

# Management Software

---

**AT-S63**



## Command Line User's Guide

For AT-9400 Switch Stacks

AT-S63 Version 3.2.0 for AT-9400 Basic Layer 3 Switches

Copyright © 2008 Allied Telesis, Inc.

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

Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications 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
How This Guide is Organized .....	14
Product Documentation .....	16
Where to Go First .....	17
Starting a Management Session .....	18
Document Conventions .....	19
Where to Find Web-based Guides .....	20
Contacting Allied Telesis .....	21
Online Support .....	21
Email and Telephone Support .....	21
Returning Products .....	21
Sales and Corporate Information .....	21
Management Software Updates .....	21
 <b>Section I: Basic Operations</b> .....	 23
<b>Chapter 1: Overview</b> .....	25
Introduction .....	26
AT-S63 Management Software .....	27
Supported Models .....	27
Supported Features .....	28
AT-StackXG Stacking Module .....	29
Maximum Number of Switches in a Stack .....	30
Management Interfaces .....	30
Management Access Methods .....	30
Enhanced Stacking .....	31
Stack Topology .....	32
Discovery Process .....	34
Master and Member Switches .....	35
Active Configuration File .....	36
Module ID Numbers .....	38
Static Module ID Numbers .....	38
Dynamic Module ID Numbers .....	39
Guidelines .....	41
Port Numbers in Commands .....	42
MAC Address Tables .....	43
File Systems .....	43
Compact Flash Memory Card Slots .....	43
Stack IP Address .....	44
Upgrading the AT-S63 Management Software .....	45
Powering On a Stack .....	46
Troubleshooting the Discovery Process .....	48

<b>Chapter 2: Starting a Command Line Management Session</b>	51
Starting a Local Management Session	52
Remote Telnet Management	54
Planning for Remote Management	54
Starting a Remote Telnet Management Session	54
Quitting a Management Session	56
Command Line Interface Features	57
Command Formatting	58
Redundant Twisted Pair Ports	59
<b>Chapter 3: Basic Command Line Commands</b>	61
CLEAR SCREEN	62
EXIT	63
HELP	64
LOGOFF, LOGOUT and QUIT	65
SAVE CONFIGURATION	66
SET PROMPT	67
SHOW USER	68
<b>Chapter 4: Stacking Commands</b>	69
SET STACK	70
SHOW STACK	72
<b>Chapter 5: Basic Stack Commands</b>	75
DISABLE TELNET	76
ENABLE TELNET	77
PING	78
RESET SWITCH	79
RESET SYSTEM	80
RESTART REBOOT	81
RESTART SWITCH	82
SET ASYN	84
SET DATE	85
SET PASSWORD MANAGER	86
SET PASSWORD OPERATOR	87
SET SWITCH CONSOLETIMER	88
SET SYSTEM	89
SET TELNET INSERTNULL	90
SET TIME	91
SET USER PASSWORD	92
SHOW ASYN	93
SHOW CONFIG DYNAMIC	94
SHOW CONFIG INFO	96
SHOW SWITCH	97
SHOW SYSTEM	100
SHOW TIME	102
<b>Chapter 6: SNMPv2 and SNMPv2c Commands</b>	103
ADD SNMP COMMUNITY	104
CREATE SNMP COMMUNITY	106
DELETE SNMP COMMUNITY	109
DESTROY SNMP COMMUNITY	111
DISABLE SNMP	112
DISABLE SNMP AUTHENTICATETRAP	113
DISABLE SNMP COMMUNITY	114
ENABLE SNMP	115
ENABLE SNMP AUTHENTICATETRAP	116
ENABLE SNMP COMMUNITY	117

SET SNMP COMMUNITY .....	118
SHOW SNMP .....	120
<b>Chapter 7: Port Parameter Commands</b> .....	123
DISABLE SWITCH PORT .....	124
DISABLE SWITCH PORT FLOW .....	125
ENABLE SWITCH PORT .....	126
ENABLE SWITCH PORT FLOW .....	127
PURGE SWITCH PORT .....	128
RESET SWITCH PORT .....	129
SET SWITCH PORT .....	130
SET SWITCH PORT FILTERING .....	134
SET SWITCH PORT RATELIMITING .....	137
SHOW SWITCH PORT .....	140
<b>Chapter 8: Port Statistics Commands</b> .....	145
RESET SWITCH PORT COUNTER .....	146
SHOW SWITCH MODULE COUNTER .....	147
SHOW SWITCH PORT COUNTER .....	150
<b>Chapter 9: MAC Address Table Commands</b> .....	151
ADD SWITCH FDB FILTER .....	152
DELETE SWITCH FDB FILTER .....	154
RESET SWITCH FDB .....	156
SET SWITCH AGINGTIMER AGEINGTIMER .....	157
SHOW SWITCH AGINGTIMER AGEINGTIMER .....	158
SHOW SWITCH FDB .....	159
<b>Chapter 10: Static Port Trunking Commands</b> .....	163
Overview .....	164
ADD SWITCH TRUNK .....	166
CREATE SWITCH TRUNK .....	168
DELETE SWITCH TRUNK .....	170
DESTROY SWITCH TRUNK .....	171
SET SWITCH TRUNK .....	172
SHOW SWITCH TRUNK .....	173
<b>Chapter 11: LACP Port Trunking Commands</b> .....	175
ADD LACP PORT .....	176
CREATE LACP AGGREGATOR .....	178
DELETE LACP PORT .....	180
DESTROY LACP AGGREGATOR .....	181
DISABLE LACP .....	182
ENABLE LACP .....	183
SET LACP AGGREGATOR .....	184
SET LACP SYSPRIORITY .....	186
SET LACP STATE .....	187
SHOW LACP .....	188
<b>Chapter 12: Port Mirroring Commands</b> .....	191
Overview .....	192
SET SWITCH MIRROR .....	193
SET SWITCH PORT MIRROR .....	194
SHOW SWITCH MIRROR .....	195

<b>Section II: Advanced Operations .....</b>	<b>197</b>
<b>Chapter 13: File System Commands .....</b>	<b>199</b>
Overview .....	200
COPY .....	201
CREATE CONFIG .....	203
DELETE FILE .....	204
FORMAT DEVICE .....	205
RENAME.....	206
SET CFLASH DIR.....	208
SET CONFIG .....	209
SHOW CFLASH.....	211
SHOW CONFIG .....	212
SHOW FILE .....	213
SHOW FLASH .....	214
<b>Chapter 14: File Download and Upload Commands .....</b>	<b>215</b>
LOAD METHOD=LOCAL.....	216
LOAD METHOD=TFTP.....	218
LOAD METHOD=XMODEM .....	223
UPLOAD METHOD=LOCAL.....	227
UPLOAD METHOD=TFTP.....	229
UPLOAD METHOD=XMODEM .....	232
<b>Chapter 15: Event Log and Syslog Client Commands .....</b>	<b>235</b>
ADD LOG OUTPUT .....	236
CREATE LOG OUTPUT .....	238
DESTROY LOG OUTPUT .....	242
DISABLE LOG .....	243
DISABLE LOG OUTPUT .....	244
ENABLE LOG .....	245
ENABLE LOG OUTPUT .....	246
PURGE LOG.....	247
SAVE LOG.....	248
SET LOG FULLACTION .....	250
SET LOG OUTPUT .....	251
SHOW LOG .....	254
SHOW LOG OUTPUT .....	259
SHOW LOG STATUS .....	261
<b>Chapter 16: Class of Service (CoS) Commands .....</b>	<b>263</b>
SET SWITCH PORT PRIORITY OVERRIDEPRIORITY .....	264
<b>Section III: Snooping Protocol .....</b>	<b>267</b>
<b>Chapter 17: IGMP Snooping Commands .....</b>	<b>269</b>
DISABLE IGMP Snooping .....	270
ENABLE IGMP Snooping .....	271
SET IP IGMP .....	272
SHOW IGMP Snooping .....	275
SHOW IP IGMP .....	277

## Section IV: SNMPv3 ..... 281

<b>Chapter 18: SNMPv3 Commands</b> .....	283
ADD SNMPV3 USER .....	285
CREATE SNMPV3 ACCESS .....	287
CREATE SNMPV3 COMMUNITY .....	290
CREATE SNMPV3 GROUP .....	292
CREATE SNMPV3 NOTIFY .....	294
CREATE SNMPV3 TARGETADDR .....	296
CREATE SNMPV3 TARGETPARAMS .....	298
CREATE SNMPV3 VIEW .....	300
DELETE SNMPV3 USER .....	302
DESTROY SNMPv3 ACCESS .....	303
DESTROY SNMPv3 COMMUNITY .....	305
DESTROY SNMPv3 GROUP .....	306
DESTROY SNMPv3 NOTIFY .....	307
DESTROY SNMPv3 TARGETADDR .....	308
DESTROY SNMPv3 TARGETPARMS .....	309
DESTROY SNMPV3 VIEW .....	310
PURGE SNMPV3 ACCESS .....	311
PURGE SNMPV3 COMMUNITY .....	312
PURGE SNMPV3 NOTIFY .....	313
PURGE SNMPV3 TARGETADDR .....	314
PURGE SNMPV3 VIEW .....	315
SET SNMPV3 ACCESS .....	316
SET SNMPV3 COMMUNITY .....	318
SET SNMPV3 GROUP .....	320
SET SNMPV3 NOTIFY .....	322
SET SNMPV3 TARGETADDR .....	324
SET SNMPV3 TARGETPARAMS .....	326
SET SNMPV3 USER .....	328
SET SNMPV3 VIEW .....	330
SHOW SNMPV3 ACCESS .....	332
SHOW SNMPV3 COMMUNITY .....	333
SHOW SNMPv3 GROUP .....	334
SHOW SNMPV3 NOTIFY .....	335
SHOW SNMPV3 TARGETADDR .....	336
SHOW SNMPV3 TARGETPARAMS .....	337
SHOW SNMPV3 USER .....	338
SHOW SNMPV3 VIEW .....	339

## Section V: Spanning Tree Protocols ..... 341

<b>Chapter 19: Spanning Tree Protocol Commands</b> .....	343
ACTIVATE STP .....	344
DISABLE STP .....	345
ENABLE STP .....	346
PURGE STP .....	347
SET STP .....	348
SET STP PORT .....	351
SET SWITCH MULTICASTMODE .....	353
SHOW STP .....	355

<b>Chapter 20: Rapid Spanning Tree Protocols Commands</b> .....	357
ACTIVATE RSTP .....	358
DISABLE RSTP .....	359
ENABLE RSTP .....	360
PURGE RSTP .....	361
SET RSTP .....	362
SET RSTP PORT .....	365
SHOW RSTP .....	368
 <b>Section VI: Virtual LANs</b> .....	 371
<b>Chapter 21: Port-based and Tagged VLAN Commands</b> .....	373
ADD VLAN .....	374
CREATE VLAN .....	376
DELETE VLAN .....	379
DESTROY VLAN .....	382
SET SWITCH INFILTRING .....	383
SET VLAN .....	384
SHOW VLAN .....	385
 <b>Section VII: Internet Protocol Routing</b> .....	 387
<b>Chapter 22: Internet Protocol Version 4 Packet Routing Commands</b> .....	389
ADD IP ARP .....	390
ADD IP INTERFACE .....	392
ADD IP ROUTE .....	394
DELETE IP ARP .....	396
DELETE IP INTERFACE .....	397
DELETE IP ROUTE .....	398
PURGE IP .....	399
SET IP ARP .....	400
SET IP ARP TIMEOUT .....	402
SET IP INTERFACE .....	403
SET IP LOCAL INTERFACE .....	405
SET IP ROUTE .....	406
SHOW IP ARP .....	408
SHOW IP COUNTER .....	410
SHOW IP INTERFACE .....	412
SHOW IP ROUTE .....	414
 <b>Section VIII: Port Security</b> .....	 419
<b>Chapter 23: 802.1x Port-based Network Access Control Commands</b> .....	421
DISABLE PORTACCESS PORTAUTH .....	422
DISABLE RADIUSACCOUNTING .....	423
ENABLE PORTACCESS PORTAUTH .....	424
ENABLE RADIUSACCOUNTING .....	425
SET PORTACCESS PORTAUTH PORT ROLE=AUTHENTICATOR .....	426
SET PORTACCESS PORTAUTH PORT ROLE=SUPPLICANT .....	435
SET RADIUSACCOUNTING .....	437
SHOW PORTACCESS PORTAUTH .....	439
SHOW PORTACCESS PORTAUTH PORT .....	441
SHOW RADIUSACCOUNTING .....	444



<b>Chapter 24: RADIUS Commands</b> .....	447
ADD RADIUSSERVER.....	448
DELETE RADIUSSERVER .....	450
PURGE AUTHENTICATION .....	451
SET AUTHENTICATION.....	452
SHOW AUTHENTICATION.....	453
 <b>Section IX: Management Security</b> .....	<b>455</b>
 <b>Chapter 25: Web Server Commands</b> .....	457
DISABLE HTTP SERVER .....	458
ENABLE HTTP SERVER .....	459
PURGE HTTP SERVER.....	460
SHOW HTTP SERVER .....	461
 <b>Index</b> .....	463



# Tables

---

Table 1. Maximum Number of Switches in a Stack of both 24-port and 48-port Switches .....	30
Table 2. Module Variable .....	94
Table 3. File Extensions and File Types .....	201
Table 4. File Name Extensions - Downloading Files .....	219
Table 5. File Name Extensions - Uploaded Files .....	230
Table 6. Default Syslog Facilities .....	240
Table 7. Numerical Code and Facility Level Mappings .....	241
Table 8. AT-S63 Modules .....	255
Table 9. Event Log Severity Levels .....	257
Table 10. Bridge Priority Value Increments .....	348
Table 11. STP Auto-Detect Port Costs .....	351
Table 12. Auto-Detect Port Trunk Costs .....	351
Table 13. Port Priority Value Increments .....	352
Table 14. Bridge Priority Value Increments .....	362
Table 15. RSTP Auto-Detect Port Costs .....	365
Table 16. RSTP Auto-Detect Port Trunk Costs .....	366
Table 17. Port Priority Value Increments .....	366



# Preface

---

This guide describes the command line interface of the AT-S63 Management Software for the AT-9400 Basic Layer 3 Gigabit Ethernet Switches. The commands detailed in this guide are used to manage the network operations of AT-9400 Switches that have been assembled into a stack with the AT-StackXG Stacking Module.

