGROUP command.

### Confirmation Command

“SHOW MLDSNOOPING” on page 439

### **Example**

The following command changes the router ports for the multicast group ff05:0:1::101 :

```
Manager > set mldsnooping mcgroup=ff05:0:1::101  
routerport=1-3
```

## SHOW MLDSNOOPING

---

### Syntax

```
show mld Snooping
```

### Parameters

None

### Description

Use this command to display the settings and status of MLD Snooping. An example of the command output is shown in Figure 65.

```

MLD Snooping Configuration:
MLD Snooping Status ..... Enabled
Host/Router Timeout Interval ..... 260 seconds
Maximum MLD Multicast Groups ..... 64 (1)
Router Port(s) ..... 1-3

IPv6 Multicast Group Address ..... ff05:0:1::101
Multicast MAC Address ..... 33-33-00-00-01-01
Router Port(s) ..... 1

Router List:
VLAN ID      Port/TrunkID      RouterIP
-----
Host List:
Number of MLD Multicast Groups: 0

MulticastGroup      VLAN ID      Port/TrunkID      HostIP      Exp Time
-----
```

Figure 65. SHOW MLDSNOOPING Command

### Example

The following example displays the settings and status of MLD Snooping:

```
Manager > show mld Snooping
```





## Chapter 25

# Quality of Service (QoS) Commands

The QoS commands are summarized in Table 52.

Table 52. QoS Commands

Command	Description
“DISABLE QOS” on page 442	Sets the switch to prioritize forwarding performance over Quality of Service (QoS).
“ENABLE QOS” on page 443	Sets the switch to prioritize Quality of Service (QoS) over forwarding performance.
“PURGE QOS” on page 444	Initializes QoS settings.
“SET QOS DSCP” on page 445	Changes the DSCP table.
“SET QOS HWPRIORITY” on page 446	Changes the QoS priority map.
“SET QOS HWQUEUE” on page 448	Changes the weight ratio to the queue.
“SET QOS SCHEDULING” on page 449	Changes the QoS scheduling method.
“SHOW QOS” on page 450	Displays the QoS settings on the switch.
“SHOW QOS DSCP” on page 451	Displays the DSCP table on the switch.
“SHOW QOS HWPRIORITY” on page 452	Displays the QoS priority mapping table on the switch.
“SHOW QOS HWQUEUE” on page 453	Displays the settings of queue weight on the switch.
“SHOW QOS SCHEDULING” on page 454	Displays the settings of QoS scheduling on the switch.

## DISABLE QOS

---

### Syntax

```
disable qos
```

### Parameters

None

### Description

Use this command to set the switch to prioritize forwarding performance over Quality of Service (QoS). This is the default setting.

### Confirmation Command

“SHOW QOS” on page 450

### Example

The following command sets the switch to prioritize forwarding performance:

```
Manager > disable qos
```

# ENABLE QOS

---

## Syntax

```
enable qos
```

## Parameters

None

## Description

Use this command to set the switch to prioritize Quality of Service (QoS) over forwarding performance. By default, the switch prioritizes forwarding performance over QoS.

---

### Note

You must restart the switch after executing this command.

---

QoS does *not* control the following UDP's:

- DVMRP packets when IGMP Snooping is enabled
- VSRP packets when STP/MSTP or EPSR is enabled
- Received LDF when Loop Detection is enabled

## Confirmation Command

"SHOW QOS" on page 450

## Example

The following command sets the switch to prioritize Quality of Service (QoS) over forwarding performance:

```
Manager > enable qos
```

## **PURGE QOS**

---

### **Syntax**

purge qos

### **Parameters**

None

### **Description**

Use this command to initialize QoS settings.

### **Confirmation Command**

“SHOW QOS” on page 450

### **Example**

The following command initializes QoS settings:

```
Manager > purge qos
```

## SET QOS DSCP

---

### Syntax

```
set qos dscp==dscp_list[all] priority=priority
```

### Parameters

*dscp\_list*

Specifies a list of the values of DiffServ Code Point (DSCP). To specify multiple values, use a comma (,) to separate them. To specify a range of values, use a hyphen (-).

all

Specifies all values from 0 to 63.

*priority*

Specifies a user priority. The range is 0 to 7. The default value is 0.

### Description

Use this command to change the DSCP table.

### Confirmation Command

“SHOW QOS DSCP” on page 451

### Example

The following command changes the DSCP table to DSCP 0 to 3:

```
Manager > set qos dscp=0-3 priority=1
```

## SET QOS HWPRIORITY

---

### Syntax

```
set qos hwpriority queue=p0,p1,p2,p3,p4,p5,p6,p7
```

### Parameters

#### queue

Specifies a list of the values of DiffServ Code Point (DSCP). To specify multiple values, use a comma (,) to separate them. To specify a range of values, use a hyphen (-).

#### *p0,p1,p2,p3,p4,p5,p6,p7*

Specifies queue numbers for the user priorities, 0 to 7. Queue numbers are 0 to 3. The highest priority queue is 3. See Table 53 for the default settings.

### Description

Use this command to change the QoS priority map.

The default settings of the QoS priority map is shown in Table 53.

Table 53. Default QoS Priority Map

Priority	Queue Number
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

### Confirmation Command

“SHOW QOS HWPRIORITY” on page 452

**Example**

The following command change QoS priority settings:

```
Manager > set qos hwpriority queue=0,0,0,1,1,2,2,3
```

## SET QOS HWQUEUE

---

### Syntax

```
set qos hwqueue=queue weight=weight
```

### Parameters

*queue*

Specifies a queue number. The range is 0 to 3.

*weight*

Specifies the weight ratio to the queue. See Table 54 for the default settings.

### Description

Use this command to change the weight ratio to the queue.

The default settings of the priority queue ratio is shown in Table 54.

Table 54. Default Priority Queue Ratio

Queue Number	Weight Ratio
0	1
1	4
2	10
3	15

### Confirmation Command

“SHOW QOS HWQUEUE” on page 453

### Example

The following command change the weight ratio on queue 0 to 2:

```
Manager > set qos hwqueue=0 weight=2
```



## SET QOS SCHEDULING

---

### Syntax

```
set qos scheduling=strict|wrr [mode=auto|802.1p]
```

### Parameters

#### scheduling

Specifies the QoS scheduling method.

#### strict

Specifies QoS to the strict method. The switch forwards packets in descending order of queue priority.

#### wrr

Specifies QoS to the WRR method. The switch forwards packets with the Weighted Round Robin (WRR) method. This is the default setting.

#### auto

Specifies the QoS mode to auto. The priority is based on the DSCP value, IEEE802.1p compliant priority tag, port priority in descending order. This is the default setting.

#### 802.1p

Specifies the QoS mode to 802.1p. The priority is based on the IEEE802.1p compliant priority tag.

### Description

Use this command to change the QoS scheduling method.

### Confirmation Command

“SHOW QOS SCHEDULING” on page 454

### Example

The following command change the QoS scheduling to the strict method and 802.1p mode:

```
Manager > set qos scheduling=strict mode=802.1p
```

# SHOW QOS

---

### Syntax

show qos

### Parameters

None

### Description

Use this command to display the QoS settings on the switch. An example of the command output is shown in Figure 66.

```
QoS Information
-----
Configured State ..... Disabled
Actual State ..... Disabled
Mode ..... Auto
Scheduling ..... Weighted Round-Robin
-----
```

Figure 66. SHOW QOS Command

### Example

The following example displays information about QoS settings:

```
Manager > show qos
```

## SHOW QOS DSCP

### Syntax

```
show qos dscp
```

### Parameters

None

### Description

Use this command to display the DiffServ Code Point (DSCP) table on the switch. An example of the command output is shown in Figure 67.

QoS DSCP Table							
DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0	16	0	32	0	48	0
1	0	17	0	33	0	49	0
2	0	18	0	34	0	50	0
3	0	19	0	35	0	51	0
4	0	20	0	36	0	52	0
5	0	21	0	37	0	53	0
6	0	22	0	38	0	54	0
7	0	23	0	39	0	55	0
8	0	24	0	40	0	56	0
9	0	25	0	41	0	57	0
10	0	26	0	42	0	58	0
11	0	27	0	43	0	59	0
12	0	28	0	44	0	60	0
13	0	29	0	45	0	61	0
14	0	30	0	46	0	62	0
15	0	31	0	47	0	63	0

Figure 67. SHOW QOS DSCP Command

### Example

The following example displays the DSCP table:

```
Manager > show qos dscp
```

## SHOW QOS HWPRIORITY

---

### Syntax

```
show qos hwpriority
```

### Parameters

None

### Description

Use this command to display the QoS priority mapping table on the switch. An example of the command output is shown in Figure 68.

Priority	Queue
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Figure 68. SHOW QOS HWPRIORITY Command

### Example

The following example displays the QoS priority mapping table:

```
Manager > show qos hwpriority
```

## SHOW QOS HWQUEUE

---

### Syntax

```
show qos hwqueue
```

### Parameters

None

### Description

Use this command to display the settings of queue weight on the switch. An example of the command output is shown in Figure 69.

Queue	weight
0	1
1	4
2	10
3	15

Figure 69. SHOW QOS HWQUEUE Command

### Example

The following example displays the settings of queue weight:

```
Manager > show qos hwqueue
```

## SHOW QOS SCHEDULING

---

### Syntax

```
show qos scheduling
```

### Parameters

None

### Description

Use this command to display the settings of QoS scheduling on the switch. An example of the command output is shown in Figure 70.

```
QoS Scheduling Mode
-----
Mode ..... 802.1p
Scheduling ..... Weighted Round-Robin
-----
```

Figure 70. SHOW QOS SCHEDULING Command

### Example

The following example displays the settings of QoS scheduling on the switch:

```
Manager > show qos scheduling
```

## Chapter 26

# Policy-Based QoS Commands

The Policy-based QoS commands are summarized in Table 55.

Table 55. Policy-Based QoS Commands

Command	Description
“ADD QOS FLOWGROUP” on page 457	Associates classifiers to a flow group.
“ADD QOS POLICY” on page 458	Associates traffic classes to a QoS policy.
“ADD QOS TRAFFICCLASS” on page 459	Associates flow groups to a traffic class.
“CREATE CLASSIFIER” on page 460	Creates a classifier.
“CREATE QOS FLOWGROUP” on page 463	Creates a flow group.
“CREATE QOS POLICY” on page 465	Creates a QoS policy.
“CREATE QOS TRAFFICCLASS” on page 468	Creates a traffic class.
“DELETE QOS FLOWGROUP” on page 471	Removes a classifier from the flow group.
“DELETE QOS POLICY” on page 472	Removes a traffic class from the QoS policy.
“DELETE QOS TRAFFICCLASS” on page 473	Removes a flow group from the traffic class.
“DESTROY CLASSIFIER” on page 474	Deletes classifiers.
“DESTROY QOS FLOWGROUP” on page 475	Deletes flow groups.
“DESTROY QOS POLICY” on page 476	Deletes QoS policies.
“DESTROY QOS TRAFFICCLASS” on page 477	Deletes traffic classes.

Table 55. Policy-Based QoS Commands (Continued)

Command	Description
"PURGE CLASSIFIER" on page 478	Deletes all classifiers.
"RESET QOS POLICY COUNTER" on page 479	Clears the counters of the flow groups assigned to the QoS policies.
"SET CLASSIFIER" on page 480	Changes the settings of the classifier.
"SET QOS FLOWGROUP" on page 483	Changes the settings of the flow group.
"SET QOS POLICY" on page 485	Changes the settings of the QoS policy.
"SET QOS TRAFFICCLASS" on page 487	Changes the settings of the traffic class.
"SHOW CLASSIFIER" on page 489	Displays the settings of classifiers.
"SHOW QOS FLOWGROUP" on page 493	Displays the settings of flow groups.
"SHOW QOS POLICY" on page 494	Displays the settings of QoS policies.
"SHOW QOS POLICY COUNTER" on page 495	Displays the counters of the classifiers.
"SHOW QOS TRAFFICCLASS" on page 496	Displays the settings of traffic classes.



## ADD QOS FLOWGROUP

---

### Syntax

```
add qos flowgroup=flowgroup_number  
classifierlist=classifier_list|none
```

### Parameters

*flowgroup\_number*

Specifies a flow group number. The range is 0 to 1023.

*classifier\_list*

Specifies a list of classifiers. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-).

### Description

Use this command to associate classifiers to the flow group.

### Confirmation Command

“SHOW QOS FLOWGROUP” on page 493

### Example

The following command adds classifiers 1, 2, and 3 to flow group 1:

```
Manager > add qos flowgroup=1 classifierlist=1,2,3
```

## ADD QOS POLICY

---

### Syntax

```
add qos policy=policy_number trafficclasslist=tc_list|none
```

### Parameters

*policy\_number*

Specifies a QoS policy number. The range is 0 to 255.

*tc\_list*

Specifies a list of classifiers. To specify multiple traffic classes, use a comma (,) to separate them. To specify a range of traffic classes, use a hyphen (-).

### Description

Use this command to associate traffic classes to a QoS policy.

### Confirmation Command

“SHOW QOS POLICY” on page 494

### Example

The following command adds traffic classes 1, 2, and 3 to QoS policy 1:

```
Manager > add qos policy=1 traffcclasslist=1-3
```

## ADD QOS TRAFFICCLASS

---

### Syntax

```
add qos trafficclass=traffic_class_number  
flowgrouplist=flow_list|none
```

### Parameters

*traffic\_class\_number*

Specifies a traffic class number. The range is 0 to 511.

*flow\_list*

Specifies a list of flow groups. To specify multiple flow groups, use a comma (,) to separate them. To specify a range of flow groups, use a hyphen (-).

### Description

Use this command to associate flow groups to a traffic class.

### Confirmation Command

“SHOW QOS TRAFFICCLASS” on page 496

### Example

The following command associates flow groups 1 and 2 to traffic class 1:

```
Manager > add qos trafficclass=1 flowgrouplist=1-3
```

## CREATE CLASSIFIER

---

### Syntax

```
create classifier=classifier_number [description=string]
[macdaddr=mac_add|any] [macdmask=mac_add|any]
[macsaddr=mac_add|any] [macsmask=mac_add|any]
[ethformat=ethii-untagged|ethii-tagged|802.2-untagged|
802.2-tagged|any] [priority=priority|any]
[vlan=vlan_name|vid|any]
[protocol=protocol_string|protocol_number|any]
[iptos=iptos|any] [ipdscp=ipdscp|any]
[ipprotocol=ipprotocol_string|ipprotocol_number|any]
[ipdaddr=ipadd/mask_len|any] [ipsaddr=ipadd/mask_len|any]
[tcpsport=tcpsport|any] [tcpdport=tcpdport|any]
[udpsport=udpsport|any] [udpport=udpport|any]
[tcpflags=urg|ack|psh|rst|syn|fin|any]
```

### Parameters

#### *classifier\_number*

Specifies a classifier number. The range is 1 to 9999.

#### *string*

Specifies the description of the classifier. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

#### macdaddr

Specifies the MAC destination address of packets. The default value is any.

#### macdmask

Specifies the mask for the MAC destination address of packets. The default value is any.

#### macsaddr

Specifies the MAC source address of packets. The default value is any.

#### macsmask

Specifies the mask for the MAC destination address of packets. The default value is any.

#### *mac\_add*

Specifies a MAC address or mask in the format: *ff-ff-ff-ff-ff*.

#### any

Specifies any.

*ethformat*

Specifies the frame format.

*ethii-untagged*

Specifies the frame format to Ethernet version 2 and untagged.

*ethii-tagged*

Specifies the frame format to Ethernet version 2 and tagged.

*802.2-untagged*

Specifies the frame format to 802.2 LLC and untagged.

*802.2-tagged*

Specifies the frame format to 802.2 LLC and tagged.

*priority*

Specifies a priority. The range is 0 to 7. The default setting is none.

*vlan\_name*

Specifies a VLAN name.

*vid*

Specifies a VLAN ID. The range is 1 to 4094.

*protocol*

Specifies the value of the protocol field in the packet with the protocol number. For the IP, ARP, or RARP protocol, you can specify this parameter with the protocol name. The default setting is any.

*iptos*

Specifies the value of the precedence in the ToS octet in the packet. The range is 0 to 7. The default setting is any.

*ipdscp*

Specifies the value of the IP DSCP field. The range is 0 to 63. The default setting is any.

*ipprotocol*

Specifies the value of the IP protocol field in the packet with the protocol number. For the TCP, UDP, ICMP, and IGMP protocol, you can specify this parameter with the protocol name. The default setting is any.

*ipsaddr*

Specifies the IP source address. You can also specify the Variable Length Subnet Mask (VLSM). The default value is any.

*ipdaddr*

Specifies the IP destination address. You can also specify the Variable Length Subnet Mask (VLSM). The default value is any.

*ip\_addr*

Specifies an IP address in the format: *nnn.nnn.nnn.nnn*.

*mask\_len*

Specifies a VLSM after the IP address. Separate the IP address and VLSM with a slash(/).

*tcpport*

Specifies the TCP source port of packets. The range is 0 to 65535. The default setting is any.

*tcpdport*

Specifies the TCP destination port of packets. The range is 0 to 65535. The default setting is any.

*udpport*

Specifies the UDP source port of packets. The range is 0 to 65535. The default setting is any.

*udpport*

Specifies the UDP destination port of packets. The range is 0 to 65535. The default setting is any.

## tcpflags

Specifies the flag in the TCP header. The options are urg, ack, psh, rst, syn, and fin. QoS filters a packet in which only the specified flag in the TCP header is on. The default setting is any.

**Description**

Use this command to create a classifier. The classifier defines criteria in order to filter traffic. Classifiers are assigned to a flow group.

Here are the guidelines for creating a flow group:

- You cannot use the *iptos* and *ipdscp* parameters at the same time.
- When the *tcpport* and *tcpdport* parameters are specified, you cannot use the *udpport* and *udpport* parameters.
- When the *iptos*, *ipdscp*, *ipprotocol*, *ipdaddr*, or *ipsaddr* parameter is specified, the protocol parameter is automatically set to ip.

**Confirmation Command**

“SHOW CLASSIFIER” on page 489

**Example**

The following command creates classifier 10:

```
Manager > create classifier=10 ipdaddr=192.168.10.0/24
```

## CREATE QOS FLOWGROUP

---

### Syntax

```
create qos flowgroup=flow_group_number [description=string]
[markvalue=mark_value|none] [priority=priority|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=tos_value|none]
[movetostoppriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[classifierlist=classifier_list|none]
```

### Parameters

*flow\_group\_number*

Specifies a flow group number. The range is 0 to 1023.

*string*

Specifies the description of the flow group. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

*mark\_value*

Specifies a value to be written in the DSCP field of the IP header. The range is 0 to 63. This value has a priority over the markvalue of the traffic class and the indscpoverwrite of the policy. The default setting is none.

*priority*

Specifies a priority. The range is 0 to 7. The default setting is none.

remarkpriority

Specifies yes, no, or none to the state that the priority of the flow group overwrites the user priority in the packet. The default setting is none.

yes, on, true

Specifies yes to the parameter state.

no, off, false

Specifies no to the parameter state.

*tos\_value*

Specifies a value for the ToS field of the IP header.

movetostoppriority

Specifies yes, no, or none to the state that the ToS value of the IP header is used to determine the priority. The default setting is none.

**moveprioritytos**

Specifies yes, no, or none to the state that the priority is used for the ToS value. The default setting is none.

**classifier\_list**

Specifies a list of classifiers. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-). The default setting is none.

**Description**

Use this command to create a flow group. You can assign flow groups to the traffic group to define more detailed traffic. The flow group consists of classifiers.

Here are the guidelines for creating a flow group:

- The markvalue parameter of the flow group has higher priority over the makrvalue parameter of the traffic class and indscpoverwrite parameter of the policy.
- The markvalue and tos parameters cannot be used concurrently.
- The markvalue and moveprioritytos parameters cannot be used concurrently.
- The tos and moveprioritytos parameters cannot be used concurrently.

**Confirmation Command**

“SHOW QOS FLOWGROUP” on page 493

**Example**

The following command creates flow group 1:

```
Manager > create qos flowgroup=1
```



## CREATE QOS POLICY

---

### Syntax

```
create qos policy=policy_number [description=string]
[indscpoverwrite=dscp_value|none] [remarkindscp=all|none]
[tos=tos_value|none]
[movetostoppriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[sendtomirror=yes|no|on|off|true|false]
[trafficclasslist=traffic_class_list|none]
[redirectport=port_number|none]
[ingressport=port_list|all|none]
[egressport=port_number|none]
```

### Parameters

*policy\_number*

Specifies a policy number. The range is 0 to 255.

*string*

Specifies the description of the policy. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

*dscp\_value*

Specifies a value to be written in the DSCP field of the IP header. The range is 0 to 63. The default setting is none.

remarkindscp

Specifies all or none to the state that the value of the indscpoverwrite parameter overwrites the DSCP field of the IP header. The default setting is none.

*tos\_value*

Specifies a value for the ToS field of the IP header.

movetostoppriority

Specifies yes, no, or none to the state that the ToS value of the IP header is used to determine the priority. The default setting is none.

moveprioritytotos

Specifies yes, no, or none to the state that the priority is used for the ToS value. The default setting is none.

yes, on, true

Yes to the parameter state.

no, off, false

Specifies no to the parameter state.

`sendtomirror`

Specifies yes, no, or none to the state that mirroring is enabled on the packets that match the conditions of the classifiers. The default setting is none.

`trafficclasslist`

Specifies a list of traffic classes. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-). The default setting is none.

`redirectport`

Specifies a port number to the traffic is forwarded from.

*port\_number*

Specifies a port number.

`ingressport`

Specifies a list of input ports that the QoS policy is applied to. The port can be an ingressport to only one QoS policy. The default setting is none.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

`all`

Specifies all the switch ports.

`egressport`

Specifies an input port that the QoS policy is applied to. The port can be an egressport to only one QoS policy. The default setting is none.

## Description

Use this command to create a QoS policy. You can prioritize network traffic with QoS policies to control bandwidth usage. The QoS policy consists of traffic classes and is applied to switch ports.

Here are the guidelines for creating a QoS policy:

- ❑ The `markvalue` parameter of the flow group has higher priority over the `markvalue` parameter of the traffic class and `indscpoverwrite` parameter of the policy.
- ❑ The `tos` and `moveprioritytotos` parameters cannot be used concurrently.
- ❑ The `CREATE QOS POLICY` command cannot be used when DCHP Snooping is enabled.

**Confirmation Command**

“SHOW QOS POLICY” on page 494

**Example**

The following command creates QoS policy 1:

```
Manager > create qos policy=1
```

## CREATE QOS TRAFFICCLASS

---

### Syntax

```
create qos trafficclass=traffic_class [description=string]
[exceedaction=drop|remark]
[exceedremarkvalue=remark_value|none]
[markvalue=mark_value|none]
[maxbandwidth=max_bandwidth|none]
[burstsize=burst_size|none] [priority=priority|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=tos_value|none]
[movetostoppriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[flowgrouplist=flow_list|none]
```

### Parameters

*traffic\_class*

Specifies a policy number. The range is 0 to 511.

*string*

Specifies the description of the traffic class. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

*exceedaction*

Specifies an action when the bandwidth for the traffic class is exceeded. is 0 to 63.

*drop*

The switch discards the packet. This is the default setting.

*remark*

The switch overwrites the value of the DSCP field in the IP header with the value of the *exceedremarkvalue* parameter and forwards the packet.

*remark\_value*

Specifies a value to be written in the DSCP field of the IP header when the bandwidth for the traffic class is exceeded. The range is 0 to 63. The default setting is none.

*mark\_value*

Specifies a value to be written in the DSCP field of the IP header. The range is 0 to 63. The default setting is none.

*max\_bandwidth*

Specifies the maximum bandwidth of the traffic class in Mbps. The range is 0 to 1016 Mbps. The default setting is none.

*burst\_size*

Specifies the buffer size, or token packet size of the traffic class. This value is effective when the maximum bandwidth is specified. The range is 4 to 512 Kbps. The default setting is none.

*priority*

Specifies the priority for the traffic class.

## remarkpriority

Specifies yes, no, or none to the state that the switch overwrites the user priority of a received packet with the priority. The default setting is none.

*tos\_value*

Specifies a value for the ToS field of the IP header.

## movetostopriority

Specifies yes, no, or none to the state that the ToS value of the IP header is used to determine the priority. The default setting is none.

## moveprioritytotos

Specifies yes, no, or none to the state that the priority is used for the ToS value. The default setting is none.

## yes, on, true

Yes to the parameter state.

## no, off, false

No to the parameter state.

flowgroup`list`

Specifies a list of flow groups. To specify multiple flow groups, use a comma (,) to separate them. To specify a range of flow groups, use a hyphen (-). The default setting is none.

**Description**

Use this command to create a traffic class. The traffic group collects flow groups to assign the same bandwidth.

Here are the guidelines for creating a flow group:

- The markvalue parameter of the flow group has higher priority over the makrvalue parameter of the traffic class and indscpoverwrite parameter of the policy.
- The markvalue and moveprioritytotos parameters cannot be used concurrently.
- The maxbandwidth parameter cannot be used when the exceedaction parameter is set to remark.