This Preface has the following sections:

- ❑ “How This Guide is Organized” on page 14
- ❑ “Product Documentation” on page 16
- ❑ “Where to Go First” on page 17
- ❑ “Starting a Management Session” on page 18
- ❑ “Document Conventions” on page 19
- ❑ “Where to Find Web-based Guides” on page 20
- ❑ “Contacting Allied Telesis” on page 21



## **Caution**

The software described in this documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a “retail encryption item” in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesis sales representative for current information on this product’s export status.

---

## How This Guide is Organized

---

This guide has the following sections and chapters:

❑ Section I: Basic Operations

Chapter 1, “Overview” on page 25

Chapter 2, “Starting a Command Line Management Session” on page 51

Chapter 3, “Basic Command Line Commands” on page 61

Chapter 4, “Stacking Commands” on page 69

Chapter 5, “Basic Stack Commands” on page 75

Chapter 6, “SNMPv2 and SNMPv2c Commands” on page 103

Chapter 7, “Port Parameter Commands” on page 123

Chapter 8, “Port Statistics Commands” on page 145

Chapter 9, “MAC Address Table Commands” on page 151

Chapter 10, “Static Port Trunking Commands” on page 163

Chapter 11, “LACP Port Trunking Commands” on page 175

Chapter 12, “Port Mirroring Commands” on page 191

❑ Section II: Advanced Operations

Chapter 13, “File System Commands” on page 199

Chapter 14, “File Download and Upload Commands” on page 215

Chapter 15, “Event Log and Syslog Client Commands” on page 235

Chapter 16, “Class of Service (CoS) Commands” on page 263

❑ Section III: Snooping Protocol

Chapter 17, “IGMP Snooping Commands” on page 269

❑ Section IV: SNMPv3

Chapter 18, “SNMPv3 Commands” on page 283

❑ Section V: Spanning Tree Protocols

Chapter 19, “Spanning Tree Protocol Commands” on page 343

Chapter 20, “Rapid Spanning Tree Protocols Commands” on page 357

- ❑ Section VI: Virtual LANs

- Chapter 21, “Port-based and Tagged VLAN Commands” on page 373

- ❑ Section VII: Internet Protocol Routing

- Chapter 22, “Internet Protocol Version 4 Packet Routing Commands” on page 389

- ❑ Section VIII: Port Security

- Chapter 23, “802.1x Port-based Network Access Control Commands” on page 421

- Chapter 24, “RADIUS Commands” on page 447

- ❑ Section IX: Management Security

- Chapter 25, “Web Server Commands” on page 457

## Product Documentation

---

For overview information on the features of the AT-9400 Switch and the AT-S63 Management Software, refer to:

- ❑ AT-S63 Management Software Features Guide  
(PN 613-001022)

For instructions on starting a local or remote management session on a stand-alone AT-9400 Switch or a stack, refer to:

- ❑ Starting an AT-S63 Management Session Guide  
(PN 613-001023)

For instructions on installing or managing a stand-alone AT-9400 Switch, refer to:

- ❑ AT-9400 Gigabit Ethernet Switch Installation Guide  
(PN 613-000987)
- ❑ AT-S63 Management Software Menus User's Guide  
(PN 613-001025)
- ❑ AT-S63 Management Software Command Line User's Guide  
(PN 613-001024)
- ❑ AT-S63 Management Software Web Browser User's Guide  
(PN 613-001026)

For instructions on installing or managing a stack of AT-9400 Basic Layer 3 Switches, refer to:

- ❑ AT-9400 Stack Installation Guide  
(PN 613-000796)
- ❑ AT-S63 Stack Command Line User's Guide  
(PN 613-001027)
- ❑ AT-S63 Stack Web Browser User's Guide  
(PN 613-001028)



## Where to Go First

---

Allied Telesis recommends that you read Chapter 1, Overview, in the *AT-S63 Management Software Features Guide* before you begin to manage the switch for the first time. There you will find a variety of basic information about the unit and the management software, like the two levels of manager access levels and the different types of management sessions.

The *AT-S63 Management Software Features Guide* is also your resource for background information on the features of the switch. You can refer there for the relevant concepts and guidelines before you begin to configure a feature for the first time.

## Starting a Management Session

---

For instructions on how to start a local or remote management session on a stack, refer to the *Starting an AT-S63 Management Session Guide* or Chapter 2, “Starting a Command Line Management Session” on page 51 in this guide.

## 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 Allied Telesis products are available in portable document format (PDF) on our web site at **[www.alliedtelesis.com](http://www.alliedtelesis.com)**. You can view the documents online or download them onto a local workstation or server.

## Contacting Allied Telesis

---

This section provides Allied Telesis contact information for technical support and for sales and corporate information.

### Online Support

You can request technical support online from the Allied Telesis Knowledge Base at **[www.alliedtelesis.com/support/kb.aspx](http://www.alliedtelesis.com/support/kb.aspx)**. You can submit questions to our technical support staff from the Knowledge Base and review answers to previously asked questions.

### Email and Telephone Support

For Technical Support via email or telephone, refer to the Allied Telesis web site at **[www.alliedtelesis.com](http://www.alliedtelesis.com)**. Select your country from the list on the web site and then select the appropriate tab.

### Returning Products

Products for return or repair must be assigned Return Materials Authorization (RMA) numbers. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact the Allied Telesis Technical Support group at **[www.alliedtelesis.com/support/rma.aspx](http://www.alliedtelesis.com/support/rma.aspx)**.

### Sales and Corporate Information

You can contact Allied Telesis for sales or corporate information at our web site at **[www.alliedtelesis.com](http://www.alliedtelesis.com)**.

### Management Software Updates

New releases of management software for our managed products are available from the following Internet sites:

- ❑ Allied Telesis web site: **[www.alliedtelesis.com](http://www.alliedtelesis.com)**
- ❑ Allied Telesis FTP server: **<ftp://ftp.alliedtelesis.com>**

If the FTP server prompts you to log on, enter "anonymous" as the user name and your email address as the password.



## Section I

# Basic Operations

---

The chapters in this section include:

- ❑ Chapter 1, “Overview” on page 25
- ❑ Chapter 2, “Starting a Command Line Management Session” on page 51
- ❑ Chapter 3, “Basic Command Line Commands” on page 61
- ❑ Chapter 4, “Stacking Commands” on page 69
- ❑ Chapter 5, “Basic Stack Commands” on page 75
- ❑ Chapter 6, “SNMPv2 and SNMPv2c Commands” on page 103
- ❑ Chapter 7, “Port Parameter Commands” on page 123
- ❑ Chapter 8, “Port Statistics Commands” on page 145
- ❑ Chapter 9, “MAC Address Table Commands” on page 151
- ❑ Chapter 10, “Static Port Trunking Commands” on page 163
- ❑ Chapter 11, “LACP Port Trunking Commands” on page 175
- ❑ Chapter 12, “Port Mirroring Commands” on page 191





# Chapter 1

## Overview

---

This chapter has the following sections:

- ❑ “Introduction” on page 26
- ❑ “AT-S63 Management Software” on page 27
- ❑ “Supported Models” on page 27
- ❑ “Supported Features” on page 28
- ❑ “AT-StackXG Stacking Module” on page 29
- ❑ “Maximum Number of Switches in a Stack” on page 30
- ❑ “Management Interfaces” on page 30
- ❑ “Management Access Methods” on page 30
- ❑ “Enhanced Stacking” on page 31
- ❑ “Stack Topology” on page 32
- ❑ “Discovery Process” on page 34
- ❑ “Master and Member Switches” on page 35
- ❑ “Active Configuration File” on page 36
- ❑ “Module ID Numbers” on page 38
- ❑ “Port Numbers in Commands” on page 42
- ❑ “MAC Address Tables” on page 43
- ❑ “File Systems” on page 43
- ❑ “Compact Flash Memory Card Slots” on page 43
- ❑ “Stack IP Address” on page 44
- ❑ “Upgrading the AT-S63 Management Software” on page 45
- ❑ “Powering On a Stack” on page 46
- ❑ “Troubleshooting the Discovery Process” on page 48

## Introduction

---

The switches in the AT-9400 Series are divided into the Layer 2+ group and the Basic Layer 3 group. The two groups share many of the same features, but there are a number of significant differences. For instance, the Internet Protocol version 4 packet routing feature and the Virtual Router Redundancy Protocol are supported only on the Basic Layer 3 switches.

Three models in the Basic Layer 3 series support an additional feature called stacking. What stacking allows you to do is assemble the switches so that they function as a unified Gigabit Ethernet switch, rather than as independent units. As a stack, the switches synchronize their actions so that network operations, like spanning tree protocols, virtual LANs, and static port trunks, are able to span across all of their Gigabit Ethernet ports.

The two principal advantages of stacking are:

- ❑ You can configure all of the switches in a stack simultaneously from the same management session, rather than individually from different sessions. This can simplify network management.
- ❑ You have more latitude in how you configure some of the features. For instance, when creating a static port trunk on a stand-alone switch you have to choose ports from the same switch. In contrast, a static trunk on a stack can have ports from different switches in the same stack.

## AT-S63 Management Software

---

Stacking requires Version 3.0.0 or later of the AT-S63 Management Software.

---

**Note**

Version 3.0.0 is only supported on the AT-9424T, AT-9424T/POE, AT-9424Ts, AT-9424Ts/XP, AT-9448T/SP, and AT-9448Ts/XP Basic Layer 3 Switches. Do not install it on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP Layer 2+ Switches.

---

## Supported Models

---

Stacking is only supported on the following AT-9400 Switches:

- ☐ AT-9424Ts
- ☐ AT-9424Ts/XP
- ☐ AT-9448Ts/XP

## Supported Features

---

A stack supports these features of the AT-S63 Management Software:

- ❑ Local Management
- ❑ Remote Telnet management
- ❑ Remote web browser management
- ❑ SNMPv1, v2c, and v3
- ❑ Basic port configuration
  - Port status (enabled or disabled)
  - Auto-Negotiation
  - Speed
  - Duplex-mode
  - Flow control and backpressure
  - MDI or MDI-X setting
  - Packet filtering and rate limiting
- ❑ Port statistics
- ❑ Static port trunks
- ❑ Link Aggregation Control Protocol (LACP) trunks
- ❑ Port mirroring
- ❑ Event log
- ❑ Syslog client
- ❑ Class of Service
- ❑ Internet Group Management Protocol (IGMP) snooping
- ❑ Spanning tree protocol (STP)
- ❑ Rapid spanning tree protocol (RSTP)
- ❑ Port-based and tagged VLANs
- ❑ Internet Protocol Version 4 packet routing with static routes (Does not support the Routing Information Protocol.)
- ❑ Basic 802.1x port-based network access control using the RADIUS authentication protocol
- ❑ Additional manager accounts using the RADIUS or TACACS+ authentication protocol

All of the other features in the AT-S63 Management Software are automatically deactivated when a stack is powered on.

## AT-StackXG Stacking Module

---

The AT-9400 Switch must have the AT-StackXG Stacking Module, shown in Figure 1, to be part of a stack. You install the module in the switch's expansion slot on the back panel. For installation instructions, refer to the *AT-9400 Stack Installation Guide*.