### **Confirmation Command**

“SHOW QOS TRAFFICCLASS” on page 496

### **Example**

The following command creates traffic class1:

```
Manager > create qos trafficclass=1
```

## DELETE QOS FLOWGROUP

---

### Syntax

```
delete qos flowgroup=flow_group_number  
classifierlist=classifier_list|none
```

### Parameters

*flow\_group\_number*

Specifies a flow group number.

*classifier\_list*

Specifies a list of classifiers. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-). The default setting is none.

### Description

Use this command to remove a classifier from the flow group.

### Confirmation Command

“SHOW QOS FLOWGROUP” on page 493

### Example

The following command deletes classifiers 1 to 3 from flow group 1:

```
Manager > delete qos flowgroup=1 classifierlist=1-3
```

## DELETE QOS POLICY

---

### Syntax

```
delete qos policy=policy_number  
[trafficclasslist=traffic_class_list|none]
```

### Parameters

*policy\_number*

Specifies a policy number.

*trafficclasslist*

Specifies a list of traffic classes. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-). The default setting is none.

### Description

Use this command to remove a traffic class from the QoS policy.

### Confirmation Command

“SHOW QOS POLICY” on page 494

### Example

The following command deletes traffic classes 1 to 3 from QoS policy 1:

```
Manager > delete qos policy=1 trafficclasslist=1-3
```



## DELETE QOS TRAFFICCLASS

---

### Syntax

```
delete qos trafficclass=traffic_class  
[flowgrouplist=flow_list|none]
```

### Parameters

*traffic\_class*

Specifies a policy number.

flowgroup~~list~~

Specifies a list of flow groups. To specify multiple flow groups, use a comma (,) to separate them. To specify a range of flow groups, use a hyphen (-). The default setting is none.

### Description

Use this command to remove a flow group from the traffic class.

### Confirmation Command

“SHOW QOS TRAFFICCLASS” on page 496

### Example

The following command deletes flow groups 1 to 3 from traffic class 1:

```
Manager > delete qos trafficclass=1 flowgrouplist=1-3
```

## DESTROY CLASSIFIER

---

### Syntax

```
destroy classifier==classifier_list|all
```

### Parameters

*classifier\_list*

Specifies a list of classifiers. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-).

all

Specifies all classifiers.

### Description

Use this command to delete classifiers. The classifiers assigned to QoS policies cannot be deleted.

### Confirmation Command

“SHOW CLASSIFIER” on page 489

### Example

The following command deletes classifier 10:

```
Manager > destroy classifier=10
```

## DESTROY QOS FLOWGROUP

---

### Syntax

```
destroy qos flowgroup=flow_group_list|all
```

### Parameters

*flow\_group\_list*

Specifies a list of flow groups. To specify multiple flow groups, use a comma (,) to separate them. To specify a range of flow groups, use a hyphen (-).

all

Specifies all flow groups.

### Description

Use this command to delete flow groups.

### Confirmation Command

“SHOW QOS FLOWGROUP” on page 493

### Example

The following command deletes flow group 1:

```
Manager > destroy qos flowgroup=1
```

## DESTROY QOS POLICY

---

### Syntax

```
destroy qos policy=policy_list|all
```

### Parameters

*policy\_list*

Specifies a list of policy numbers. To specify multiple QoS policies, use a comma (,) to separate them. To specify a range of QoS policies, use a hyphen (-).

### Description

Use this command to delete QoS policies.

### Confirmation Command

“SHOW QOS POLICY” on page 494

### Example

The following command deletes QoS policy 1:

```
Manager > destroy qos policy=1
```

## DESTROY QOS TRAFFICCLASS

---

### Syntax

```
destroy qos trafficclass=traffic_class_list|all
```

### Parameters

*traffic\_class\_list*

Specifies a list of traffic classes. To specify multiple traffic classes, use a comma (,) to separate them. To specify a range of traffic classes, use a hyphen (-).

### Description

Use this command to delete traffic classes.

### Confirmation Command

“SHOW QOS TRAFFICCLASS” on page 496

### Example

The following command deletes traffic class 1:

```
Manager > destroy qos trafficclass=1
```

## **PURGE CLASSIFIER**

---

### **Syntax**

```
purge classifier
```

### **Parameters**

None

### **Description**

Use this command to delete all classifiers. When some classifiers are assigned to QoS policies, you cannot delete classifiers with this command.

### **Confirmation Command**

“SHOW CLASSIFIER” on page 489

### **Example**

The following command deletes all classifiers:

```
Manager > purge classifier
```

## RESET QOS POLICY COUNTER

---

### Syntax

```
reset qos policy[=policy_list|all] counter
```

### Parameters

*policy\_list*

Specifies a list of policy numbers. To specify multiple QoS policies, use a comma (,) to separate them. To specify a range of QoS policies, use a hyphen (-).

### Description

Use this command to clear the counters of the flow groups assigned to the QoS policies.

### Confirmation Command

“SHOW QOS POLICY COUNTER” on page 495

### Example

The following command clears the counters of the flow groups assigned to QoS policy 1:

```
Manager > reset qos policy=1 counter
```

## SET CLASSIFIER

---

### Syntax

```
set classifier=classifier_number [description=string]
[macdaddr=mac_add|any] [macdmask=mac_add|any]
[macsaddr=mac_add|any] [macsmask=mac_add|any]
[ethformat=ethii-untagged|ethii-tagged|802.2-untagged|
802.2-tagged|any] [priority=priority|any]
[vlan=vlan_name|vid|any]
[protocol=protocol_string|protocol_number|any]
[iptos=tos_value|any] [ipdscp=dscp_value|any]
[ipprotocol=ipprotocol_string|ipprotocol_number|any]
[ipdaddr=ip_add/mask_len|any] [ipsaddr=ip_add/mask_len|any]
[tcpsport=tcpsport|any] [tcpdport=tcpdport|any]
[udpsport=udpsport|any] [udpport=udpport|any]
[tcpflags=urg|ack|psh|rst|syn|fin|any]
```

### Parameters

*classifier\_number*

Specifies a classifier number.

*string*

Specifies the description of the classifier. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

macdaddr

Specifies the MAC destination address of packets. The default value is any.

macdmask

Specifies the mask for the MAC destination address of packets. The default value is any.

macsaddr

Specifies the MAC source address of packets. The default value is any.

macsmask

Specifies the mask for the MAC destination address of packets. The default value is any.

*mac\_add*

Specifies a MAC address or mask in the format: *ff-ff-ff-ff-ff-ff*.

any

Specifies any.



*ethformat*

Specifies the frame format.

*ethii-untagged*

Specifies the frame format to Ethernet version 2 and untagged.

*ethii-tagged*

Specifies the frame format to Ethernet version 2 and tagged.

*802.2-untagged*

Specifies the frame format to 802.2 LLC and untagged.

*802.2-tagged*

Specifies the frame format to 802.2 LLC and tagged.

*priority*

Specifies a priority. The range is 0 to 7. The default setting is none.

*vlan\_name*

Specifies a VLAN name.

*vid*

Specifies a VLAN ID. The range is 1 to 4094.

*protocol*

Specifies the value of the protocol field in the packet with the protocol number. For the IP, ARP, or RARP protocol, you can specify it with the protocol name. The default setting is any.

*iptos*

Specifies the value of the precedence in the ToS octet in the packet. The range is 0 to 7. The default setting is any.

*ipdscp*

Specifies the value of the IP DSCP field. The range is 0 to 63. The default setting is any.

*ipprotocol*

Specifies the value of the IP protocol field in the packet with the protocol number. For the TCP, UDP, ICMP, and IGMP protocol, you can specify it with the protocol name. The default setting is any.

*ipsaddr*

Specifies the IP source address. You can also specify the Variable Length Subnet Mask (VLSM). The default value is any.

*ipdaddr*

Specifies the IP destination address. You can also specify the Variable Length Subnet Mask (VLSM). The default value is any.

*ip\_add*

Specifies an IP address in the format: *nnn.nnn.nnn.nnn*.

*mask\_len*

Specifies a VLSM after the IP address. Separate the IP address and VLSM with a slash(/).

*tcpSPORT*

Specifies the TCP source port of packets. The range is 0 to 65535. The default setting is any.

*tcpdport*

Specifies the TCP destination port of packets. The range is 0 to 65535. The default setting is any.

*udpSPORT*

Specifies the UDP source port of packets. The range is 0 to 65535. The default setting is any.

*udpdport*

Specifies the UDP destination port of packets. The range is 0 to 65535. The default setting is any.

*tcpflags*

Specifies the flag in the TCP header. The options are urg, ack, psh, rst, syn, and fin. QoS filters a packet in which only the specified flag in the TCP header is on. The default setting is any.

### **Description**

Use this command to change the settings of the classifier.

### **Confirmation Command**

“SHOW CLASSIFIER” on page 489

### **Example**

The following command changes the IP address of classifier 10 to 192.168.11.0/24:

```
Manager > set classifier=10 ipdaddr=192.168.11.0/24
```

## SET QOS FLOWGROUP

---

### Syntax

```
set qos flowgroup=flow_group_number [description=string]
[markvalue=mark_value|none] [priority=priority|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=tos_value|none]
[movetostoppriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[classifierlist=classifier_list|none]
```

### Parameters

*flow\_group\_number*

Specifies a flow group number.

*string*

Specifies the description of the flow group. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

*mark\_value*

Specifies a value to be written in the DSCP field of the IP header. The range is 0 to 63. This value has a priority over the markvalue of the traffic class and the indscpoverwrite of the policy.

*priority*

Specifies a priority. The range is 0 to 7. The default setting is none.

remarkpriority

Specifies yes, no, or none to the state that the priority of the flow group overwrites the user priority in the packet.

yes, on, true

Specifies yes to the parameter state.

no, off, false

Specifies no to the parameter state.

*tos\_value*

Specifies a value for the ToS field of the IP header.

movetostoppriority

Specifies yes, no, or none to the state that the ToS value of the IP header is used to determine the priority.

moveprioritytotos

Specifies yes, no, or none to the state that the priority is used for the ToS value.

*classifier\_list*

Specifies a list of classifiers. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-).

**Description**

Use this command to change the settings of the flow group.

**Confirmation Command**

“SHOW QOS FLOWGROUP” on page 493

**Example**

The following command changes the priority of flow group 1 to 3:

```
Manager > set qos flowgroup=1 priority=3
```

## SET QOS POLICY

---

### Syntax

```
set qos policy=policy_number [description=string]
[indscpoverwrite=dscp_value|none] [remarkindscp=all|none]
[tos=tos_value|none]
[movetostoppriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[sendtomirror=yes|no|on|off|true|false]
[trafficclasslist=traffic_class_list|none]
[redirectport=port_number|none]
[ingressport=port_list|all|none]
[egressport=port_number|none]
```

### Parameters

*policy\_number*

Specifies a policy number.

*string*

Specifies the description of the policy. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

*dscp\_value*

Specifies a value to be written in the DSCP field of the IP header. The range is 0 to 63. The default setting is none.

remarkindscp

Specifies all or none to the state that the value of the indscpoverwrite parameter overwrites the DSCP field of the IP header.

*tos\_value*

Specifies a value for the ToS field of the IP header.

movetostoppriority

Specifies yes, no, or none to the state that the ToS value of the IP header is used to determine the priority.

moveprioritytotos

Specifies yes, no, or none to the state that the priority is used for the ToS value.

yes, on, true

Yes to the parameter state.

no, off, false

No to the parameter state.

`sendtomirror`

Specifies yes, no, or none to the state that mirroring is enabled on the packets that match the conditions of the classifiers.

`trafficclasslist`

Specifies a list of traffic classes. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-).

`redirectport`

Specifies a port number to which the traffic is forwarded from.

*port\_number*

Specifies a port number.

`ingressport`

Specifies a list of input ports to which the QoS policy is applied. The port can be an ingressport to only one QoS policy.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

`all`

Specifies all the switch ports.

`egressport`

Specifies an input port to which the QoS policy is applied. The port can be an egressport to only one QoS policy.

**Description**

Use this command to change the settings of the QoS policy.

**Confirmation Command**

“SHOW QOS POLICY” on page 494

**Example**

The following command changes the ingressport of QoS policy 1 to port 2:

```
Manager > set qos policy=1 ingressport=2
```

## SET QOS TRAFFICCLASS

---

### Syntax

```
set qos trafficclass=traffic_class [description=string]
[exceedaction=drop|remark]
[exceedremarkvalue=remark_value|none]
[markvalue=mark_value|none]
[maxbandwidth=max_bandwidth|none]
[burstsize=burst_size|none] [priority=priority|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=tos_value|none]
[movetostoppriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[flowgrouplist=flow_list|none]
```

### Parameters

*traffic\_class*

Specifies a policy number.

*string*

Specifies the description of the traffic class. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

*exceedaction*

Specifies an action when the bandwidth for the traffic class is exceeded. is 0 to 63.

*drop*

The switch discards the packet.

*remark*

The switch overwrites the value of the DSCP field in the IP header with the value of the exceedremarkvalue parameter and forwards the packet.

*remark\_value*

Specifies a value to be written in the DSCP field of the IP header when the bandwidth for the traffic class is exceeded. The range is 0 to 63.

*mark\_value*

Specifies a value to be written in the DSCP field of the IP header. The range is 0 to 63.

*max\_bandwidth*

Specifies the maximum bandwidth of the traffic class in Mbps. The range is 0 to 1016 Mbps.

*burst\_size*

Specifies the buffer size, or token packet size of the traffic class. This value is effective when the maximum bandwidth is specified. The range is 4 to 512 Kbps.

*priority*

Specifies the priority for the traffic class.

remarkpriority

Specifies yes, no, or none to the state that the switch overwrites the user priority of a received packet with the priority.

*tos\_value*

Specifies a value for the ToS field of the IP header.

movetostopriority

Specifies yes, no, or none to the state that the ToS value of the IP header is used to determine the priority.

moveprioritytotos

Specifies yes, no, or none to the state that the priority is used for the ToS value.

yes, on, true

Yes to the parameter state.

no, off, false

No to the parameter state.

flowgroup`list`

Specifies a list of flow groups. To specify multiple flow groups, use a comma (,) to separate them. To specify a range of flow groups, use a hyphen (-).

**Description**

Use this command to change the settings of the traffic class.

**Confirmation Command**

“SHOW QOS TRAFFICCLASS” on page 496

**Example**

The following command changes the maxbandwidth of traffic class 1 to 500 Mbps:

```
Manager > set qos trafficclass=1 maxbandwidth=500
```



## SHOW CLASSIFIER

---

### Syntax

```
show classifier[=classifier_list|all] [description=string]
[macdaddr=mac_add|any] [macdmask=mac_add|any]
[macsaddr=mac_add|any] [macsmask=mac_add|any]
[ethformat=ethii-untagged|ethii-tagged|802.2-untagged|
802.2-tagged|any] [priority=priority|any]
[vlan=vlan_name|vid|any]
[protocol=protocol_string|protocol_number|any]
[iptos=iptos|any] [ipdscp=ipdscp|any]
[ipprotocol=ipprotocol_string|ipprotocol_number|any]
[ipdaddr=ipadd/mask_len|any] [ipsaddr=ipadd/mask_len|any]
[tcpsport=tcpsport|any] [tcpdport=tcpdport|any]
[udpsport=udpsport|any] [udpport=udpsport|any]
[tcpflags=urg|ack|psh|rst|syn|fin|any]
```

### Parameters

#### *classifier\_list*

Specifies a list of classifiers. To specify multiple classifiers, use a comma (,) to separate them. To specify a range of classifiers, use a hyphen (-). The default setting is none.

#### all

Specifies all classifiers.

#### *string*

Specifies the description of the classifier. The description is up to 31 alphanumeric characters. To include a space, place a double quote (") before and after the space.

#### macdaddr

Specifies the MAC destination address of packets. The default value is any.

#### macdmask

Specifies the mask for the MAC destination address of packets. The default value is any.

#### macsaddr

Specifies the MAC source address of packets. The default value is any.

#### macsmask

Specifies the mask for the MAC destination address of packets. The default value is any.

#### *mac\_add*

Specifies a MAC address or mask in the format: *ff-ff-ff-ff-ff*.

*any*  
Specifies any.

*ethformat*  
Specifies the frame format.

*ethi i-untagged*  
Specifies the frame format to Ethernet version 2 and untagged.

*ethi i-tagged*  
Specifies the frame format to Ethernet version 2 and tagged.

*802.2-untagged*  
Specifies the frame format to 802.2 LLC and untagged.

*802.2-tagged*  
Specifies the frame format to 802.2 LLC and tagged.

*priority*  
Specifies a priority. The range is 0 to 7. The default setting is none.

*vlan\_name*  
Specifies a VLAN name.

*vid*  
Specifies a VLAN ID. The range is 1 to 4094.

*protocol*  
Specifies the value of the protocol field in the packet with the protocol number. For the IP, ARP, or RARP protocol, you can specify it with the protocol name. The default setting is any.

*iptos*  
Specifies the value of the precedence in the ToS octet in the packet. The range is 0 to 7. The default setting is any.

*ipdscp*  
Specifies the value of the IP DSCP field. The range is 0 to 63. The default setting is any.

*ipprotocol*  
Specifies the value of the IP protocol field in the packet with the protocol number. For the TCP, UDP, ICMP, and IGMP protocol, you can specify it with the protocol name. The default setting is any.

*ipsaddr*  
Specifies the IP source address. You can also specify the Variable Length Subnet Mask (VLSM). The default value is any.

**ipdaddr**

Specifies the IP destination address. You can also specify the Variable Length Subnet Mask (VLSM). The default value is any.

**ip\_add**

Specifies an IP address in the format: *nnn.nnn.nnn.nnn*.

**mask\_len**

Specifies a VLSM after the IP address. Separate the IP address and VLSM with a slash(/).

**tcpsport**

Specifies the TCP source port of packets. The range is 0 to 65535. The default setting is any.

**tcpdport**

Specifies the TCP destination port of packets. The range is 0 to 65535. The default setting is any.

**udpsport**

Specifies the UDP source port of packets. The range is 0 to 65535. The default setting is any.

**udpport**

Specifies the UDP destination port of packets. The range is 0 to 65535. The default setting is any.

**tcpflags**

Specifies the flag in the TCP header. The options are urg, ack, psh, rst, syn, and fin. QoS filters a packet in which only the specified flag in the TCP header is on. The default setting is any.

**Description**

Use this command to display the settings of classifiers. An example of the command output is shown in Figure 71 on page 492.

```

Manager > show classifier
-----
Classifier ID: ..... 1
TCP Dst Port: ..... 80
Number of References: ..... 1
Number of Active Associations: .. 0

Manager > show classifier=2
-----
Classifier ID: ..... 2
Description: ..... atkk-ud1
Eth Format: ..... 802.2-Tagged
Priority: ..... 7
Protocol: ..... 0x806 (ARP)
Number of References: ..... 0
Number of Active Associations: .. 0

Manager > show classifier ethformat=802.2-untagged
-----
Classifier ID: ..... 3
Description: ..... atkk-ud2
Eth Format: ..... 802.2-Untagged
Priority: ..... 5
Protocol: ..... 0x8035 (RARP)
Number of References: ..... 0
Number of Active Associations: .. 0

```

Figure 71. SHOW CLASSIFIER Command

**Example**

The following example displays the settings of classifier 2:

```

Manager > show classifier=2

```

## SHOW QOS FLOWGROUP

---

### Syntax

```
show qos flowgroup[=flow_list|all]
```

### Parameters

flowgroup

Specifies a list of flow groups. To specify multiple flow groups, use a comma (,) to separate them. To specify a range of flow groups, use a hyphen (-).

### Description

Use this command to display the settings of flow groups. An example of the command output is shown in Figure 72.

```
-----
FlowGroup ID ..... 0
Description .....
DSCP value .....
Priority .....
Remark Priority ..... No
Classifier List .....
Parent Traffic Class ID .....
Is Active ..... No
```

Figure 72. SHOW QOS FLOWGROUP Command

### Example

The following example displays the settings of flow groups:

```
Manager > show qos flowgroup
```

## SHOW QOS POLICY

---

### Syntax

```
show qos policy[=policy_list|all]
```

### Parameters

*port\_list*

Specifies a list of QoS policies. To specify multiple policies, use a comma (,) to separate them. To specify a range of policies, use a hyphen (-).

### Description

Use this command to display the settings of QoS policies. An example of the command output is shown in Figure 73.

```
-----
Policy ID ..... 1
Description .....
Remark DSCP ..... None
In DSCP Overwrite ....
Traffic Class List ...
Redirect Port .....
Ingress Port List ....
Egress Port List .....
IS Active ..... No
```

Figure 73. SHOW QOS POLICY Command

### Example

The following example displays the settings of QoS policy 1:

```
Manager > show qos policy=1
```

## SHOW QOS POLICY COUNTER

### Syntax

```
show qos policy[=policy_list|all] counter
```

### Parameters

*port\_list*

Specifies a list of QoS policies. To specify multiple policies, use a comma (,) to separate them. To specify a range of policies, use a hyphen (-).

### Description

Use this command to display the counters of the classifiers assigned to the flow groups that are associated to QoS policy. An example of the command output is shown in Figure 74.

Policy/TrafficClass/FlowGroup Classifier				Hit Counter
1	Policy 1			
1	TrafficClass 1			
1	FlowGroup 1	1	Classifier 1	1840569814
2	TrafficClass 2			
2	FlowGroup 2	2	Classifier 2	10
3	TrafficClass 3			
3	FlowGroup 3	3	Classifier 3	987
4	TrafficClass 4			
4	FlowGroup 4	4	Classifier 4	2365490092
5	TrafficClass 5			
5	FlowGroup 5	5	Classifier 5	4567
6	TrafficClass 6			
6	FlowGroup 6	6	Classifier 6	4554
7	TrafficClass 7			
7	FlowGroup 7	7	Classifier 7	15604285020
8	TrafficClass 8			
8	FlowGroup 8	8	Classifier 8	23394

Figure 74. SHOW QOS POLICY COUNTER Command

### Example

The following example displays the counters of the classifiers:

```
Manager > show qos policy=1 counter
```

## SHOW QOS TRAFFICCLASS

---

### Syntax

```
show qos trafficclass[=traffic_class_list|all]
```

### Parameters

*traffic\_class\_list*

Specifies a list of traffic classes. To specify multiple traffic classes, use a comma (,) to separate them. To specify a range of traffic classes, use a hyphen (-).

### Description

Use this command to display the settings of traffic classes. An example of the command output is shown in Figure 75.

```
-----
Traffic Class ID ..... 0
Description .....
Exceed Action ..... Drop
Exceed Remark Value .. 0
Mark Value .....
Max bandwidth .....
Burst Size .....
Priority .....
Remark Priority ..... No
Flow Group List .....
Parent Policy ID .....
Is Active ..... No
```

Figure 75. SHOW QOS TRAFFICCLASS Command

### Example

The following example displays the settings of traffic classes:

```
Manager > show qos trafficclass
```



## Chapter 27

# Port-Based Authentication Commands

The Port-Based Authentication commands are summarized in Table 56.

Table 56. Port-Based Authentication Commands

Command	Description
“ADD PORTAUTH PORT SUPPLICANTMAC” on page 499	Adds the MAC address of the supplicant that communicates through the supplicant port.
“DELETE PORTAUTH PORT SUPPLICANTMAC” on page 501	Deletes the MAC address of the supplicant specified on the port.
“DISABLE PORTAUTH” on page 502	Disables Port-based Authentication on the switch.
“DISABLE PORTAUTH PORT LOGTYPE” on page 503	Disables logging on the specified authentication option and port.
“DISABLE WEBAUTHSERVER” on page 505	Disables the Web-based Authentication function.
“ENABLE PORTAUTH” on page 506	Enables Port-based Authentication on the switch.
“ENABLE PORTAUTH PORT LOGTYPE” on page 507	Enables logging on the specified authentication option and port.
“ENABLE WEBAUTHSERVER” on page 509	Enables the Web-based Authentication function.
“SET PORTAUTH AUTHMETHOD” on page 510	Specifies the authentication protocol to RADIUS EAP.
“SET PORTAUTH CSIDFORMAT” on page 511	Specifies the MAC address format for RADIUS packets.
“SET PORTAUTH DHCPSEVER” on page 513	Enables or disables the DHCP server function for Authentication and specify the lease time of an IP address.
“SET PORTAUTH PORT (Authenticator Port for All Methods)” on page 514	Changes the authenticator settings for all authentication methods including 802.1x Port-based, MAC address-based, and Web-based authentication on the specified port.