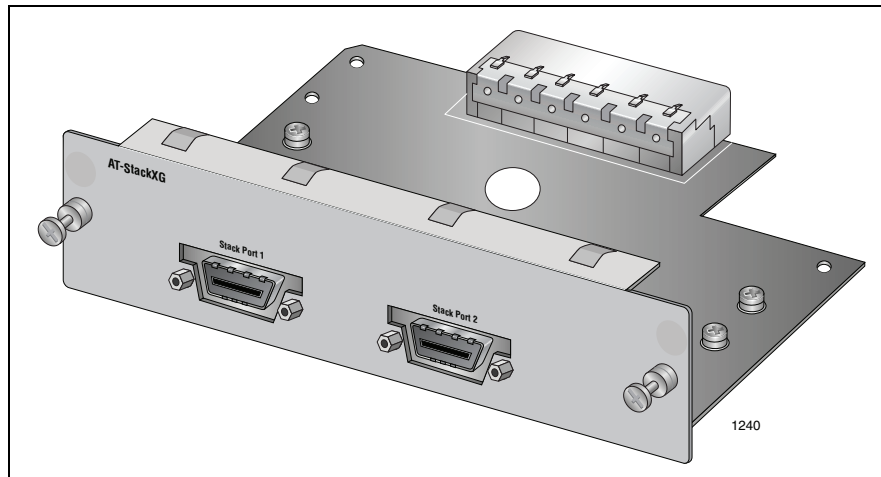


Figure 1. AT-StackXG Stacking Module

## Maximum Number of Switches in a Stack

Stacks of the 24-port AT-9424Ts Switch or the AT-9424Ts/XP Switch can have up to eight units. A stack can have both models and either model can be the master switch of the stack.

Allied Telesis does not recommend using the 48-port AT-9448Ts/XP Switch as the master switch of a stack. Consequently, a stack with one or more 48-port switches should have as the master switch the 24-port AT-9424Ts Switch or the AT-9424Ts/XP Switch. For stacks of more than three switches, both the master switch and the backup switch should be 24-port switches. A mixed stack of both 24-port and 48-port switches should not have more than four AT-9448Ts/XP Switches and should not exceed a total of eight units, as shown in this table.

Table 1. Maximum Number of Switches in a Stack of both 24-port and 48-port Switches

	Number of 24-Port AT-9424Ts and AT-9424Ts/XP Switches							
		1	2	3	4	5	6	7
Number of 48-Port AT-9448Ts/XP Switches	1							
	2							
	3							
	4							

## Management Interfaces

The AT-S63 Management Software has three management interfaces: menus, command line commands, and web browser windows. You can use either the command line commands or the web browser windows to manage a stack. The menus are only supported when the switches are used as stand-alone devices.

## Management Access Methods

You can manage a stack locally through the Terminal Port on the master switch or remotely using a Telnet client or a web browser (HTTP). A stack does not support the Secure Shell (SSH) protocol, secured web browser windows (HTTPS) or enhanced stacking.

## Enhanced Stacking

---

If you have prior experience with Allied Telesis products, you might already be familiar with a feature that happens to have a similar name to the feature discussed in this manual. The feature is *enhanced stacking* and what it allows you to do is manage the different Allied Telesis switches in your network from one management session by redirecting the management session from switch to switch. This can save you time as well as reduce the number of IP addresses that you have to assign to the managed devices in your network.

It is important not to confuse the stacking feature explained in this guide with enhanced stacking because they have no functional or operational similarities. Their principal differences are outlined here.

In a stack:

- ❑ The AT-9400 Gigabit Ethernet Switches operate as a single, logical unit in which functions such as static port trunks and port mirrors, are able to span all the devices in the stack.
- ❑ The switches are managed as a unit.
- ❑ The switches in a stack have the same MAC address tables.
- ❑ The switches must be installed in the same equipment rack.
- ❑ The switches are linked together with the AT-StackXG Stacking Module.
- ❑ The stacking feature is only supported on the AT-9424Ts, AT-9424Ts/XP, and AT-9448Ts/XP Switches.

In enhanced stacking:

- ❑ The AT-9400 Gigabit Ethernet Switches operate as independent units.
- ❑ Though the switches of an enhanced stack can be accessed from the same management session, they must still be configured individually.
- ❑ Each switch maintains its own MAC address table.
- ❑ The devices can be located across a large geographical area.
- ❑ The switches are connected together with a common virtual LAN.
- ❑ Enhanced stacking is supported by all AT-9400 Gigabit Ethernet Switches, as well as other Allied Telesis managed products.

The stacking feature does not support enhanced stacking. A stack can be managed locally through the Terminal Port on the master switch of the stack or remotely with a Telnet client or a web browser.

## Stack Topology

The switches of a stack are cabled with the AT-StackXG Stacking Module and its two full-duplex, 12-Gbps stacking ports. There are two supported topologies. The first topology is the duplex-chain topology, where a port on one stacking module is connected to a port on the stacking module in the next switch, which is connected to the next switch, and so on. The connections must crossover to different numbered ports on the modules. Port 1 on the stacking module in one switch must be connected to Port 2 on the stacking module in the next switch. An example of this topology of a stack of four switches is illustrated in Figure 2.

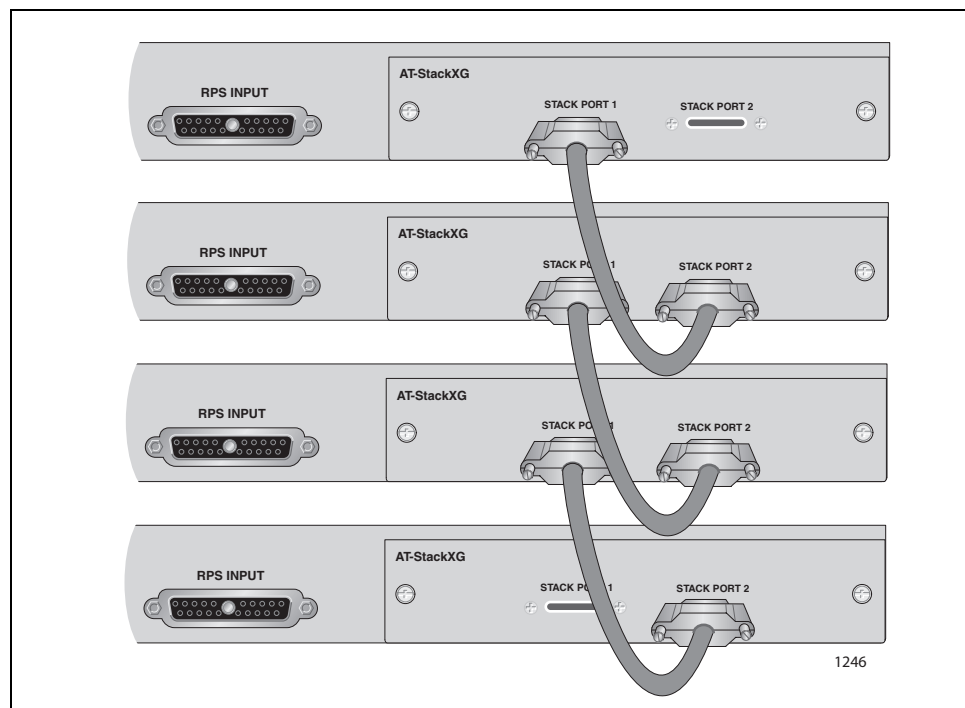


Figure 2. Duplex-chain Topology

The second topology, the duplex-ring topology, is identical to the daisy-chain, except that the stacking module in the switch at the top of the stack is connected to the stacking module in the switch at the bottom of the stack to form a physical loop. An example of this topology is shown in Figure 3.



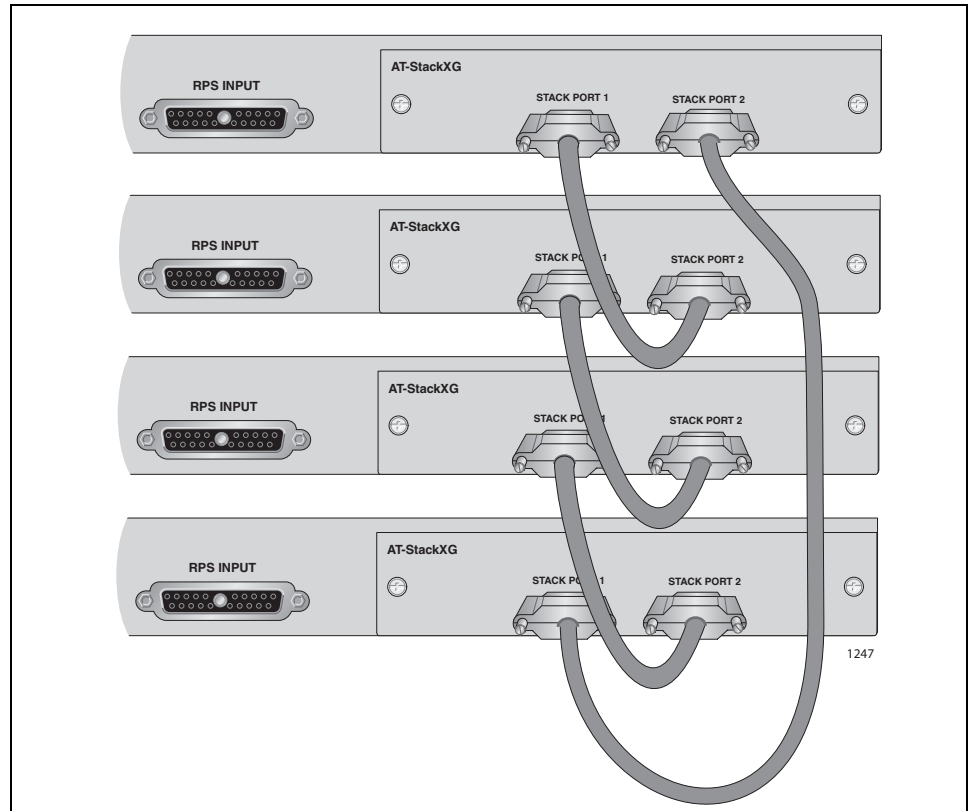


Figure 3. Duplex-ring Topology

Both topologies offer the same in terms of network speed and performance. But the duplex-ring topology adds redundancy by providing a secondary path through the stacking modules. This can protect a stack against the failure of a stacking port or cable. A disruption in the primary path automatically activates the secondary path.

## Discovery Process

---

When the switches of a stack are powered on or reset, they synchronize their operating software in a two phase process before they begin to forward network traffic through their ports.

In the first phase the switches initialize their AT-S63 Management Software. It takes about one minute for a switch to fully initialize its software.

In the second phase the switches determine the number of devices in the stack, the cabling topology of the stacking modules, and, in the case of the duplex-ring topology, the active path through the stacking modules. It is also in this phase that the master switch of the stack is identified and the parameter settings of the devices are configured with the commands in the active configuration file in the master switch's file system.

This second phase is referred to as the discovery process. The length of time of the discovery process can vary depending on a number of factors, like the number of switches in the stack, the switch models, and the number and complexity of the commands in the active configuration file on the master switch. For instance, a small stack of two switches might take less than fifteen seconds to complete the discovery process, while a stack of eight AT-9424Ts Switches might take several minutes.

When the discovery process is finished the switches of the stack begin to forward network traffic from their ports.

A stack will perform both phases whenever the switches are powered on or reset. However, a stack will automatically repeat the discovery phase whenever there is change to its topology or composition. For example, disconnecting a stacking cable from a stacking module, powering off a switch, or adding or removing a switch from the stack are all examples of events that will prompt a repetition of the discovery process.

Since the switches of a stack do not forward traffic during the discovery process, a change to a stack's topology will be disruptive to the activity of your network. Consequently, changes to the composition of a stack should be scheduled during periods of low network traffic to minimize the impact on your network.

## Master and Member Switches

---

A stack must have a master switch to coordinate the activity of the devices. There can be only one master switch, but it can be any unit. In a stack with different AT-9400 Switch models, the master switch can be any model. The master switch is selected during the discovery process and is based on the module ID numbers of the units, as explained in “Module ID Numbers” on page 38. The master switch has module ID 1.

The other switches of a stack are called as member switches.

## Active Configuration File

---

The parameter settings of the stack are stored in the active configuration file in the master switch's file system. In the file are the commands that reestablish the current configuration of the ports and switches in the stack. The file is used by the master switch whenever the stack performs the discovery process, such as after a reset or a power cycle, or a change to a stack's composition.

The master switch does not automatically update the active configuration file when a change is made to a parameter setting on a stack device. Instead, you must manually initiate the update with the `SAVE CONFIGURATION` command. In response to the command, the master switch polls all of the devices in the stack for their current settings and updates the active configuration file. Since changes to the parameter settings that are not saved to the configuration file are discarded whenever the stack performs the discovery process, you should always perform the `SAVE CONFIGURATION` command after you have made changes to parameter settings that you want the stack to retain.