Table 56. Port-Based Authentication Commands (Continued)

Command	Description
“SET PORTAUTH PORT (802.1X Authenticator Port)” on page 518	Changes the authenticator port settings for 802.1x authentication method on the specified port.
“SET PORTAUTH PORT (802.1X Supplicant Port)” on page 522	Changes the supplicant port settings for on the specified port.
“SET PORTAUTH PORT (Authenticator Port for MAC and Web)” on page 524	Changes the authenticator port settings for MAC address-based and Web-based authentication on the specified port.
“SET PORTAUTH PORT (Canceling the Authentication Type)” on page 527	Cancels the port as an authenticator or supplicant.
“SET PORTAUTH PORT SUPPLICANTMAC” on page 528	Adds the MAC address of the supplicant that communicates through the supplicant port.
“SET PORTAUTH USERIDFORMAT” on page 529	Specifies the MAC address format for RADIUS packets for Web-Based Authentication.
“SET WEBAUTHSERVER” on page 531	Changes the TCP port for the Web-based authentication server, specifies the URL that the user is redirected after authenticated, and specifies messages to display on the Web-based authentication login screen.
“SHOW PORTAUTH” on page 532	Displays information about Port-Based Authentication.
“SHOW PORTAUTH PORT AUTHENTICATOR” on page 534	Displays authenticator information about Port-based Authentication on the specified port.
“SHOW PORTAUTH PORT SUPPLICANT” on page 536	Displays supplicant information about Port-based Authentication on the specified port.
“SHOW WEBAUTHSERVER” on page 538	Displays information about Web-based Authentication.

## ADD PORTAUTH PORT SUPPLICANTMAC

---

### Syntax

```
add portauth port=port_number supplicantmac=mac_add
[control=authorised]
```

### Parameters

*port\_number*

Specifies the port number of a supplicant.

supplicantmac

Specifies the MAC address of the

*mac\_add*

Specifies a MAC address or mask in the format: *ff-ff-ff-ff-ff*.

control

Specifies the state of authenticator port. The options is authorised only.

supplicantmac

Specifies all the switch ports.

### Description

Use this command to add the MAC address of the supplicant that communicates through the supplicant port. The supplicant is authenticated based on its MAC address.

802.1x Port-based Authentication is implemented with three parties:

- Supplicant: a host device connected to a switch.
- Authenticator: a switch that allows a supplicant to communicate through the port.
- Authentication Server: a server that authenticates supplicants via an authenticator.

---

### Note

When MAC-based Authentication is used on a port, Extensible Authentication Protocol (EAP) is not effective on the port.

---

### Confirmation Command

“SHOW PORTAUTH” on page 532

### **Example**

The following command adds the supplicant MAC address 00-00-f4-11-11-11 on port 1:

```
Manager > add portauth port=1 supplicantmac=00-00-f4-11-11-11
```

## DELETE PORTAUTH PORT SUPPLICANTMAC

---

### Syntax

```
delete portauth port=port_number [supplicantmac=mac_add]
```

### Parameters

*port\_number*

Specifies a port number.

supplicantmac

Specifies the MAC address of the supplicant. When omitted this parameter, all the supplicant MAC address on the port are deleted.

*mac\_add*

Specifies a MAC address or mask in the format: *ff-ff-ff-ff-ff*.

### Description

Use this command to delete the MAC address of the supplicant specified on the port.

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command deletes all supplicant MAC addresses on port 2:

```
Manager > delete portauth port=2
```

## DISABLE PORTAUTH

---

### Syntax

```
disable portauth
```

### Parameters

None

### Description

Use this command to disable Port-Based Authentication on the switch. By default, Port-Based Authentication is disabled.

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command disables Port-Based Authentication on the switch:

```
Manager > disable portauth
```

## DISABLE PORTAUTH PORT LOGTYPE

---

### Syntax

```
disable portauth[=all|8021x|macbased|webbased]
port=port_list|all logtype=success|failure|logoff|all
```

### Parameters

portauth

Specifies an authentication method.

all

Specifies all the authentication methods.

8021x

Specifies 802.1x Port-Based Authentication using EAP.

macbased

Specifies MAC-Based Authentication.

webbased

Specifies Web-based Authentication.

*port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

logtype

Specifies a log type.

success

Specifies the log type of authentication success.

failure

Specifies the log type of authentication failure.

logoff

Specifies the log type of logoff.

all

Specifies all log types.

### Description

Use this command to disable logging on the specified authentication option and port. By default, all log types are enabled.

### **Confirmation Command**

“SHOW PORTAUTH” on page 532

### **Example**

The following command disables logging on all authentication options and all log types on port 1 to port 5:

```
Manager > disable portauth=all port=1-5 logtype=all
```



## DISABLE WEBAUTHSERVER

---

### Syntax

```
disable webauthserver
```

### Parameters

None

### Description

Use this command to disable the Web-based Authentication function. By default, the Web-based Authentication function is disabled.

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command disables the Web-based Authentication function on the switch:

```
Manager > disable webauthserver
```

## ENABLE PORTAUTH

---

### Syntax

```
enable portauth
```

### Parameters

None

### Description

Use this command to enable Port-based Authentication on the switch. By default, Port-based Authentication is disabled.

Here are the guidelines for enabling Port-based Authentication:

- RSTP and MSTP cannot be enabled on authenticator or supplicant ports.
- Authenticator and supplicant ports cannot belong to a trunk group.
- Authenticator and supplicant ports cannot be mirror ports.
- When Port-based authentication is enabled, authentication using EAP does not work.
- A combo port cannot be an authenticator port.

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command enables Port-Based Authentication on the switch:

```
Manager > enable portauth
```

## ENABLE PORTAUTH PORT LOGTYPE

---

### Syntax

```
enable portauth[=all|8021x|macbased|webbased]
port=port_list|all logtype=success|failure|logoff|all
```

### Parameters

**portauth**

Specifies an authentication option.

**all**

Specifies all the authentication options.

**8021x**

Specifies 802.1x Port-Based Authentication using EAP.

**macbased**

Specifies MAC-Based Authentication.

**webbased**

Specifies Web-based Authentication.

***port\_list***

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

**logtype**

Specifies a log type.

**success**

Specifies the log type of authentication success.

**failure**

Specifies the log type of authentication failure.

**logoff**

Specifies the log type of logoff.

**all**

Specifies all log types.

### Description

Use this command to enable logging on the specified authentication option and port. By default, all log types are enabled.

### **Confirmation Command**

“SHOW PORTAUTH” on page 532

### **Example**

The following command enables logging on all authentication options and all log types on port 1 to port 5:

```
Manager > enable portauth=all port=1-5 logtype=all
```

## ENABLE WEBAUTHSERVER

---

### Syntax

```
enable webauthserver
```

### Parameters

None

### Description

Use this command to enable the Web-based Authentication function. By default, the Web-based Authentication function is disabled.

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command enables the Web-based Authentication function on the switch:

```
Manager > enable webauthserver
```

## SET PORTAUTH AUTHMETHOD

---

### Syntax

```
set portauth authmethod=radius_eap
```

### Parameters

None

### Description

Use this command to specify the authentication protocol to RADIUS EAP.

---

#### Note

The GS900M series switch supports RADIUS EAP only.

---

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command specifies RADIUS EAP.

```
Manager > set portauth authmethod=radius_eap
```

## SET PORTAUTH CSIDFORMAT

---

### Syntax

```
set portauth csidformat [separator=hyphen|colon|period|none]
[digit=2|4] [uppercase=true|false]
```

### Parameters

#### separator

Specifies the separator of a MAC address for the Calling-Station-Id and Called-Station-Id attributes in a RADIUS packet. The default setting is hyphen.

#### hyphen

Specifies a hyphen as the separator. This is the default setting. For example, a MAC address using hyphens is 00-00-F4-11-11-A3.

#### colon

Specifies a colon as the separator. For example, a MAC address using colons is 00:00:F4:11:11:A3.

#### period

Specifies a period as the separator. For example, a MAC address using periods is 00.00.F4.11.11.A3.

#### none

Specifies no separator. For example, a MAC address without separators is 0000F41111A3.

#### digit

Specifies the number of digits that the separator should be inserted between. When the separator parameter is none, this parameter is ignored.

#### 2

Specifies 2 digits that the separator is inserted between. This is the default setting. For example, a MAC address with separators every 2 digits is 00-00-F4-11-11-A3.

#### 4

Specifies 4 digits that the separator is inserted between. For example, a MAC address with separators every 4 digits is 0000-F411-11A3.

#### uppercase

Specifies either uppercase or lowercase for the MAC address notation. The default setting is true (uppercase).

### **Description**

Use this command to specify the MAC address format for RADIUS packets.

### **Confirmation Command**

“SHOW PORTAUTH” on page 532

### **Example**

The following command specifies the MAC address format using a period as the separator:

```
Manager > set portauth csidformat separator=period
```



## SET PORTAUTH DHCPSEVER

---

### Syntax

```
set portauth dhcpserver[=enabled|disabled]
[leasetime = lease_time]
```

### Parameters

#### dhcpserver

Enables or disables the DHCP server for Authentication. By default, the DCHP server function for Authentication is disabled.

#### leasetime

Specifies the lease time of an IP address. The default value is 20 seconds. The range is 10 to 86400 seconds.

### Description

Use this command to enable or disable the DHCP server function for Authentication and specify the lease time of an IP address.

When the DCHP server for Authentication is enabled, only the ports that Web-Based Authentication is enabled on receive DHCP packets.

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command enables the DHCP server for Authentication:

```
Manager > set portauth dhcpserver=enabled
```

## SET PORTAUTH PORT (Authenticator Port for All Methods)

---

### Syntax

```
set portauth=auto port=port_list|all type=authenticator
[mode=single|multi] [control=authorised|unauthorised|auto]
[eapolversion=1|2] [servertimeout=servertimeout]
[quietperiod=quietperiod] [txperiod=txperiod]
[reauthperiod=reauthperiod] [supptimeout=timeout]
[maxreq=maxreq] [reauthenabled=enabled|disabled]
[piggyback=enabled|disabled] [guestvlan=vlan_name|vid|none]
[securevlan=on|off] [vlanassignment=enabled|disabled]
[vlanassignmenttype=user|port]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### mode

Specifies the mode of an authenticator port that is connected to single or multiple supplicants.

#### single

When the port is connected to one supplicant device.

#### multi

When the port is connected to multiple supplicant devices.

#### control

Specifies the state of the authenticator port.

#### auto

The state of the authenticator port is based on the result of the authentication. This is the default setting.

#### authorised

The state of the authenticator port is fixed to be authorized.

#### unauthorised

The state of the authenticator port is fixed to be unauthorized.

#### eapolversion

Specifies the EAPOL version on the 802.1x authenticator port.

1 Specifies the version 1 of EAPOL, IEEE802.1x-2001 compliant mode.

2 Specifies the version 2 of EAPOL, IEEE802.1x-2004 compliant mode.

*servertimeout*

Specifies the maximum amount of time in seconds that the 802.1x or Web-based authenticator port waits for a response from a RADIUS authentication server after sending an Access-request. The range is 1 to 600 seconds. The default setting is 30 seconds.

*quietperiod*

Specifies the amount of time in seconds that the 802.1x, MAC address-based, or Web-based authenticator port discards all EAPOL packets from supplicants. The range is 0 to 65535 seconds. The default setting is 60 seconds.

*txperiod*

Specifies the interval in seconds that the 802.1x authenticator port resends EAPOL packets to supplicants. The range is 1 to 65535 seconds. The default setting is 30 seconds.

*reauthperiod*

Specifies the interval in seconds that the 802.1x or MAC address-based authenticator port re-authenticates supplicants. The Web-based authenticator port does not re-authenticate automatically so that the link is disconnected when the reauthperiod has passed. The range is 1 to 86400 seconds. The default setting is 3600 seconds.

*supptimeout*

Specifies the maximum amount of time in seconds that the 802.1x authenticator port waits for a response from a supplicant after sending an EAP-request. The range is 1 to 600 seconds. The default setting is 30 seconds.

*maxreq*

Specifies how many times the 802.1x or Web-based authenticator port resends an EAPOL-request packet to a supplicant. The range is 1 to 10 seconds. The default setting is 2 times.

*reauthenable*

Specifies that the 802.1x, MAC address-based, or Web-based authenticator port enables or disables re-authentication. When re-authentication is enabled, Web-based authenticator port is disconnected after the reauthperiod has passed. By default, re-authentication is enabled.

`piggyback`

Specifies that the 802.1x authenticator port enables or disables authenticating other devices after authenticating one device when the mode parameter is set to single. By default, authenticating other devices is disabled. When the mode parameter is set to multi, this setting is ignored.

`guestvlan`

Specifies the guest VLAN in the VLAN name or VID on the 802.1x, MAC address-based, or Web-based authenticator port. To specify no guest VLAN, use the keyword none. When authenticated, the authenticator port belongs to another VLAN. When failed to be authenticated, the authenticator port is back to the guest VLAN. The default setting is none.

`securevlan`

Specifies how the authenticator with the multiple supplicants authenticates the second or following supplicant when using a dynamic VLAN. The default setting is none.

`on`

The second or following supplicant must be authenticated through the same VLAN that the first supplicant was authenticated. This is the default setting.

`off`

The second or following supplicant passes authentication; however, it belongs to the same VLAN as the first authenticated supplicant.

`vlanassignment`

Specifies that the 802.1x, MAC address-based, or Web-based authenticator port enables or disables Dynamic VLAN.

`vlanassignmenttype`

Specifies that Dynamic VLAN is set based on ports or users (MAC addresses). This parameter is effective when the mode is multi and `vlanassignment` is enabled. The default setting is port.

**Description**

Use this command to change the authenticator port settings for all authentication methods including 802.1x Port-based, MAC address-based, and Web-based authentication on the specified port.

Here are references for other usage of this command:

- ❑ To change the authenticator port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Authenticator Port)” on page 518.

- ❑ To change the supplicant port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Supplicant Port)” on page 522.
- ❑ To change the authenticator port settings for MAC address-based and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for MAC and Web)” on page 524.
- ❑ To cancel the port as an authenticator and supplicant on the specified port, see “SET PORTAUTH PORT (Canceling the Authentication Type)” on page 527.

### **Confirmation Command**

“SHOW PORTAUTH” on page 532

“SHOW VLAN” on page 216

### **Example**

The following command changes the settings for all authentication methods in the authenticator port type on port 1 to 8:

```
Manager > set portauth=auto port=1-8 type=authenticator
```

## SET PORTAUTH PORT (802.1X Authenticator Port)

---

### Syntax

```
set portauth[=8021x] port=port_list|all type=authenticator
[mode=single|multi] [control=authorised|unauthorised|auto]
[eapolversion=1|2] [servertimeout=servertimeout]
[quietperiod=quietperiod] [txperiod=txperiod]
[reauthperiod=reauthperiod] [supptimeout=timeout]
[maxreq=maxreq] [reauthenabled=enabled|disabled]
[piggyback=enabled|disabled] [guestvlan=vlan_name|vid|none]
[securevlan=on|off] [vlanassignment=enabled|disabled]
[vlanassignmenttype=user|port]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### mode

Specifies the mode of an authenticator port that is connected to single or multiple supplicants.

#### single

When the port is connected to one supplicant device.

#### multi

When the port is connected to multiple supplicant devices.

#### control

Specifies the state of the authenticator port.

#### auto

The state of the authenticator port is based on the result of the authentication. This is the default setting.

#### authorised

The state of the authenticator port is fixed to be authorized.

#### unauthorised

The state of the authenticator port is fixed to be unauthorized.

#### eapolversion

Specifies the EAPOL version on the 802.1x authenticator port.

1 Specifies the version 1 of EAPOL, IEEE802.1x-2001 compliant mode.

2 Specifies the version 2 of EAPOL, IEEE802.1x-2004 compliant mode.

*servertimeout*

Specifies the maximum amount of time in seconds that the 802.1x or Web-based authenticator port waits for a response from a RADIUS authentication server after sending an Access-request. The range is 1 to 600 seconds. The default setting is 30 seconds.

*quietperiod*

Specifies the amount of time in seconds that the 802.1x, MAC address-based, or Web based authenticator port discards all EAPOL packets from supplicants. The range is 0 to 65535 seconds. The default setting is 60 seconds.

*txperiod*

Specifies the interval in seconds that the 802.1x authenticator port resends EAPOL packets to supplicants. The range is 1 to 65535 seconds. The default setting is 30 seconds.

*reauthperiod*

Specifies the interval in seconds that the 802.1x or MAC address-based authenticator port re-authenticates supplicants. The Web-based authenticator port does not re-authenticate automatically so that the link is disconnected when the reauthperiod has passed. The range is 1 to 86400 seconds. The default setting is 3600 seconds.

*supptimeout*

Specifies the maximum amount of time in seconds that the 802.1x authenticator port waits for a response from a supplicant after sending an EAP-request. The range is 1 to 600 seconds. The default setting is 30 seconds.

*maxreq*

Specifies how many times the 802.1x or Web-based authenticator port resends an EAPOL-request packet to a supplicant. The range is 1 to 10 seconds. The default setting is 2 times.

*reauthenable*

Specifies that the 802.1x, MAC address-based, or Web-based authenticator port enables or disables re-authentication. When re-authentication is enabled, Web-based authenticator port is disconnected after the reauthperiod has passed. By default, re-authentication is enabled.

**piggyback**

Specifies that the 802.1x authenticator port enables or disables authenticating other devices after authenticating one device when the mode parameter is set to single. By default, authenticating other devices is disabled. When the mode parameter is set to multi, this setting is ignored.

**guestvlan**

Specifies the guest VLAN in the VLAN name or VID on the 802.1x, MAC address-based, or Web-based authenticator port. To specify no guest VLAN, use the keyword none. When authenticated, the authenticator port belongs to another VLAN. When failed to be authenticated, the authenticator port is back to the guest VLAN. The default setting is none.

**securevlan**

Specifies how the authenticator with the multiple supplicants authenticates the second or following supplicant when using a dynamic VLAN. The default setting is none.

**on**

The second or following supplicant must be authenticated through the same VLAN that the first supplicant was authenticated. This is the default setting.

**off**

The second or following supplicant passes authentication; however, it belongs to the same VLAN as the first authenticated supplicant.

**vlanassignment**

Specifies that the 802.1x, MAC address-based, or Web-based authenticator port enables or disables Dynamic VLAN.

**vlanassignmenttype**

Specifies that Dynamic VLAN is set based on ports or users (MAC addresses). This parameter is effective when the mode is multi and vlanassignment is enabled. The default setting is port.

**Description**

Use this command to change the authenticator port settings for 802.1x Port-based authentication on the specified port.

Here are references for other usage of this command:

- ❑ To change the authenticator port settings for all authentication methods including 802.1x Port-based, MAC address-based, and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for All Methods)” on page 514.



- ❑ To change the supplicant port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Supplicant Port)” on page 522.
- ❑ To change the authenticator port settings for MAC address-based and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for MAC and Web)” on page 524.
- ❑ To cancel the port as an authenticator and supplicant. on the specified port, see “SET PORTAUTH PORT (Canceling the Authentication Type)” on page 527.

### **Confirmation Command**

“SHOW PORTAUTH” on page 532

“SHOW VLAN” on page 216

### **Example**

The following command changes the EAPOL version for the 802.1x authentication in the authenticator port type on port 1 to 8:

```
Manager > set portauth=8021x port=1-8 type=authenticator  
eapolversion=2
```

## SET PORTAUTH PORT (802.1X Supplicant Port)

---

### Syntax

```
set portauth[=8021x] port=port_list|all type=supplicant
[authperiod=authperiod] [heldperiod=heldperiod]
[maxstart=maxstart] [startperiod=startperiod]
[username=username] [password=password]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### *authperiod*

Specifies the amount of time in seconds that the 802.1x supplicant port waits for a response from the authenticator after sending an EAP-response packet. The range is 1 to 300 seconds. The default setting is 30 seconds.

#### *heldperiod*

Specifies the amount of time in seconds that the 802.1x supplicant port does not communicate with the authenticator after the supplicant failed to be authenticated. The range is 0 to 65535 seconds. The default setting is 60 seconds.

#### *maxstart*

Specifies how many times the 802.1x supplicant sends an EAPOL packet before it stops the attempt of being authenticated. The range is 1 to 10 times. The default setting is 3 times.

#### *startperiod*

Specifies the interval in seconds that the 802.1x supplicant port resends EAPOL-start packets to the authenticator. The range is 1 to 65535 seconds. The default setting is 30 seconds.

#### *username*

Specifies the user name of the supplicant. The user name must be up to 63 alphanumeric characters.

#### *password*

Specifies the password of the supplicant. The password must be up to 63 alphanumeric characters.

## Description

Use this command to change the supplicant port settings for 802.1x Port-based authentication on the specified port.

Here are references for other usage of this command:

- ❑ To change the authenticator port settings for all authentication methods including 802.1x Port-based, MAC address-based, and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for All Methods)” on page 514.
- ❑ To change the authenticator port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Authenticator Port)” on page 518.
- ❑ To change the authenticator port settings for MAC address-based and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for MAC and Web)” on page 524.
- ❑ To cancel the port as an authenticator and supplicant. on the specified port, see “SET PORTAUTH PORT (Canceling the Authentication Type)” on page 527.

## Confirmation Commands

“SHOW PORTAUTH” on page 532

## Example

The following command changes the EAPOL version for the 802.1x authentication in the authenticator port type on port 1 to 8:

```
Manager > set portauth=8021x port=1-8 type=supplicant  
username=user1 password=secret
```

## SET PORTAUTH PORT (Authenticator Port for MAC and Web)

---

### Syntax

```
set portauth=[macbased|webbased] port=port_list|all
type=authenticator [mode=single|multi]
[control=authorised|unauthorised|auto]
[quietperiod=quietperiod] [reauthperiod=reauthperiod]
[reauthenable=enabled|disabled]
[guestvlan=vlan_name|vid|none] [securevlan=on|off]
[vlanassignment=enabled|disabled]
[vlanassignmenttype=user|port]
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### mode

Specifies the mode of an authenticator port that is connected to single or multiple supplicants.

#### single

When the port is connected to one supplicant device.

#### multi

When the port is connected to multiple supplicant devices.

#### control

Specifies the state of the authenticator port.

#### auto

The state of the authenticator port is based on the result of the authentication. This is the default setting.

#### authorised

The state of the authenticator port is fixed to be authorized.

#### unauthorised

The state of the authenticator port is fixed to be unauthorized.

*quietperiod*

Specifies the amount of time in seconds that the 802.1x, MAC address-based, or Web based authenticator port discards all EAPOL packets from supplicants. The range is 0 to 65535 seconds. The default setting is 60 seconds.

*reauthperiod*

Specifies the interval in seconds that the 802.1x or MAC address-based authenticator port re-authenticates supplicants. The Web-based authenticator port does not re-authenticate automatically so that the link is disconnected when the reauthperiod has passed. The range is 1 to 86400 seconds. The default setting is 3600 seconds.

## reauthenable

Specifies that the 802.1x, MAC address-based, or Web-based authenticator port enables or disables re-authentication. When re-authentication is enabled, Web-based authenticator port is disconnected after the reauthperiod has passed. By default, re-authentication is enabled.

## guestvlan

Specifies the guest VLAN in the VLAN name or VID on the 802.1x, MAC address-based, or Web-based authenticator port. To specify no guest VLAN, use the keyword none. When authenticated, the authenticator port belongs to another VLAN. When failed to be authenticated, the authenticator port is back to the guest VLAN. The default setting is none.

## securevlan

Specifies how the authenticator with the multiple supplicants authenticates the second or following supplicant when using a dynamic VLAN. The default setting is none.

## on

The second or following supplicant must be authenticated through the same VLAN that the first supplicant was authenticated. This is the default setting.

## off

The second or following supplicant passes authentication; however, it belongs to the same VLAN as the first authenticated supplicant.

## vlanassignment

Specifies that the 802.1x, MAC address-based, or Web-based authenticator port enables or disables Dynamic VLAN.

**vlanassignmenttype**

Specifies that Dynamic VLAN is set based on ports or users (MAC addresses). This parameter is effective when the mode is multi and vlanassignment is enabled. The default setting is port.

**Description**

Use this command to change the authenticator port settings for MAC address-based and Web-based authentication on the specified port.

Here are references for other usage of this command:

- ❑ To change the authenticator port settings for all authentication methods including 802.1x Port-based, MAC address-based, and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for All Methods)” on page 514.
- ❑ To change the authenticator port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Authenticator Port)” on page 518.
- ❑ To change the supplicant port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Supplicant Port)” on page 522.
- ❑ To cancel the port as an authenticator and supplicant. on the specified port, see “SET PORTAUTH PORT (Canceling the Authentication Type)” on page 527.

**Confirmation Commands**

“SHOW PORTAUTH” on page 532

“SHOW VLAN” on page 216

**Example**

The following command changes the mode for MAC address-based and Web-based authentication in the authenticator port type on port 1 to 8:

```
Manager > set portauth=webbased port=1-8 type=authenticator
mode=single
```

## SET PORTAUTH PORT (Canceling the Authentication Type)

---

### Syntax

```
set portauth port=port_list|all type=none
```

### Parameters

#### *port\_list*

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

#### all

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

### Description

Use this command to cancel the port as an authenticator and supplicant on the specified port.