If the switches of a stack have static module ID numbers, a backup copy of the master switch's active configuration file is stored in the file system in the switch assigned module ID 2. The backup configuration file is updated whenever the `SAVE CONFIGURATION` command is issued, and so is an exact duplicate of the active configuration file on the master switch.

Under normal operating conditions, the backup configuration file remains inactive. However, if the master switch stops operating or is removed from the stack, the switch assigned module ID 2 assumes the role of the master switch during the subsequent discovery process and configures the stack devices with its backup copy of the configuration file. If the original master switch resumes operations, it reassumes the master switch role after the discovery process and configures the stack with the active configuration file in its file system. The configuration file on the switch assigned module ID 2 reverts to its backup status.

Beginning with Version 3.0.0 of the AT-S63 Management Software a switch has two default configuration files. One file is for stand-alone operation and the other for stack operation, specifically when it is the master switch of a stack. A switch chooses the appropriate file during the discovery process. If, during the process, the switch determines it is not part of a stack, it uses its stand-alone configuration file to set its parameter settings. If it is the master switch of a stack, it uses its stack configuration file to set the parameter settings of all the devices. Finally, if the switch detects that it is part of a stack, but is not the master switch, it ignores the configuration files in its file system and waits to receive its settings from the master switch.

By having two standard configuration files, a switch can retain its prior configuration settings when converted from a stand-alone configuration to a stack member, or vice versa. This saves you the trouble of having to reconfigure the device.

It should be noted, however, that the parameter settings from a stand-alone configuration file cannot be transferred to a stack configuration file. For a switch to have the same settings in a stack that it had as a stand-alone device, you must reapply the settings after adding the switch to the stack.

## Module ID Numbers

---

A switch has to have a unique module ID number in the range of 1 to 5 or 1 to 8 to be a member of a stack. The two ranges happen to correspond to the maximum size of a stack, as explained in “Maximum Number of Switches in a Stack” on page 30.

The switch assigned module ID number 1 becomes the stack’s master switch.

The switches of a stack are identified in the boot configuration file on the master switch by their module ID numbers. Consequently, any change to the numbering system of the switches of an established stack can have a significant impact on the configurations of the units.

Module ID numbers can be assigned two ways. The preferred method is to assign the numbers yourself with the SET STACK command. Module ID numbers assigned in this fashion are referred to as static numbers because the switches retain their numbers even when new switches are added or removed from a stack.

The second approach is to have the management software make the assignments automatically during the discovery process of a stack. These numbers are called dynamic module ID numbers because they can change if the composition of a stack changes.

The commands for managing the module ID numbers are “SET STACK” on page 70 and “SHOW STACK” on page 72. The SET STACK command should only be used when a switch is functioning as a stand-alone device, because changing a switch’s module ID number when the unit is part of a stack can have unpredictable results.

### Static Module ID Numbers

Static module ID numbers are preferred over dynamic numbers for the following reasons:

- ❑ You can number the devices to reflect their order in the equipment rack, making them easier to identify.
- ❑ A stack with static module ID numbers stores a backup copy of the active configuration file on the switch assigned ID number 2. For information, refer to “Active Configuration File” on page 36.
- ❑ It is easier to replace a member switch. A new switch assigned the same module ID number of the switch that it replaces assumes the same configuration. This will save you from having to configure the new unit.

Static module ID numbers are assigned with the SET STACK command. The numbers should be assigned when the switches are operating as stand-alone devices, because there can be unpredictable results if you assign the numbers when the switches are part of a stack.

The switches should be numbered starting with ID number 1. The switch assigned ID number 1 will be the master switch of the stack. Any switch can be the master switch, but it should be either the top or bottom switch in the stack to make it easy to identify. Additionally, the switches do not have to be numbered in the same order as their arrangement in the rack in relation to the master switch, but they will be easier to identify if their numbers and their order in the stack are the same.

## **Dynamic Module ID Numbers**

Dynamic module ID numbers are based on the MAC addresses of the units and are automatically assigned by the management software during the discovery process of the stack,. The module ID 1 is assigned to the switch with the lowest MAC address. That switch becomes the master switch of the stack. The module ID 2 is assigned to the switch with the second lowest address, and so on.

Dynamic module ID numbers are a quick way to build a stack, but they can be problematic, especially for stacks of more than two switches. First, although the switches of a stack do not have to be numbered in any special order, they will be easier to identify if they are numbered in sequence starting with the top or the bottom unit. With dynamic module ID numbers, there is no guarantee that will happen. For example, a stack of five switches might be assigned these dynamic module ID numbers starting with the top unit: 2, 4, 1, 3, 5. Such a numbering sequence could easily lead to confusion and mistakes when you configure the devices.

Another drawback to this approach is that the assignments of the numbers could change if you were to add or remove a switch from a stack. This, in turn, could alter the configurations of the switches because, as explained previously, the switches are identified by their module ID numbers in the active configuration file on the master switch. For instance, if you were to add a new switch whose MAC address was lower than the MAC address of an existing switch, the module ID assignments of one or more of the devices would change and so, in all likelihood, would their configurations. The new switch would take on the module ID number and configuration of a preexisting switch since it has a lower MAC address, while the displaced switch would assume another module ID number and configuration, and so on.

Furthermore, if a new switch's MAC address is the lowest in the stack, it becomes the new master switch. The entire stack would probably lose its configuration, because the new master switch would be unlikely to have the same stack configuration file as the previous master switch.

It should also be noted that a backup master switch is not supported in a stack with dynamic module ID numbers. That feature is reserved for stacks with static ID numbers.

If you do decide to use the dynamic method for assigning module ID numbers, there is a way for controlling the ID numbers assignments by assigning each switch a stack priority value with the SET STACK

command. A switch can have only one stack priority value. The lower the number, the higher the priority. The switch with the lowest stack priority is assigned module ID 1 and becomes the master switch. The switch with the next lowest priority is assigned module ID 2, and so on. In cases where switches have the same priority value, ID number assignments are based on MAC addresses, as explained previously.

The range of the stack priority value is 1 to 16. The default is 16. It is important not to confuse the range of this parameter with the permitted number of switches in a stack. There is no correlation between the two.

The following example of a stack of four switches illustrates how the management software uses the stack priority value to assign module ID numbers:

- ❑ Switch A is assigned the stack priority value 2.
- ❑ Switch B is assigned the stack priority value 5.
- ❑ Switches C and D use the default priority value 16.

Switch A, having the lowest priority value, would be assigned module ID value 1 by the management software and would become the master switch of the stack. Switch B, having the next lowest priority value, would be assigned module ID 2. Switches C and D, having identical priority values, would be assigned module ID numbers based on their MAC addresses. The switch with the lower MAC address would be assigned module ID 3 and the last switch would be assigned module ID 4.

Of course, you could assign the stack priority values starting at 1 for the switches of a stack, as shown here, and so create a direct correlation between a switch's stack priority number and its module ID number assignments:

- ❑ Switch A is assigned the priority value 1.
- ❑ Switch B is assigned the priority value 2.
- ❑ Switches C is assigned the priority value 3.
- ❑ Switches D is assigned the priority value 4.

In this scenario, a switch's priority value and module ID number would match. But, of course, this approach is really no different than assigning static module ID numbers to the switches.



## Guidelines

Here are the guidelines for module ID numbers:

- ❑ Each switch must have a unique module ID number.
- ❑ The module ID numbers are set with the SET STACK command and displayed with the SHOW STACK command. The SET STACK command should only be used when a switch is operating as a stand-alone device. Setting a switch's module ID number while it is part of a stack can have unpredictable results. For information, refer to "SET STACK" on page 70 and "SHOW STACK" on page 72.
- ❑ If you use static module ID numbers, number the devices starting at 1.
- ❑ The switch assigned the dynamic or static module ID number 1 is the master switch of the stack.
- ❑ If you use static module ID numbers, the switch assigned module ID number 2 functions as the backup master switch. Dynamic module ID numbers do not support a backup master switch.
- ❑ Static module ID numbers do not have to be consecutive (for example, 1, 2, 4), but this is not recommended because it can make it difficult to match a switch with its appropriate module ID number, which in turn could lead to mistakes when configuring the devices.
- ❑ The parameter settings in the active configuration file on the master switch are tied to the module ID numbers. If, for any reason, the numbering sequence of the devices in a stack changes, which can happen with dynamic module ID numbers, a mismatch could result between the devices and their corresponding parameter settings in the file. It is because of this that Allied Telesis recommends controlling the assignment of the module ID numbers with static numbers.
- ❑ The module ID numbers of the switches do not have to match the physical arrangement of the units in the stack. For example, any switch in a stack can be assigned module ID number 1 and so be the master switch. However, if you are assigning static numbers, the units will be easier to identify if they are numbered in either ascending or descending order in the equipment rack.
- ❑ The module ID numbers of the switches in a stack must be all static or dynamic. A stack will not function if some of the numbers are static and others are dynamic.
- ❑ A switch should be assigned a module ID number while it is operating as a stand-alone device, before it is added to a stack. If you need to change a switch's module ID number after the unit is added to a stack, disconnect the stacking cables from the device's AT-StackXG Stacking Module.
- ❑ A change with the SET STACK command to a switch's module ID number takes affect the next time the device is reset or power cycled.
- ❑ You do not have to perform the SAVE CONFIGURATION command after changing a device's module ID number. The new module ID number is automatically saved in a hidden file in the unit's file system after you enter the SET STACK command.

## Port Numbers in Commands

---

Some of the commands in the AT-S63 Management Software are used to configure or display the settings of the individual ports on the switches in the stack. The ports are designated with the PORT parameter. Because a stack has more than one switch, entering just a port number will obviously not be enough. Instead, a port number must be preceded by the module ID number of the switch in the stack with the port. Here is the format of the parameter:

*port=module ID.port number*

To view the module ID numbers of the switches in a stack, refer to “SHOW STACK” on page 72.

This example specifies port 22 on the switch assigned module ID 1:

*port=1.22*

Most of the commands that have the PORT parameter let you specify more than one port at a time. To identify individual ports, separate them with a comma. This example specifies ports 1.12, 3.1 and 4.5:

*port=1.12,3.1,4.5*

You can also enter ranges:

*port=4.12-4.16*

Notice that the module ID number is included with the ending port number of a range.

A range in the SHOW, ENABLE, and PURGE commands can span more than one switch:

*port=2.14-3.12*

However, a range in a SET command cannot span two switches. Here is an example of an invalid range for a SET command:

*port=1.1-2.24*

To correct this, you create a separate range for each switch:

*port=1.1-1.24,2.1-2.24*

Individual ports and ranges can be combined in the same command:

*port=1.12,3.1,4.5,4.12-4.16*

The following is an example of the PORT parameter in the CREATE SWITCH TRUNK command, which is used to create static port trunks. The example creates a static port trunks of ports 3 to 5 on module 2 and ports 7 and 8 on module 4:

```
create switch trunk=load22 port=2.3-2.5,4.7-4.8
```

## MAC Address Tables

---

When a switch in a stack learns a new source MAC address of a node connected to one of its port, it stores the address in its MAC address table and then shares the address with the other switches, which store the address in their tables. This sharing of addresses by the switches in a stack means that all the MAC address tables have the same entries.

The SHOW SWITCH FDB command is used to display the contents of the MAC address table of a switch. You will notice when you use the command that it does not permit you to specify a particular switch in a stack. Rather, it displays only the MAC address table in the master switch. However, since all of the tables in a stack are the same, viewing the master switch's table is equivalent to viewing the MAC address tables in the other switches, too.

## File Systems

---

The master switch has the only active file system in a stack. The file systems on the member switches are not accessible.

## Compact Flash Memory Card Slots

---

The master switch has the only active compact flash memory card slot in a stack. The slots in the member switches are inactive.

## Stack IP Address

---

A stack does not need an IP address to forward network packets through the ports of the switches. However, it does need an address if it will be performing any of the following management functions:

- ❑ Remote Telnet or web browser management
- ❑ Sending event messages to a syslog server
- ❑ Sending or receiving TCP/IP pings
- ❑ Uploading or downloading files to the master switch's file system from a TFTP server

To assign an IP address to the stack you have to create an IPv4 routing interface. The stack uses the routing interface's IP address as its address when performing the functions listed above. For further information on routing interfaces, refer to the *AT-S63 Management Software Features Guide*.

Here are the general steps to assigning an IP address to the stack:

1. Create a virtual LAN (VLAN) on the stack. The VLAN must include the port(s) from where the stack will communicate with the remote servers or the Telnet or web browser clients. You can skip this step if you will be using the Default\_VLAN for the remote management sessions. The commands for creating VLANs are in Chapter 21, "Port-based and Tagged VLAN Commands" on page 373.
2. Add an IPv4 routing interface to the VLAN. The command for creating a new IPv4 routing interface is "ADD IP INTERFACE" on page 392. If the IP addresses of the routing interface and the remote servers or Telnet clients are part of different subnets, the subnets must be connected with Layer 3 routing devices.
3. To manage the stack from a remote Telnet client, designate the routing interface as the stack's local interface with "SET IP LOCAL INTERFACE" on page 405. This instructs the management software to monitor the subnet of the interface for the remote management packets from the Telnet client.