Here are references for other usage of this command:

- ❑ To change the authenticator port settings for all authentication methods including 802.1x Port-based, MAC address-based, and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for All Methods)” on page 514.
- ❑ To change the authenticator port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Authenticator Port)” on page 518.
- ❑ To change the supplicant port settings for 802.1x Port-based authentication on the specified port, see “SET PORTAUTH PORT (802.1X Supplicant Port)” on page 522.
- ❑ To change the authenticator port settings for Web address-based and Web-based authentication on the specified port, see “SET PORTAUTH PORT (Authenticator Port for MAC and Web)” on page 524.

### Confirmation Commands

“SHOW PORTAUTH” on page 532

### Example

The following command cancels port 1 to 8 as authenticator ports:

```
Manager > set portauth port=1-8 type=none
```

## SET PORTAUTH PORT SUPPLICANTMAC

---

### Syntax

```
set portauth port=port_number supplicantmac=mac_add  
[control=authorised]
```

---

### Note

This command is identical to the ADD PORTAUTH PORT SUPPLICANTMAC command. See “ADD PORTAUTH PORT SUPPLICANTMAC” on page 499.

---



## SET PORTAUTH USERIDFORMAT

---

### Syntax

```
set portauth useridformat  
[separator=hyphen|colon|period|none] [digit=2|4]  
[uppercase=true|false]
```

### Parameters

#### separator

Specifies the separator of a MAC address for the User-Name and User-Password attributes in a RADIUS packet for MAC-Based Authentication. The default setting is hyphen.

#### hyphen

Specifies a hyphen as the separator. This is the default setting. For example, a MAC address using hyphens is 00-00-F4-11-11-A3.

#### colon

Specifies a colon as the separator. For example, a MAC address using colons is 00:00:F4:11:11:A3.

#### period

Specifies a period as the separator. For example, a MAC address using periods is 00.00.F4.11.11.A3.

#### none

Specifies no separator. For example, a MAC address without separators is 0000F41111A3.

#### digit

Specifies the number of digits that the separator should be inserted between. When the separator parameter is none, this parameter is ignored.

#### 2

Specifies 2 digits that the separator is inserted between. This is the default setting. For example, a MAC address with separators every 2 digits is 00-00-F4-11-11-A3.

#### 4

Specifies 4 digits that the separator is inserted between. For example, a MAC address with separators every 4 digits is 0000-F411-11A3.

#### uppercase

Specifies either uppercase or lowercase for the MAC address notation. The default setting is true (uppercase).

### **Description**

Use this command to specify the MAC address format for RADIUS packets for Web-Based Authentication.

### **Confirmation Command**

“SHOW PORTAUTH” on page 532

### **Example**

The following command specifies the MAC address format without separators.

```
Manager > set portauth useridformat separator=none
```

## SET WEBAUTHSERVER

---

### Syntax

```
set webauthserver [port=port] [redirecturl=redirect_url]  
[message1=message] [message2=message] [message3=message]  
[message4=message] [message5=message]
```

### Parameters

#### *port*

Specifies the TCP port number. The default port number is 8080.

#### *redirect\_url*

Specifies a URL up to 128 bytes. The user is redirected to the URL after authenticated.

#### *message*

Specifies a message up to 128 alphanumeric characters except a hash (#), question (?), percent (%), and double quote ("). The message is displayed on the Web Authentication Login screen. The default value is NULL.

### Description

Use this command to change the TCP port for the Web Authentication server, to specify the URL that the user is redirected after authenticated and to specify messages to display on the Web Authentication Login screen.

### Confirmation Command

“SHOW PORTAUTH” on page 532

### Example

The following command changes the TCP port for the Web Authentication server to 8081:

```
Manager > set webauthserver port=8081
```

## SHOW PORTAUTH

---

### Syntax

```
show portauth[=8021x|macbased|webbased] [config|status]
```

### Parameters

portauth

Specifies an authentication method to display the information about. By default, the system displays information about all authentication methods.

8021x

Specifies 802.1x Port-Based Authentication using EAP.

macbased

Specifies MAC-Based Authentication.

webbased

Specifies Web-based Authentication.

config

Displays the configuration information.

status

Displays the status.

### Description

Use this command to display information about Port-Based Authentication. An example of the command output is shown in Figure 76 on page 533.

```

Manager > show portauth

Port Access Configuration Information:
Port Access Control..... Disabled
Authentication Method ..... RADIUS EAP
DHCP Server ..... Enabled
DHCP Server Lease Time ..... 20
Number of Total Supplicants..... 0/480
Number of DynamicVlan per USER.... 0/62
MAC Based Auth User-ID Format..... XX-XX-XX-XX-XX-XX
Calling/Called-Station-ID Foramt.. XX-XX-XX-XX-XX-XX

-----
Port AuthMode PortRole  VLAN  PortStatus  Status  Additional Info
-----
1          ----- None      -----
2          ----- None      -----
3          ----- None      -----
4          MACBASE Auth      10    Unauthorized Held      00:00:F4:97:66:1A
4          MACBASE Auth      1000  Authorized  Authenticated 00:90:99:18:29:36
4          MACBASE Auth      1000  Authorized  Authenticated 00:E0:4C:C7:7D:99
5          MACBASE Auth      1000  Authorized  Authenticated 00:00:F4:27:2C:70
5          MACBASE Auth      1000  Authorized  Authenticated 00:09:41:86:FA:45
5          MACBASE Auth      1000  Authorized  Authenticated 00:09:41:A4:15:E1
5          MACBASE Auth      1000  Authorized  Authenticated 00:09:41:A4:59:43
6          8021x  Auth      1000  Authorized  Authenticated 00:03:47:B5:79:89
7          8021x  Auth      1000  Authorized  Authenticated 00:09:41:A4:18:11
8          ----- None      -----
9          ----- None      -----
10         ----- None      -----
11         ----- None      -----
12         ----- None      -----
13         ----- None      -----
14         ----- None      -----
15         ----- None      -----
16         ----- None      -----

```

Figure 76. SHOW PORTAUTH Command

**Example**

The following example displays information about Port-Based Authentication:

```

Manager > show portauth

```

## SHOW PORTAUTH PORT AUTHENTICATOR

---

### Syntax

```
show portauth[=8021x|macbased|webbased] port=port_list|all  
[authenticator] [config|status]
```

### Parameters

**portauth**

Specifies an authentication method to display the information about. By default, the system displays information about all authentication methods.

**8021x**

Specifies 802.1x Port-Based Authentication using EAP.

**macbased**

Specifies MAC-Based Authentication.

**webbased**

Specifies Web-based Authentication.

***port\_list***

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

**all**

Specifies all the switch ports.

**authenticator**

Displays information about the authenticator.

**config**

Displays the configuration information.

**status**

Displays the status.

### Description

Use this command to display authenticator information about Port-Based Authentication on the specified port. An example of the command output is shown in Figure 77 on page 535.

```

Manager > show portauth port=5
-----All Authenticator Configuration -----
-----
Port Number                5
Auth Mode                  MACBASED
Log Type                   [8021x] None
Log Type                   [Mac] All
Log Type                   [web] None
Port Control               Auto
Supplicant Mode            Multi
eapolVersion               [8021x] 1
Quiet Period               [8021x] 60
Tx Period                  [8021x] 30
Reauth Enabled             Enabled
Reauth Period              3600
Supplicant Timeout        [8021x] 30
Server Timeout             [web] [8021x] 30
Max Requests               [8021x] 2
Piggyback Mode             [8021x] Disabled
vlanAssignment             Enabled
secureVlan                 On
guestVlan                  None
-----
Port AuthMode Role  VID  PortStatus  Status  ReAuth Timer  Tag
                   MAC Address  IP Address  User Name
-----
5    MACBASE Auth  1000 Authorized  Authenticated  100          n
                   00:00:F4:27:2C:70 255.255.255.255 00-00-F4-27-2C-70
5    MACBASE Auth  1000 Authorized  Authenticated  3600         n
                   00:09:41:86:FA:45 255.255.255.255 00-09-41-86-FA-45
5    MACBASE Auth  1000 Authorized  Authenticated  10          n
                   00:09:41:A4:15:E1 255.255.255.255 00-09-41-A4-15-E1
5    MACBASE Auth  1000 Authorized  Authenticated  8          n
                   00:09:41:A4:59:43 255.255.255.255 00-09-41-A4-59-43

```

Figure 77. SHOW PORTAUTH PORT AUTHENTICATOR Command

**Example**

The following example displays authenticator information about Port-Based Authentication on port 5:

```
Manager > show portauth port=5
```

## SHOW PORTAUTH PORT SUPPLICANT

### Syntax

```
show portauth[=8021x] port=port_list|all supplicant
[config|status]
```

### Parameters

**portauth**

Specifies an authentication method to display the information about. The option is only 8021x.

***port\_list***

Specifies a list of ports. To specify multiple ports, use a comma (,) to separate them. To specify a range of ports, use a hyphen (-).

**all**

Specifies all the switch ports.

**config**

Displays the configuration information.

**status**

Displays the status.

### Description

Use this command to display supplicant information about Port-Based Authentication on the specified port. An example of the command output is shown in Figure 78.

```
Manager > show portauth port=1 supplicant
-----Supplicant Configuration -----
-----
Port Number      1
Auth Period     30
Hold Period     60
Max Start       3
Start Period    30
User Name
User Password
-----
Port  PortRole  VLAN  PortStatus  Status  Additional Info
-----
1    Supp      -----
```

Figure 78. SHOW PORTAUTH PORT SUPPLICANT Command



**Example**

The following example displays supplicant information about Port-Based Authentication on port 5:

```
Manager > show portauth port=1 supplicant
```

## SHOW WEBAUTHSERVER

---

### Syntax

```
show webauthserver
```

### Parameters

None

### Description

Use this command to display information about Web-Based Authentication. An example of the command output is shown in Figure 79.

```
Manager > show webauthserver
Web Authentication Server Module Configuration:
-----
Status       : Enabled
TCP port     : 8080
RedirectURL  :
Message1    : Allied-Telesis
Message2    : User Login
Message3    :
Message4    :
Message5    : Copyright (C) Allied Telesis K.K.
```

Figure 79. SHOW WEBAUTHSERVER Command

### Example

The following example displays information about Web-Based Authentication:

```
Manager > show webauthserver
```

# Command Index

---

## A

ACTIVATE SCRIPT command 73  
 ACTIVATE SWITCH PORT AUTONEGOTIATE command 222  
 ADD ACCESS FILTER command 406  
 ADD DCHPSNOOPING command 305  
 ADD EPSR DATAVLAN command 280  
 ADD IGMP Snooping MCGROUP command 418  
 ADD IP ADDRESS command 196  
 ADD MLDSNOOPING MCGROUP command 430  
 ADD MSTP MSTI VLAN command 379  
 ADD NTP PEER command 146  
 ADD PORTAUTH PORT SUPPLICANTMAC command 499  
 ADD QOS FLOWGROUP command 457  
 ADD QOS POLICY command 458  
 ADD QOS TRAFFICCLASS command 459  
 ADD RADIUS SERVER command 180  
 ADD SNMP COMMUNITY command 113  
 ADD SWITCH FILTER command 292  
 ADD SWITCH TRUNK command 223  
 ADD VLAN PORT command 210

## B

bridge priority  
 Rapid Spanning Tree Protocol (RSTP) 365  
 BYE command 39

## C

CLS command 40  
 COPY command 75, 168  
 COPY FLASH TFTP command 106  
 COPY FLASH TOTALLY command 74  
 CREATE CLASSIFIER command 460  
 CREATE CONFIG command 76  
 CREATE DHCP Snooping MACFILTER command 306  
 CREATE EPSR command 281  
 CREATE MSTP MSTI command 380  
 CREATE QOS FLOWGROUP command 463  
 CREATE QOS POLICY command 465  
 CREATE QOS TRAFFICCLASS command 468  
 CREATE SNMP COMMUNITY command 115  
 CREATE SWITCH TRUNK command 224  
 CREATE TRIGGER command 346  
 CREATE VLAN command 212

## D

DELETE ACCESS FILTER ENTRY command 408  
 DELETE DCHPSNOOPING command 308  
 DELETE EPSR DATAVLAN command 283