## Upgrading the AT-S63 Management Software

---

The AT-9400 Switch must have Version 3.0.0 or later of the AT-S63 Management Software to be a member of a stack.

To update the management software on an existing stack for versions after Version 3.0.0, you must disconnect the stacking cables and update the switches individually, either locally through the Terminal Port on the units or over the network using a TFTP server. You reconnect the stacking cables after the management software on all of the switches has been updated.

---

**Note**

The switches of a stack must use the same version of the management software.

---

## Powering On a Stack

---

The switches of a stack can be powered on in any order. The units initialize their management software, which takes about one minute to complete, and afterwards perform the discovery process. The length of the discovery process can vary from fifteen seconds to several minutes, depending on the size of the stack and the number of the commands in the active configuration file on the master switch.

You can monitor the progress of the stack during these tasks by connecting a terminal or a personal computer with a terminal emulation program to the Terminal Port on the master switch, assigned the static module ID number 1. (For a stack that is using dynamic module ID numbers, the master switch will be the unit with the lowest MAC address. The MAC addresses of the switches can be found on a label on the back panel.)

The commencement by the stack of the discovery process is signalled with the messages in Figure 4.

Stack discovery is in progress ...

PLEASE DO NOT ADD/DELETE UNITS TO/FROM THE STACK UNTIL THE  
CURRENT STACK SETUP AND THE STACK CONFIGURATION IS LOADED.

Figure 4. Commencement of the Discovery Process

---

**Note**

If you see an error message during the discovery process, go to “Troubleshooting the Discovery Process” on page 48.

---

After the completion of the discovery process, the master switch displays the number of switches in the stack and its own MAC address twice, once as the switch of the local management session and again as the master switch of the stack. Figure 5 is an example of the messages.

4 module(s) discovered

Local MAC address: 00:04:75:00:00:11

Master MAC address: 00:04:75:00:00:11

Figure 5. Conclusion of the Discovery Process

In the final stage the master switch configures the devices with the commands in the active configuration file in its file system. If this is the first time the stack is booted up, you will see the messages in Figure 6.

```
Configuring the Stack..... done!  
Reinitializing Software Modules ..... done!  
Configuration file "stack.cfg" not found!  
Loading default configuration ..... done!
```

Figure 6. Console Messages at the Completion of the Discovery Process

At this point, the stack is operational and ready to forward network traffic on the ports. To log in and manage the stack, press Return to display the login prompt.

An alternative method for monitoring the initialization process is by observing the Stack MSTR LED on the front panel of the master switch. The LED becomes steady green when the stack is ready for network operations. (Do not confuse the Stack MSTR LED with the Status MASTER LED. The latter is used with enhanced stacking, a feature not supported on a stack.)

## Troubleshooting the Discovery Process

---

The easiest way to troubleshoot a stack that is unable to complete the discovery process is by watching for error messages on the Terminal Port of the master switch. Here are the steps:

1. Connect a terminal or a personal computer with a terminal emulation program to the Terminal Port on the master switch, as explained in “Starting a Local Management Session” on page 52.
2. Power on all the switches in the stack. If the switches are already powered on, power off the master switch, wait a few seconds and then power it back on again. Alternatively, disconnect and then reconnect a stacking cable from a stacking module.

Possible error messages are:

`More than maximum allowed number of switches.`

The stack has too many switches. Remove one or more of the devices after reviewing “Maximum Number of Switches in a Stack” on page 30.

`Mixed module ID mode is not supported. Failed to form a stack`

`Failed to elect a stack Master in the static mode.  
Stack setup has failed.`

These message could indicate that the switches of the stack have both dynamic and static module ID numbers. A stack can have all static or all dynamic numbers, but not a combination of the two. Resolving the problem will require disconnecting the stacking cables from the switches and resetting the numbers with the SET STACK command. For instructions, refer to “SET STACK” on page 70.

The second message could also indicate that there are no switches numbered 1 or 2 in the stack, a problem that can only occur with static module ID numbers. A stack must have at least one switch assigned module ID number 1 or 2.

`Module ID conflict. Failed to form a stack`

This message indicates that two or more switches have the same static module ID number. To resolve the issue, use the SET STACK command. For instructions, refer to “SET STACK” on page 70.



If the master switch successfully completes the discovery process but the SHOW STACK command displays only one switch or a subset of the switches of the stack, try the following:

- ❑ Verify that all the switches are powered on.
- ❑ Verify that all the switches are using the same version of the AT-S63 Management Software. For instructions, refer to *AT-9400 Stack Installation Guide*.
- ❑ Verify that the stacking cables are securely connected to the ports on the AT-StackXG Stacking Modules and that the cables crossover to different numbered ports on the modules. For information, refer to the “Stack Topology” on page 32.



## Chapter 2

# Starting a Command Line Management Session

---

This chapter contains the following sections:

- ❑ “Starting a Local Management Session” on page 52
- ❑ “Remote Telnet Management” on page 54
- ❑ “Quitting a Management Session” on page 56
- ❑ “Command Line Interface Features” on page 57
- ❑ “Command Formatting” on page 58
- ❑ “Redundant Twisted Pair Ports” on page 59

## Starting a Local Management Session

---

### Note

A stack does not need an IP address for local management.

---

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

1. Identify the master switch of the stack. (Local management sessions must be conducted through the master switch.) If you followed the instructions in the *AT-9400 Stack Installation Guide*, the switches should have labels with their module ID numbers. The switch labelled module ID 1 is the master switch of the stack.

If the switches are not labeled, examine the Stack MSTR LED on the units. The LED will be steady green on the master switch. (Do not confuse the Stack MSTR LED and the Status Master LED. The latter relates to enhanced stacking, a feature not supported in a stack.)

2. Connect one end of the RJ-45 to RS-232 management cable included with the switch to the Terminal Port on the front panel of the master switch, as shown in Figure 7.

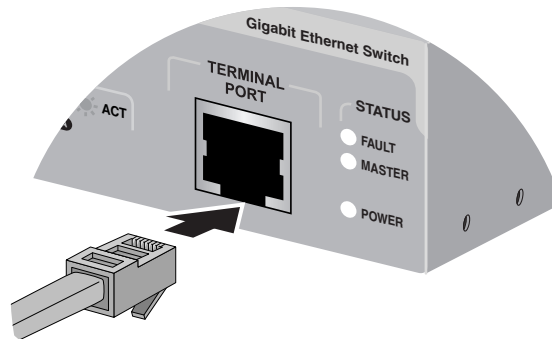


Figure 7. Connecting the Management Cable to the RJ-45 Serial Terminal Port

3. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
4. Configure the terminal or terminal emulation program as follows:
  - ☐ Baud rate: 9600 bps (The baud rate of the Terminal Port is adjustable from 9600 to 115200 bps. The default is 9600 bps. To change the baud rate, refer to “SET ASYN” on page 84.)
  - ☐ Data bits: 8
  - ☐ Parity: None

- ☐ Stop bits: 1
- ☐ Flow control: None

**Note**

The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

5. Press Enter.

You are prompted for a user name and password.

6. Enter a user name and password. The stack comes with two standard user accounts: manager and operator. The manager account lets you configure the stack's settings while the operator account only lets you view them.

To log in as the manager, enter "**manager**" as the user name. The default password for manager access is "friend." To log in as an operator, enter "**operator**" as the user name. The default password for operator access is "operator." User names and passwords are case sensitive.

**Note**

A stack can support one manager session and eight operator sessions simultaneously.

7. The local management session starts and the command line interface (CLI) prompt is displayed, as shown in Figure 8. If the stack has a name, the name appears below the master switch's model name.

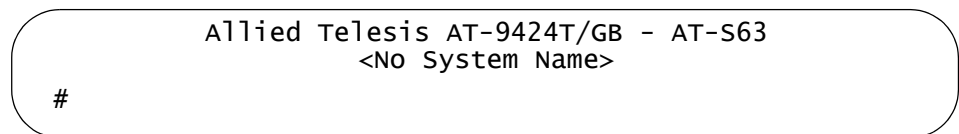


Figure 8. CLI Prompt

8. You can now begin to manage the stack with the commands described in this guide.

## Remote Telnet Management

---

### Planning for Remote Management

Before you can remotely manage a stack with a Telnet client from a network workstation, you must assign an IP address to the stack, as outlined in the steps here:

1. Create a virtual LAN (VLAN) on the stack. The VLAN must include the port(s) through which the stack and the remote Telnet clients will conduct the management sessions. You can skip this step if you will be using the Default\_VLAN for the remote management sessions. The commands for creating VLANs are in Chapter 21, “Port-based and Tagged VLAN Commands” on page 373.
2. Add an IPv4 routing interface to the VLAN. The IP addresses of the routing interface and the remote Telnet client must be members of the same subnet. Alternatively, if the routing interface and the remote Telnet client are on different networks, they must be connected with Layer 3 routing devices. The command for creating a new IPv4 routing interface is “ADD IP INTERFACE” on page 392.
3. Designate the routing interface as the stack’s local interface with “SET IP LOCAL INTERFACE” on page 405. This instructs the management software to monitor the subnet of the interface for the remote management packets from the Telnet client.

### Starting a Remote Telnet Management Session

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

1. In the Telnet client on the remote management workstation, enter the IP address of the local interface on the stack.

Prompts are displayed for a user name and password.

2. Enter a user name and password. The management software comes with two default user accounts: manager and operator. The manager account lets you configure the switch’s settings while the operator account only lets you view them.

To log in as the manager, enter “manager” as the user name. The default password for manager access is “friend.” To log in as an operator to just view the settings, enter “operator” as the user name. The default password for operator access is “operator.” User names and passwords are case sensitive. To change a password, refer to “SET PASSWORD MANAGER” on page 86 or “SET PASSWORD OPERATOR” on page 87.

---

**Note**

A stack can support one manager session and eight operator sessions simultaneously.

---

After you have logged on, the command line interface (CLI) prompt is displayed, as shown in Figure 8 on page 53. If the stack has a name, the name is displayed below the master switch's model name.

3. You can now begin to manage the stack with the commands detailed in this guide.

## Quitting a Management Session

---

To quit a local management session, type **EXIT**. You should always exit from a management session at the completion of a session. This can prevent an unauthorized individual from making changes to a stack's configuration in the event you leave your management station unattended.

The management software has a console timer that automatically ends a management session if there is no management activity for the duration of the timer. The default is ten minutes. To change the console timer, refer to "SET SWITCH CONSOLETIMER" on page 88.

---

**Note**

Failure to properly exit from a management session may block future management sessions until the console timer times out.

---



## Command Line Interface Features

---

The following features are supported in the command line interface:

- ❑ Command history - Use the up and down arrow keys.
- ❑ Context-specific help - Press the question mark key at any time to see a list of legal next parameters.
- ❑ Keyword abbreviations - Any keyword can be recognized by typing an unambiguous prefix, for example, “sh” for “show”.
- ❑ Tab key - Pressing the Tab key fills in the rest of the keyword. For example, typing “di” and pressing the Tab key enters “disable.”

## Command Formatting

---

The following formatting conventions are used in this manual:

- ❑ `screen text font` - This font illustrates the format of a command and command examples.
- ❑ *screen text font* - Italicized screen text indicates a variable for you to enter.
- ❑ `[ ]` - Brackets indicate optional parameters.
- ❑ `|` - Vertical line separates parameter options for you to choose from.

## Redundant Twisted Pair Ports

---

The twisted pair ports 21R to 24R on the AT-9424Ts and AT-9424Ts/XP Switches are paired with four SFP slots. Follow these guidelines when using these ports and slots:

- ❑ Only one port in a pair — either the twisted pair port or the corresponding SFP module — can be active at a time.
- ❑ The twisted pair port is the active port when its SFP slot is empty, or when an SFP module is installed but has not established a link to an end node.
- ❑ The twisted pair port automatically changes to the redundant status mode when an SFP module establishes a link with an end node.
- ❑ A twisted pair port automatically transitions back to the active status when the link is lost on the SFP module.
- ❑ A twisted pair port and an SFP module share the same configuration settings, including port settings, VLAN assignments, access control lists, and spanning tree.
- ❑ An exception to the shared settings is port speed. If you disable Auto-Negotiation on a twisted pair port and set the speed and duplex mode manually, the speed reverts to Auto-Negotiation when a GBIC or SFP module establishes a link with an end node.
- ❑ Omit the letter “R” when specifying a redundant twisted pair port in a command line command. For instance, the following command assigns the description “Sales server” to port 23R on the AT-9424T/GB Switch. The switch has the module ID 2:

```
set switch port=2.23 description="sales server"
```

---

**Note**

These guidelines do not apply to the XFP slots on the AT-9424Ts/XP and AT-9448Ts/XP switches.

---



## Chapter 3

# Basic Command Line Commands

---

This chapter contains the following commands:

- ❑ “CLEAR SCREEN” on page 62
- ❑ “EXIT” on page 63
- ❑ “HELP” on page 64
- ❑ “LOGOFF, LOGOUT and QUIT” on page 65
- ❑ “SAVE CONFIGURATION” on page 66
- ❑ “SET PROMPT” on page 67
- ❑ “SHOW USER” on page 68

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

## CLEAR SCREEN

---

### Syntax

```
clear screen
```

### Parameters

None.

### Description

This command clears the screen.

### Example

```
clear screen
```

# EXIT

---

## Syntax

`exit`

## Parameters

None.

## Description

This command ends a management session.

## Example

`exit`

## Equivalent Commands

`logoff`

`logout`

`quit`

For information, see “LOGOFF, LOGOUT and QUIT” on page 65.

## HELP

---

### Syntax

help

### Parameters

None.

### Description

This command lists the CLI keywords. Each keyword has a brief description.

### Example

help



## LOGOFF, LOGOUT and QUIT

---

### Syntax

logoff

logout

quit

### Parameters

None.

### Description

These three commands end a management session.

### Example

The following command ends a management session:

logoff

## SAVE CONFIGURATION

---

### Syntax

`save configuration`

### Parameters

None.

### Description

This command saves your changes to the parameter settings of the stack in the master switch's active boot configuration file for permanent storage.

Changes to the operating parameters of a stack, such as the creation of a new virtual LAN or static port trunk, are initially stored in temporary memory, where they will be lost the next time the stack is reset or power cycle.

To permanently save your changes, you must use this command. It saves your changes as a series of commands in the active boot configuration file on the master switch. The master switch uses the file whenever you reset or power cycle the stack to recreate the settings.

To view the name of the active boot configuration file, see "SHOW CONFIG" on page 212. To view the contents of a configuration file, see "SHOW FILE" on page 213.

### Example

`save configuration`

# SET PROMPT

---

## Syntax

```
set prompt="prompt"
```

## Parameter

prompt	Specifies the command line prompt. The prompt can be from one to 12 alphanumeric characters. Spaces and special characters are allowed. The prompt must be enclosed in quotes.
--------	--

## Description

This command changes the command line prompt. Assigning each stack a different command prompt can make them easier to identify.

---

### Note

If you define the system name but not the system prompt, the first sixteen characters of the system name are used as the prompt. See "SET SYSTEM" on page 89.

---

## Example

This command changes the command prompt to "Sales Stack":

```
set prompt="Sales Stack"
```

## Equivalent Command

```
set asyn prompt="prompt"
```

For information, see "SET ASYN" on page 84.

## SHOW USER

---

### Syntax

`show user`

### Parameter

None.

### Description

Displays the user account used to log on to manage the stack.

### Example

`show user`

## Chapter 4

# Stacking Commands

---

This chapter contains the following commands:

- ❑ “SET STACK” on page 70
- ❑ “SHOW STACK” on page 72

## SET STACK

---

### Syntax

```
set stack moduleid=value newmoduleid=auto|static|value
priority=value
```

### Parameters

mymoduleid	Specifies the switch's current ID number. To view this number, refer to "SHOW STACK" on page 72.						
newmoduleid	Specifies a new stack ID number for the switch. Options are: <table data-bbox="714 724 1438 1165"> <tr> <td>auto</td><td>Sets the switch's ID dynamically, based on the device's MAC address or stack priority number.</td></tr> <tr> <td>static</td><td>Converts the switch's current dynamic module ID into a static ID.</td></tr> <tr> <td><i>value</i></td><td>Assigns a static module ID to the switch. The range is 1 to 5 for a stack of 48-port AT-9448Ts/XP Switches and 1 to 8 for a stack of 24-port AT-9424Ts or AT-9424Ts/XP Switches or a stack of both 24-port and 48-port switches.</td></tr> </table>	auto	Sets the switch's ID dynamically, based on the device's MAC address or stack priority number.	static	Converts the switch's current dynamic module ID into a static ID.	<i>value</i>	Assigns a static module ID to the switch. The range is 1 to 5 for a stack of 48-port AT-9448Ts/XP Switches and 1 to 8 for a stack of 24-port AT-9424Ts or AT-9424Ts/XP Switches or a stack of both 24-port and 48-port switches.
auto	Sets the switch's ID dynamically, based on the device's MAC address or stack priority number.						
static	Converts the switch's current dynamic module ID into a static ID.						
<i>value</i>	Assigns a static module ID to the switch. The range is 1 to 5 for a stack of 48-port AT-9448Ts/XP Switches and 1 to 8 for a stack of 24-port AT-9424Ts or AT-9424Ts/XP Switches or a stack of both 24-port and 48-port switches.						
priority	Specifies a stack priority value for the switch, used with dynamic stack ID numbers. The range is 1 to 16. The lower the value the higher the priority. The default value is 16.						

### Description

This command assigns an ID number to a switch. ID numbers can be either dynamic or static. Dynamic ID numbers are based on the devices' MAC addresses or their priority values, and are assigned during the discovery process of the stack. Static ID numbers are numbers manually assigned to the devices. For further information, refer to "Module ID Numbers" on page 38.

Note the following before performing this command:

- ❑ This command should be performed before a switch is connected to a stack. The results may be unpredictable if you perform this command while a switch is part of a stack.

- ❑ You must reset or power cycle the unit after performing this command to activate a switch's new ID number.
- ❑ You do not have to issue the SAVE CONFIGURATION command with this command. A device's new ID number is automatically stored in a hidden system file in the unit's file system.

---

**Note**

All of the switches of a stack must have the same type of stack ID number of static or dynamic. A stack will not function if one or more of the module ID numbers are dynamic and others are static.

---

For further information on module ID numbers, refer to "Module ID Numbers" on page 38.

### Examples

This command assigns the static ID 1 to the switch. The command assumes that the switch's current module ID number of 1 was set dynamically:

```
set stack moduleid=1 newmoduleid=1
```

This command assigns to the switch the static ID 4. The switch's current module ID number is 1:

```
set stack moduleid=1 newmoduleid=4
```

This command assigns the static ID 3 to the switch. The switch's current module ID number is 2:

```
set stack moduleid=2 newmoduleid=3
```

This command sets the switch's module ID number dynamically:

```
set stack moduleid=1 newmoduleid=auto
```

This command sets the switch's module ID number dynamically and assigns it a priority of 5:

```
set stack moduleid=1 newmoduleid=auto priority=5
```

## SHOW STACK

---

### Syntax

```
show stack
```

### Parameters

None.

### Description

This command displays the module ID number of a switch. The command displays different information depending on whether the switch is a stand-alone unit or the master switch of a functioning stack. Figure 9 is an example of the information from a stand-alone switch. This information is useful when setting or changing a switch's ID number, which should only be performed when the device is not connected to a stack.

Local MAC Addr	:00:30:84:00:00:03
Standalone Mode ID	:1
Stack Mode	:AUTO
Stack ID	:1
Stack Priority	:16

Figure 9. SHOW STACK Command of a Stand-alone Switch

The fields are defined here:

- ❑ Local MAC Addr: The MAC address of the switch.
- ❑ Standalone Mode ID: The ID number of the switch when the device is not a part of a stack. This parameter can be ignored.
- ❑ Stack Mode: The method by which the ID number was assigned. Auto means the number was assigned dynamically by the management software when the switch was powered on. Static means the number was assigned with the SET STACK command.
- ❑ Stack ID: The switch's current module ID number.
- ❑ Stack Priority: The switch's current stack priority value, used to control dynamic ID numbers. For an explanation, refer to the "Module ID Numbers" on page 38.

---

### Note

If you changed a switch's ID number with the SET STACK command but do not see the change reflected in this command, it could be because you did not reset the switch. A change to a switch's ID number does not take effect until the unit is reset.

---



Figure 10 is an example of the command when it is performed on the master switch of a functioning stack. The switches in the stack and their module ID numbers are displayed in a table.

Local MAC Addr	:	00:30:84:00:00:02
Master MAC Addr	:	00:30:84:00:00:02
Backup Master MAC Addr	:	00:30:84:00:00:54
Topology	:	Duplex_Chain
My ModuleID	:	1
ModuleID Assignment Mode	:	STATIC
Current State	:	Master
Module Count	:	4

Module	Stack State	Model Name	Priority	Mac Address
1	Master	AT-9424Ts/XP	16	00:30:84:00:00:02
2	Member	AT-9424Ts/XP	16	00:30:84:00:00:52
3	Member	AT-9424Ts/XP	16	00:30:84:00:00:22
4	Member	AT-9424Ts/XP	16	00:30:84:00:00:82

Figure 10. SHOW STACK Command of a Stack

The fields and columns are defined here:

- ❑ Local MAC Addr - The MAC address of the master switch of the stack. The local and master MAC addresses will always be the same.
- ❑ Master MAC Addr - The MAC address of the master switch of the stack.
- ❑ Backup Master MAC Addr - The MAC address of the backup master switch of the stack. A stack will have a backup master if the switches have static ID numbers. A stack with dynamic module ID numbers will not have a backup master.
- ❑ Topology - The cabling topology of the stack. Possible values are Duplex\_Chain and Duplex\_Ring.
- ❑ My ModuleID - The module ID number of the master switch of the stack. The master switch always has the ID number 1.
- ❑ ModuleID Assignment Mode - The assignment method of the ID numbers of the switches. If AUTOMATIC, the switches were assigned dynamic ID numbers. If STATIC, the switches were assigned static ID numbers.
- ❑ Current State - The current state of the master switch. This will always be Master.
- ❑ Module Count - The number of switches in the stack.
- ❑ Module - The module ID number of a switch.
- ❑ Stack State - The state of a switch. A switch will be either Master or Member.
- ❑ Model Name - The Allied Telesis model name of a switch.

- ❑ Priority - The priority number of a switch. The range is 1 to 16. The lower the number, the higher the priority. To set this value, refer to “SET STACK” on page 70. This value only applies when the ID numbers are set automatically.
- ❑ Mac Address - The MAC address of a switch.

For information on module ID numbers, refer to “Module ID Numbers” on page 38.

### **Example**

```
show stack
```

# Basic Stack Commands

---

This chapter contains the following commands:

- ❑ “DISABLE TELNET” on page 76
- ❑ “ENABLE TELNET” on page 77
- ❑ “PING” on page 78
- ❑ “RESET SWITCH” on page 79
- ❑ “RESET SYSTEM” on page 80
- ❑ “RESTART REBOOT” on page 81
- ❑ “RESTART SWITCH” on page 82
- ❑ “SET ASYN” on page 84
- ❑ “SET DATE” on page 85
- ❑ “SET PASSWORD MANAGER” on page 86
- ❑ “SET PASSWORD OPERATOR” on page 87
- ❑ “SET SWITCH CONSOLETIMER” on page 88
- ❑ “SET SYSTEM” on page 89
- ❑ “SET TELNET INSERTNULL” on page 90
- ❑ “SET TIME” on page 91
- ❑ “SET USER PASSWORD” on page 92
- ❑ “SHOW ASYN” on page 93
- ❑ “SHOW CONFIG DYNAMIC” on page 94
- ❑ “SHOW CONFIG INFO” on page 96
- ❑ “SHOW SWITCH” on page 97
- ❑ “SHOW SYSTEM” on page 100
- ❑ “SHOW TIME” on page 102

---

### Note

Remember to save your changes with the SAVE CONFIGURATION command.

---

## DISABLE TELNET

---

### Syntax

```
disable telnet
```

### Parameters

None.

### Description

This command disables the Telnet server on the master switch. You might disable the server to prevent anyone from managing the stack with a Telnet client. The default setting for the Telnet server is enabled.

### Example

The following command deactivates the Telnet server:

```
disable telnet
```

## ENABLE TELNET

---

### Syntax

```
enable telnet
```

### Parameters

None.

### Description

This command activates the Telnet server on the master switch. When the server is activated, you can remotely manage the stack using the Telnet application protocol. To disable the server, refer to “DISABLE TELNET” on page 76. The default setting for the Telnet server is enabled.

### Example

The following command activates the Telnet server:

```
enable telnet
```

# PING

---

## Syntax

`ping ipaddress`

## Parameter

`ipaddress` Specifies the IP address of an end node to be pinged.

## Description

This command instructs the stack to ping an end node. You can use this command to determine whether an active link exists between the stack and another network device. Follow these guidelines when using this command:

- ❑ The stack must have a routing interface. It uses the IP address of the interface as its source address when pinging a device. The command for adding a routing interface is “ADD IP INTERFACE” on page 392.
- ❑ The stack can only ping devices that are accessible from the local subnet of the routing interface.

## Example

The following command pings an end node with the IP address of 149.245.22.22

```
ping 149.245.22.22
```

The results of the ping are displayed on the screen.