DELETE FILE command 77  
 DELETE IGMP Snooping command 421  
 DELETE IP command 198  
 DELETE MLDSNOOPING command 432  
 DELETE MSTP MSTI VLAN command 381  
 DELETE NTP PEER command 147  
 DELETE PORTAUTH PORT SUPPLICANTMAC command 501  
 DELETE QOS FLOWGROUP command 471  
 DELETE QOS POLICY command 472  
 DELETE QOS TRAFFICCLASS command 473  
 DELETE RADIUS SERVER command 181  
 DELETE SNMP COMMUNITY command 118  
 DELETE SWITCH FILTER command 294  
 DELETE SWITCH TRUNK command 226  
 DELETE VLAN PORT command 213  
 DESTROY SNMP COMMUNITY command 119  
 DESTROY CLASSIFIER command 474  
 DESTROY DHCP Snooping MACFILTER command 309  
 DESTROY EPSR command 284  
 DESTROY MSTP MSTI command 382  
 DESTROY QOS FLOWGROUP command 475  
 DESTROY QOS POLICY command 476  
 DESTROY QOS TRAFFICCLASS command 477  
 DESTROY SWITCH TRUNK command 227  
 DESTROY TRIGGER command 349  
 DESTROY VLAN command 214  
 DISABLE ACCESS FILTER command 410  
 DISABLE DCHPSNOOPING command 310  
 DISABLE DHCP Snooping ARPSECURITY command 311  
 DISABLE DHCP Snooping LOG command 312  
 DISABLE DHCP Snooping OPTION82 command 313  
 DISABLE EPSR command 285  
 DISABLE FTP SERVER command 78  
 DISABLE HTTP SERVER command 174  
 DISABLE IGMP Snooping command 422  
 DISABLE INTERFACE LINKTRAP command 120  
 DISABLE IP DHCP command 199  
 DISABLE IP REMOTEASSIGN command 200  
 DISABLE LOG command 96  
 DISABLE LOG OUTPUT command 97  
 DISABLE MLDSNOOPING command 433  
 DISABLE MSTP command 383  
 DISABLE MSTP DEBUG MSTI command 384  
 DISABLE NTP command 148  
 DISABLE POE PORT command 334  
 DISABLE PORTAUTH command 502  
 DISABLE PORTAUTH PORT LOGTYPE command 503  
 DISABLE QOS command 442  
 DISABLE RADIUS ACCOUNTING command 182  
 DISABLE RSTP command 387  
 DISABLE SNMP command 121

DISABLE SNMP COMMUNITY command 122  
 DISABLE SNMP COMMUNITY TRAP command 123  
 DISABLE SNMP TRAP command 124  
 DISABLE STP command 362  
 DISABLE SUMMER-TIME command 149  
 DISABLE SWITCH AGEINGTIMER command 295  
 DISABLE SWITCH BPDUFORWARDING command 228  
 DISABLE SWITCH EAPFORWARDING command 229  
 DISABLE SWITCH INFILTERING command 230  
 DISABLE SWITCH LOOPDETECTION command 231  
 DISABLE SWITCH MIRROR command 232  
 DISABLE SWITCH PORT AUTOMDI command 234  
 DISABLE SWITCH PORT command 233  
 DISABLE SWITCH PORT FLOW command 235  
 DISABLE SWITCH POWERSAVE command 236  
 DISABLE SWITCH STORMDETECTION command 237  
 DISABLE SYSTEM FAN-STARTSTOP-ALARM command 41  
 DISABLE TELNET SERVER command 162  
 DISABLE TRIGGER command 350  
 DISABLE WEBAUTHSERVER command 505

**E**

edge ports

Rapid Spanning Tree Protocol (RSTP) 368  
 ENABLE ACCESS FILTER command 411  
 ENABLE DHCP Snooping ARPSECURITY command 316  
 ENABLE DHCP Snooping command 314  
 ENABLE DHCP Snooping LOG command 317  
 ENABLE DHCP Snooping OPTION82 command 318  
 ENABLE EPSR command 286  
 ENABLE FTP SERVER command 79  
 ENABLE HTTP SERVER command 175  
 ENABLE IGMP Snooping command 423  
 ENABLE INTERFACE LINKTRAP command 125  
 ENABLE IP DHCP command 201  
 ENABLE IP PROMOTEASSIGN command 202  
 ENABLE LOG command 98  
 ENABLE LOG OUTPUT command 99  
 ENABLE MLDSNOOPING command 434  
 ENABLE MSTP command 385  
 ENABLE MSTP DEBUG MSTI command 387  
 ENABLE NTP command 150  
 ENABLE POE PORT command 335  
 ENABLE PORTAUTH command 506  
 ENABLE PORTAUTH PORT LOGTYPE command 507  
 ENABLE QOS command 443  
 ENABLE RADIUSACCOUNTING command 183  
 ENABLE SNMP command 126  
 ENABLE SNMP COMMUNITY command 127  
 ENABLE SNMP COMMUNITY TRAP command 128  
 ENABLE SNMP TRAP command 129  
 ENABLE STP command 363  
 ENABLE SUMMER-TIME command 151  
 ENABLE SWITCH AGEINGTIMER command 296  
 ENABLE SWITCH BPDUFORWARDING command 238  
 ENABLE SWITCH EAPFORWARDING command 239  
 ENABLE SWITCH INFILTERING command 240

ENABLE SWITCH LOOPDETECTION command 241  
 ENABLE SWITCH MIRROR command 242  
 ENABLE SWITCH PORT AUTOMDI command 244  
 ENABLE SWITCH PORT FLOW command 245  
 ENABLE SWITCH POWERSAVE command 246  
 ENABLE SWITCH STORMDETECTION command 247  
 ENABLE SYSTEM FAN-STARTSTOP-ALARM command 42  
 ENABLE TELNET SERVER command 163  
 ENABLE TRIGGER command 351  
 ENABLE WEBAUTHSERVER command 509  
 ENALBE SWITCH PORT command 243  
 EXIT command 43

**F**

FLUSH LOG OUTPUT command 100  
 force version  
   Rapid Spanning Tree Protocol (RSTP) 365  
 forwarding delay  
   Rapid Spanning Tree Protocol (RSTP) 365

**H**

hello time  
   Rapid Spanning Tree Protocol (RSTP) 365  
 HELP command 44

**L**

LOAD command 80  
 LOGOUT command 46, 47

**M**

maximum age time  
   Rapid Spanning Tree Protocol (RSTP) 365  
 migration check  
   Rapid Spanning Tree Protocol (RSTP) 368

**P**

path cost  
   Rapid Spanning Tree Protocol (RSTP) 368  
 PING command 203  
 point-to-point ports  
   Rapid Spanning Tree Protocol (RSTP) 368  
 port cost  
   Rapid Spanning Tree Protocol (RSTP) 368  
 port priority  
   Rapid Spanning Tree Protocol (RSTP) 368  
 ports  
   configuring Rapid Spanning Tree Protocol (RSTP) parameters 368  
   displaying Rapid Spanning Tree Protocol (RSTP) parameters 371, 374, 375  
 PUERGE NTP command 152  
 PURGE CLASSIFIER command 478  
 PURGE DHCP Snooping command 319  
 PURGE EPSR command 287  
 PURGE LOG command 101  
 PURGE MSTP command 389  
 PURGE QOS command 444  
 PURGE STP command 364

PURGE TRIGGER command 352

## Q

QUIT command 48

## R

Rapid Spanning Tree Protocol (RSTP)

- configuring bridge settings 365
- configuring port settings 368
- disabling 362, 387
- displaying bridge settings 371, 374, 375
- displaying port settings 371, 374, 375
- enabling 363
- restoring default settings 364

RESET DHCP Snooping Counter command 320

RESET DHCP Snooping Database command 321

RESET MSTP Counter Port command 390

RESET NTP command 153

RESET QoS Policy Counter command 479

RESET Switch command 248

RESET Switch FDB command 297

RESET Switch Loop Detection Counter command 249

RESET Switch Port command 250

RESET Switch Storm Detection Counter command 251

RESTART command 49

## S

SET Access Filter command 412

SET Access Filter Entry command 413

SET ASYN command 164

SET Authentication command 184

SET Classifier command 480

SET CONFIG command 81

SET Console command 165

SET DHCP Snooping Check Interval command 322

SET DHCP Snooping Check Option command 323

SET DHCP Snooping MAC Filter command 324

SET DHCP Snooping Port command 324, 326

SET FTP Listen Port command 82

SET HTTP Listen Port command 176

SET IGMP Snooping command 424

SET IGMP Snooping MCGROUP command 426

SET INSTALL command 50

SET IP command 204

SET LED Mode command 353

SET LED Port command 354

SET Loader command 83

SET Log Output command 102

SET MLDSnooping command 435

SET MLDSnooping MCGROUP command 437

SET MSTP CIST command 393

SET MSTP CIST Port command 394

SET MSTP command 391

SET MSTP MSTI command 397

SET MSTP MSTI Port command 398

SET NTP command 154

SET Password command 51

SET POE Detect command 336

SET POE Guardband command 337

SET POE Management command 338

SET POE Port command 339

SET POE Threshold command 341

SET PortAuth AuthMethod command 510

SET PortAuth CSIDFormat command 511

SET PortAuth DHCP Server command 513

SET PortAuth Port (802.1X Authenticator Port) command 518

SET PortAuth Port (802.1X Supplicant Port) command 522

SET PortAuth Port (Authenticator Port for All Methods) command 514

SET PortAuth Port (Authenticator Port for MAC and Web) command 524

SET PortAuth Port (Canceling the Authentication Type) command 527

SET PortAuth Port SupplicantMAC command 528

SET PortAuth UserIDFormat command 529

SET QoS DSCP command 445

SET QoS FlowGroup command 483

SET QoS HwPriority command 446

SET QoS HwQueue command 448

SET QoS Policy command 485

SET QoS Scheduling command 449

SET QoS TrafficClass command 487

SET RADIUS command 185

SET RADIUS Accounting command 186

SET SNMP Community command 130

SET SNMP ListenPort command 132

SET SNMP Trap ListenPort command 133

SET STP command 365

SET STP Port command 368

SET Summer-Time command 157

SET Switch AgeingTimer command 298

SET Switch Limitation command 252

SET Switch Loop Detection command 253

SET Switch Mirror command 255

SET Switch Port command 257

SET Switch Storm Detection command 263

SET Switch Trunk command 266

SET System command 52

SET System SFP-Temperature Threshold command 53

SET Telnet command 167

SET TFTP ListenPort command 84

SET Time command 54

SET Trigger command 356

SET VLAN Port command 215

SET WebAuthServer command 531

SHOW Access Filter command 415

SHOW Authentication command 188

SHOW Classifier command 489

SHOW CONFIG command 85

SHOW Console command 169

SHOW CPU command 55

SHOW CrashLog command 105

SHOW Debug command 56

SHOW DHCP Snooping command 328

SHOW DHCP Snooping Counter command 329  
SHOW DHCP Snooping Database command 330  
SHOW DHCP Snooping MacFilter command 331  
SHOW DHCP Snooping Port command 332  
SHOW EPSR command 288  
SHOW EPSR Counter command 289  
SHOW FILE command 86  
SHOW FTP command 88  
SHOW HTTP Server command 177  
SHOW IGMP Snooping command 427  
SHOW INSTALL command 57  
SHOW INTERFACE command 134  
SHOW IP command 206  
SHOW LED command 359  
SHOW Loader command 89  
SHOW LOG Counter command 108  
SHOW LOG Output command 109  
SHOW LOG Status command 110  
SHOW MLDSnooping command 439  
SHOW MSTP command 399  
SHOW MSTP Counter Port command 401  
SHOW MSTP Debug MSTI command 402  
SHOW NTP command 158  
SHOW POE command 342  
SHOW POE Port command 343  
SHOW PortAuth command 532  
SHOW PortAuth Port Authenticator command 534  
SHOW PortAuth Port Supplicant command 536  
SHOW QoS command 450  
SHOW QoS DSCP command 451  
SHOW QoS FlowGroup command 493  
SHOW QoS HwPriority command 452  
SHOW QoS HwQueue command 453  
SHOW QoS Policy command 494  
SHOW QoS Policy Counter command 495  
SHOW QoS Scheduling command 454  
SHOW QoS TrafficClass command 496  
SHOW RADIUS command 190  
SHOW RADIUS Accounting command 191  
SHOW SNMP command 137  
SHOW SNMP Community command 140  
SHOW SNMP Trap command 142  
SHOW STP command 371, 374, 375  
SHOW Summer-Time command 160  
SHOW SWITCH command 267  
SHOW SWITCH Counter command 268  
SHOW SWITCH FDB command 299  
SHOW SWITCH Filter command 301  
SHOW SWITCH LoopDetection command 269  
SHOW SWITCH Mirror command 271  
SHOW SWITCH Port command 272  
SHOW SWITCH Port Counter command 274  
SHOW SWITCH StormDetection command 276  
SHOW SWITCH Trunk command 278  
SHOW SYSTEM command 58  
SHOW TELNET command 171  
SHOW TFTP command 90  
SHOW TIME command 61

SHOW TRIGGER command 360  
SHOW VLAN command 216  
SHOW WebAuthServer command 538

## U

UPLOAD command 91