## RESET SWITCH

---

### Syntax

```
reset switch [module=id]
```

### Parameters

<code>id</code>	Specifies the ID number of a switch in the stack. You can specify only one switch at a time. To view the ID numbers of the switches, refer to “SHOW STACK” on page 72.
-----------------	--

### Description

This command does the following:

- ❑ Performs a soft reset on all of the ports on a switch or in a stack. The reset takes less than a second to complete. The ports retain their current operating parameter settings. To perform this function on a per-port basis, refer to “RESET SWITCH PORT” on page 129.
- ❑ Resets the statistics counters for all ports to zero. To perform this function on a per-port basis, refer to “RESET SWITCH PORT COUNTER” on page 146.
- ❑ Deletes all dynamic MAC addresses from the MAC address table. To perform this function on a per-port basis, refer to “RESET SWITCH FDB” on page 156.

### Examples

This command resets all of the ports in the stack:

```
reset switch
```

This command resets all the ports on chassis 2:

```
reset switch module=2
```

## RESET SYSTEM

---

### Syntax

```
reset system [name] [contact] [location]
```

### Parameters

name           Deletes the switch's name.

contact       Deletes the switch's contact.

location      Deletes the switch's location.

### Description

This command delete's the stack's name, the name of the network administrator responsible for managing it, and its location. To set these parameters, refer to "SET SYSTEM" on page 89. To view the current settings, refer to "SHOW SYSTEM" on page 100.

### Examples

This command deletes all three parameter settings:

```
reset system
```

This command deletes just the name:

```
reset system name
```



# RESTART REBOOT

---

## Syntax

restart reboot

## Parameters

None.

## Description

This command resets the entire stack. The switches run their internal diagnostics, load the AT-S63 Management Software, and perform the discovery process. The reset can take several minutes to complete. For further information, refer to “Discovery Process” on page 34.

---

### Note

The switches of a stack do not forward traffic during the reset process. Some network traffic may be lost.

---

---

### Note

Be sure to use the SAVE CONFIGURATION command to save your changes before resetting the stack. Any unsaved changes are lost.

---

Your local or remote management session with the stack ends when it is reset. You must reestablish the session to continue managing it.

## Example

The following resets the stack:

```
restart reboot
```

## RESTART SWITCH

---

### Syntax

```
restart switch config=none|filename.cfg
```

### Parameters

**config** Specifies the configuration file. The file must already exist on the master switch. The NONE option returns all of the parameter settings in the stack to the default values.

### Description

This command can load a different configuration file on the stack or return the stack's parameter settings to their default values. This command can also be used to reset a stack.

If you specify a configuration file, the master switch automatically resets itself and configures its parameters according to the settings in the configuration file specified in the command. However, the assignment of the active boot configuration file does not change. Resetting or power cycling the stack again causes it to revert to its previous configuration. To change the assignment of the active boot configuration file, refer to "SET CONFIG" on page 209.

Specifying the NONE option returns the stack's operating parameters to the default setting. Note the following before using this option:

- ❑ Returning all parameter settings to their default values deletes all routing interfaces as well as all port-based and tagged VLANs on the switch.
- ❑ This option does not delete files from the file system on the master switch. To delete files, refer to "DELETE FILE" on page 204.
- ❑ Returning the parameter settings of a stack to their default values does not change the settings in the active boot configuration file. To return the active configuration file to the default settings, you must use the SAVE CONFIGURATION command after the stack reboots and you have reestablished your management session. Otherwise, the stack reverts to the previous configuration the next time you reset it.

---

### Note

The stack does not forward network traffic during the reset process. Some network traffic may be lost.

---

---

**Note**

For a list of default values, refer to Appendix A, “AT-S63 Default Settings” in the *AT-S63 Management Software Features Guide*.

---

Your local or remote management session ends when you reset the stack. You must reestablish the session to continue managing it.

**Examples**

The following command configures the stack using the configuration file named `stack12.cfg`:

```
restart switch config=stack12.cfg
```

The following command resets all of the parameter settings in the stack to their default values:

```
restart switch config=none
```

The following command resets the stack:

```
restart switch
```

**Equivalent Command**

```
restart reboot
```

For information, see “RESTART REBOOT” on page 81.

## SET ASYN

---

### Syntax

```
set asyn [speed=1200|2400|4800|9600|19200|38400|
57600|115200] [prompt="prompt"]
```

### Parameters

speed	Sets the speed (baud rate) of the serial terminal port on the master switch. The default is 9600 bps.
prompt	Specifies the command line prompt. The prompt can be from one to 12 alphanumeric characters. Spaces and special characters are allowed. The prompt must be enclosed in double quotes. This parameter performs the same function as "SET PROMPT" on page 67.

### Description

This command sets the baud rate of the serial terminal port on the master switch of the stack. The port is used for local management. You can also use this command to set the command line prompt.

---

#### Note

A change to the baud rate of the port ends your management session if you are managing the stack locally. To reestablish a local management session you must change the speed of the terminal or the terminal emulator program to match the new speed of the serial terminal port on the master switch.

---

### Example

The following command sets the baud rate to 115200 bps:

```
set asyn speed=115200
```

### Equivalent Command

```
set prompt="prompt"
```

For information, see "SET PROMPT" on page 67.

## SET DATE

---

### Syntax

```
set date=dd-mm-yyyy
```

### Parameter

date	Specifies the date for the stack in day-month-year format.
------	--

### Description

This command manually sets the date on the stack. You can use this command to set the stack's date if you are not using an SNTP server. The date and time are maintained even when a switch is powered off because the unit has an onboard battery.

### Example

The following command sets the stack's date to December 11, 2004:

```
set date=11-12-2004
```

## SET PASSWORD MANAGER

---

### Syntax

```
set password manager
```

### Parameters

None.

### Description

This command sets the manager's password. The manager account allows you to view and change all of the stack parameters. The default password is "friend." The password can be from 0 to 16 alphanumeric characters. Allied Telesis recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

### Example

The following command changes the manager's password:

```
set password manager
```

Follow the prompts to enter the new password.

### Equivalent Command

```
set user manager password=password
```

For information, see "SET USER PASSWORD" on page 92.

## SET PASSWORD OPERATOR

---

### Syntax

set password operator

### Parameters

None.

### Description

This command sets the operator's password. Logging in as operator allows you to only view the parameter settings in a stack. The default password is "operator." The password can be from 0 to 16 alphanumeric characters. Allied Telesis recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

### Example

The following command changes the operator's password:

```
set password operator
```

Follow the prompts to enter the new password.

### Equivalent Command

```
set user operator password=password
```

For information, see "SET USER PASSWORD" on page 92.

## SET SWITCH CONSOLETIMER

---

### Syntax

```
set switch consoletimer=value
```

### Parameter

consoletimer	Specifies the console timer in minutes. The range is 1 to 60 minutes. The default is 10 minutes.
--------------	--

### Description

This command sets the console timer, which the management software uses to end inactive management sessions. The AT-S63 Management Software automatically ends a management session if it does not detect any activity from a local or remote management station for the length of time specified by the console timer. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a stack. To view the current console timer setting, refer to “SHOW SWITCH” on page 97.

### Example

The following command sets the console timer to 25 minutes:

```
set switch consoletimer=25
```



## SET SYSTEM

---

### Syntax

```
set system [name="name"] [contact="contact"]  
[location="location"]
```

### Parameters

name	Specifies the name of the stack. The name can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes (" "). Spaces are allowed.
contact	Specifies the name of the network administrator responsible for managing the stack. The contact can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes. Spaces are allowed.
location	Specifies the location of the stack. The location can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes. Spaces are allowed.

### Description

This command sets a stack's name, the name of the network administrator responsible for managing it, and the location of the devices. If a parameter already has a value, the new value replaces the existing value. To view the current values for these parameters, refer to "SHOW SYSTEM" on page 100. To delete a value without assigning a new value, refer to "RESET SYSTEM" on page 80.

---

#### Note

If you define the system name before you set up a system prompt, the master switch uses the first 16 characters of the system name as the prompt. See "SET PROMPT" on page 67.

---

### Examples

The following command sets a stack's information:

```
set system name="Sales" contact="Jane Smith" location="Bldg  
3, rm 212"
```

The following command sets just the stack's name:

```
set system name="PR Office"
```

## SET TELNET INSERTNULL

---

### Syntax

```
set telnet insertnull=on|off
```

### Parameters

**insertnull** Controls whether the Telnet server inserts a NULL character after each CR sent to the remote client. Options are:

- on** Sends a NULL character after each CR sent to the remote client.
- off** Specifies that no NULL character is sent to the remote client. This is the default setting.

### Description

You can use this command to toggle the Telnet server on the master switch to add a NULL character after each CR for those Telnet clients that require the character in order to display the information correctly. The default setting on the master switch is to not send the NULL character after a CR. To view the current setting, see “SHOW SWITCH” on page 97.

### Example

This command configures the master switch to send a NULL character after each CR during a Telnet management session:

```
set telnet insertnull=on
```

## SET TIME

---

### Syntax

```
set time=hh:mm:ss
```

### Parameter

time	Specifies the hour, minute, and second for the stack's time in 24-hour format.
------	--

### Description

This command manually sets the time on the stack. You can use this command to set the stack's time if you are not using an SNTP server. The date and time are maintained even when the switch is powered off because the unit has an onboard battery.

### Example

The following command sets the stack's time to 4:34 pm and 52 seconds:

```
set time=16:34:52
```

## SET USER PASSWORD

---

### Syntax

```
set user manager|operator password=password
```

### Parameter

**password** Specifies the password.

### Description

This command sets the manager or operator's password. The default manager password is "friend." The default operator password is "operator." The password can be from 0 to 16 alphanumeric characters. Allied Telesis recommends against using special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

### Example

The following command sets the operator's password to "newby":

```
set user operator password=newby
```

### Equivalent Commands

```
set password manager
```

For information, see "SET PASSWORD MANAGER" on page 86

```
set password operator
```

For information, see "SET PASSWORD OPERATOR" on page 87

## SHOW ASYN

---

### Syntax

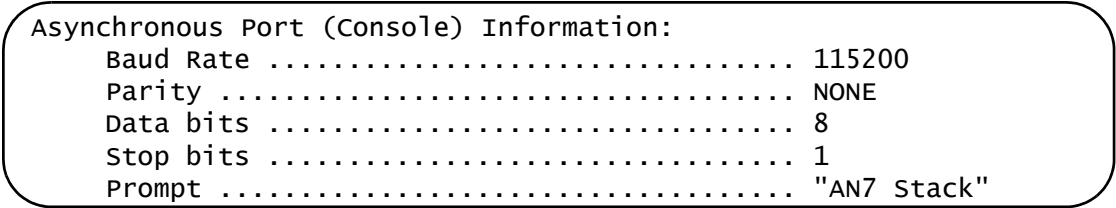
show asyn

### Parameters

None.

### Description

This command displays the settings for the serial terminal port on the master switch. The port is used for local management of the stack. An example of the display is shown in Figure 11.



```
Asynchronous Port (Console) Information:
Baud Rate ..... 115200
Parity ..... NONE
Data bits ..... 8
Stop bits ..... 1
Prompt ..... "AN7 Stack"
```

Figure 11. SHOW ASYN Command

To configure the serial port's baud rate, refer to "SET ASYN" on page 84. To configure the command line prompt, refer to "SET PROMPT" on page 67. You cannot adjust the parity, data bits, or stop bit of the serial terminal port.

### Example

The following command displays the serial terminal port settings:

```
show asyn
```

# SHOW CONFIG DYNAMIC

## Syntax

show config dynamic[=*module*]

## Parameters

**module**     Displays the settings of a specific module in the management software. You can specify only one module at a time. For a list of modules, refer to Table 2.

## Description

This command displays the parameter settings of the stack that have been changed from their default values, including those not yet saved to the active boot configuration file. The parameters are displayed in their command line command equivalents. You can view all of the settings or limit the display to just those of a particular management software module. An example of the display is shown in Figure 12.

```
---Start of current configuration -----  
  
#  
# System Configuration  
#  
set system name="Production Stack"  
set system contact="Jane Smith"  
set system location="Bldg. 2, room 411"  
  
#  
# User Authentication Configuration  
#
```

Figure 12. SHOW CONFIG DYNAMIC Command

The MODULE variable limits the display to a particular management software module. You can specify only one module per command. The modules are listed in Table 2.

Table 2. Module Variable

Variable	Description
ARP	Static ARP entries
EVTLOG	Event log and syslog client
INTF	Routing interface

Table 2. Module Variable (Continued)

Variable	Description
MAC	Static MAC addresses
MACTIMER	MAC address table timeout value
MIRROR	Source ports of port mirror
MIRTO	Destination port of port mirror
PORT	Port configuration
PORTTRUNK	Static port trunks
ROUTE	Static routes
STP	Spanning Tree and Rapid Spanning Protocols
SWITCH	Master Switch console timer, console startup mode, serial port baud rate, Telnet server
SYSTEM	Administrator name, switch name, and stack location
VLAN	Port-based and tagged VLANs

### Examples

This command displays all of the non-default parameter settings in the stack:

```
show config dynamic
```

This command displays the non-default parameter settings for port-based and tagged VLANs:

```
show config dynamic=vlan
```

## SHOW CONFIG INFO

---

### Syntax

```
show config info
```

### Parameters

None.

### Description

This command displays all of the parameter settings on a stack, including those not yet saved to the active boot configuration file.

### Example

```
show config info
```



## SHOW SWITCH

---

### Syntax

```
show switch module=id
```

### Parameters

**id** Specifies the ID number of a switch in the stack. You can specify only one switch at a time. To view the module ID numbers, refer to “SHOW STACK” on page 72.

### Description

This command displays a variety of information and parameter settings about the switches in a stack. You can only view one switch at a time. Since these parameter settings are only active on the master switch, the command should only be used to view that unit. An example of the display is shown in Figure 13.

#### Switch Information:

```
Application Software Version ..... ATS63 v3.0.0
Application Software Build Date ..... May 14 2007 16:27:38
Bootloader Version ..... ATS63_LOADER v3.0.0
Bootloader Build Date ..... May 11 2007 16:25:19
MAC Address ..... 00:21:46:A7:B4:43
VLAN Mode ..... User Configured
Ingress Filtering ..... OFF
Active Spanning Tree version ..... RSTP
Mirroring State ..... Disabled
Enhanced Stacking mode ..... Master
Console Disconnect Timer Interval .... 10 minute(s)
Web Server Status ..... Enabled
Telnet Server status ..... Enabled
Telnet insert NULL ..... OFF
MAC address aging time ..... 300 second(s)
Console Startup Mode ..... CLI
Multicast Mode ..... Forward Across VLANs
```

Figure 13. SHOW SWITCH Command

This command displays the following information:

- ❑ Application software version and Application software build date - The version number and build date of the AT-S63 Management Software.
- ❑ Bootloader version and Bootloader build date - The version number and build date of the AT-S63 bootloader.

- ❑ MAC address - The MAC address of the switch. This value cannot be changed.
- ❑ VLAN mode - The stack's VLAN mode. The three possible VLAN modes are:
  - ❑ User configured (for creating your own port-based and tagged VLANs)
  - ❑ 802.1Q-compliant
  - ❑ Non-802.1Q-compliant

The default is user configured VLANs. Version 3.0.0 of the management software does not support 802.1Q-compliant or non-802.1Q-compliant in a stack.

- ❑ Ingress filtering - The status of ingress filtering on the switch. When ingress filtering is activated, tagged frames are filtered when they are received on a port. When ingress filtering is deactivated, which is the default, tagged frames are filtered before they are transmitted out a port. To set ingress filtering, refer to "SET SWITCH INFILTERING" on page 383.
- ❑ Active Spanning Tree version - The active spanning tree protocol in the stack.
- ❑ Mirroring state - The status of port mirroring. The display includes the destination port as well as the ingress and egress source ports if port mirroring is activated on the switch. To configure port mirroring, refer to "SET SWITCH MIRROR" on page 193 and "SET SWITCH PORT MIRROR" on page 194.
- ❑ Enhanced stacking mode - The enhanced stacking mode of the switch, which can be master, slave, or unavailable. This feature is not supported in a stack.
- ❑ Console disconnect timer interval - The current value of the console timer, used by the management software to end inactive management sessions. The AT-S63 software ends a local or remote management session if it does not detect any management activity for the length of time specified by the console timer. The default is 10 minutes. To set the console timer, refer to "SET SWITCH CONSOLETIMER" on page 88.
- ❑ Web server status - The status of the web server. The stack does not support management from a web browser.
- ❑ Telnet server status - The status of the Telnet server. When the Telnet server is disabled, you cannot remotely manage the switch using the Telnet application protocol. The default setting is enabled. To enable or disable the server, refer to "ENABLE TELNET" on page 77 and "DISABLE TELNET" on page 76.
- ❑ Telnet insert NULL - The status of the Telnet NULL parameter. When ON, the Telnet server on the switch adds a NULL character after each CR for those Telnet clients that require the character to display the

information correctly. When OFF, the default setting, no NULL character is set after a CR. To set this feature, see “SET TELNET INSERTNULL” on page 90.

- ❑ MAC address aging time - The current value for the MAC address aging timer. The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. To set this value, refer to “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 157.
- ❑ Console startup mode - The management interface —menus or command line — that initially appears at the start of a local or remote management session. The default is the command line interface. This cannot be changed on a stack, because a stack must be configured from the command line interface.
- ❑ Multicast Mode - The multicast mode, which determines the behavior of the stack when forwarding ingress spanning tree BPDU packets and 802.1x port-based access control EAPOL packets To set the multicast mode, refer to “SET SWITCH MULTICASTMODE” on page 353.

### Example

This command displays information about the master switch:

```
show switch module=1
```

## SHOW SYSTEM

---

### Syntax

`show system`

### Parameters

None.

### Description

This command displays the following information about the master switch of a stack:

#### MAC Address

The MAC address of the master switch.

#### Model Name

The model name of the master switch.

#### Serial Number

The serial number of the master switch.

#### IP Address

The IP address of the local interface.

#### Subnet Mask

The subnet mask of the local interface.

#### Default Gateway

For a stack, this field displays the default gateway address. This is the IP address of a router interface on your network. The management software uses this address as the next hop to reaching a remote network device when the stack's local interface and the remote device are on different subnets. The default value is 0.0.0.0.

#### System Up Time

The length of time since the stack was last reset or power cycled.

#### Bootloader

The version number and build date of the AT-S63 bootloader.

#### Application

The version number and build date of the AT-S63 Management Software.

#### System Name

The name of the stack.

**Administrator**

The name of the network administrator responsible for managing the stack.

**Location**

The location of the stack, (for example, 4th Floor - rm 402B).

---

**Note**

To configure the name, administrator, and location parameters, refer to “SET SYSTEM” on page 89.

---

**Power Information**

The status of the main power supply, the redundant power supply (if present), and internal power consumption in the master switch.

**Temperature (Deg.C)**

The ambient temperature as measured where the air enters the cooling vents on the side of the master switch.

**Fan Information**

The speed or operating status of the system fan(s).

**Example**

```
show system
```

## SHOW TIME

---

### Syntax

```
show time
```

### Parameters

None.

### Description

This command shows the stack's current date and time.

### Example

```
show time
```

## Chapter 6

# SNMPv2 and SNMPv2c Commands

---

This chapter contains the following commands:

- ❑ “ADD SNMP COMMUNITY” on page 104
- ❑ “CREATE SNMP COMMUNITY” on page 106
- ❑ “DELETE SNMP COMMUNITY” on page 109
- ❑ “DESTROY SNMP COMMUNITY” on page 111
- ❑ “DISABLE SNMP” on page 112
- ❑ “DISABLE SNMP AUTHENTICATETRAPH” on page 113
- ❑ “DISABLE SNMP COMMUNITY” on page 114
- ❑ “ENABLE SNMP” on page 115
- ❑ “ENABLE SNMP AUTHENTICATETRAPH” on page 116
- ❑ “ENABLE SNMP COMMUNITY” on page 117
- ❑ “SET SNMP COMMUNITY” on page 118
- ❑ “SHOW SNMP” on page 120

---

### **Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

## ADD SNMP COMMUNITY

---

### Syntax

```
add snmp community="community" [traphost=ipaddress]  
[manager=ipaddress]
```

### Parameters

community	Specifies an existing SNMP community string on the stack. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character such as an exclamation point. Otherwise, the quotes are optional.
traphost	Specifies the IP address of a trap receiver.
manager	Specifies the IP address of a management station to have SNMP access to the stack using the community string.

### Description

This command adds the IP address of a trap receiver or a management station to an existing community string.

The TRAPHOST parameter specifies a trap receiver for the SNMP community string. This is the IP address of a device to which traps generated by the stack are sent. A community string can have up to eight IP addresses of trap receivers, but only one can be added at a time with this command.

The MANAGER parameter specifies a management station to be allowed SNMP management access to the stack using the community string. This parameter applies only to community strings with a closed status. A community string can have up to eight IP addresses of management stations, but only one can be added at a time with this command.

To create a new community string, refer to “CREATE SNMP COMMUNITY” on page 106. To view the current community strings, refer to “SHOW SNMP” on page 120.

### Examples

The following command permits access by a management station with the IP address 149.212.11.22 to the stack through the “private” community string:

```
add snmp community=private manager=149.212.11.22
```



The following command adds the IP address 149.212.10.11 as a trap receiver to the “public” community string:

```
add snmp community=public traphost=149.212.10.11
```

## CREATE SNMP COMMUNITY

---

### Syntax

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

### Parameters

community	Specifies a new community string. The maximum length of a community string is 15 alphanumeric characters. Spaces are allowed. The name must be enclosed in double quotes if it includes a space or other special character such as an exclamation point. Otherwise, the quotes are optional. The string is case sensitive.
access	Specifies the access level of the new community string. Options are “read” for read only access and “write” for both read and write access. The default is “read.”
open	Specifies the open or closed status of the community string. The options are: <div> <div>yes, on, true</div> <div>The community string is open, meaning any management station can use the string to access the stack. These values are equivalent.</div> <div>no, off, false</div> <div>The community string is closed, meaning only those management stations whose IP addresses are assigned to the string can use it to access the stack. You can assign a management IP address to the string using the MANAGER option in this command. The default setting for a community string is closed. These values are equivalent.</div> </div>
traphost	Specifies the IP address of a trap receiver to receive system traps.
manager	Specifies the IP address of a management station that can use the community string to access the stack. This option applies if you specify the status of the community string as closed. A community string can have up to eight IP addresses of management stations, but only one can be assigned with this option.

## Description

This command creates a new SNMP community string on the stack. The stack comes with two default community strings, “public,” with an access of read only, and “private,” with an access level of read and write. A stack can support up to eight community strings.

The COMMUNITY parameter specifies the new community string. The string can be up to 15 alphanumeric characters. The string is case sensitive.

The ACCESS parameter defines the access level for the new community string. The access level can be either read or read and write. The READ option specifies the read access level and the WRITE option specifies the read and write access level.

The OPEN parameters controls whether the string will have an open or closed status. If you specify YES, ON or TRUE, the string will have an open status. Any management station will be able to use the string to access the stack. If you specify NO, OFF or FALSE, the string will have a closed status and only those management stations whose IP addresses are assigned to the stack will be able to use the string. This is the default.

The TRAPHOST parameter specifies the IP address of a trap receiver to receive traps from the stack. A community string can have up to eight trap receivers, but only one can be assigned when a community string is created. To add IP addresses of trap receivers to an existing community string, see “ADD SNMP COMMUNITY” on page 104.

The MANAGER parameter specifies the IP address of a management station to be permitted SNMP access to the stack through the community string. You use this parameter when you give a community string a closed status. A community string with a closed status can only be used by those management stations whose IP addresses have been assigned to the string.

A community string can have up to eight manager IP addresses, but only one can be assigned when a community string is created. To add IP addresses of management stations to an existing community string, see “ADD SNMP COMMUNITY” on page 104.

## Examples

The following command creates the new community string “serv12” with read access level and an access status of open:

```
create snmp community=serv12 access=read open=yes
```

The following command creates the new community string “wind11” with read and write access level. To limit the use of the string, its access status is specified as closed and it is assigned the IP address of the management

station that will use the string:

```
create snmp community=wind11 access=write open=no  
manager=149.35.24.22
```

(The OPEN=NO parameter can be omitted from the example because closed status is the default for a new community string.)

This command creates a community string called “serv12” with a closed status. The command assigns the string the IP address of a management station that can use the string and also receive SNMP traps:

```
create snmp community=serv12 access=write open=no  
traphost=149.35.24.22 manager=149.35.24.22
```

## DELETE SNMP COMMUNITY

---

### Syntax

```
delete snmp community="community" traphost=ipaddress  
manager=ipaddress
```

### Parameters

community	Specifies the SNMP community string on the stack to be modified. The community string must already exist on the stack. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character, such as an exclamation point. Otherwise, the quotes are optional.
traphost	Specifies the IP address of a trap receiver to be removed from the community string.
manager	Specifies the IP address of a management station to be removed from the community string.

### Description

This command removes the IP addresses of trap receivers and management workstations from a community string.

The TRAPHOST parameter removes the IP address of a trap receiver from an SNMP community string. Once an IP address is removed, the stack will not send SNMP traps to the trap receiver represented by the address.

The MANAGER parameter removes the IP address of a management station from the community string. A management station removed from a community string with a closed status can no longer use SNMP and the community string to manage the stack. If you remove the last management station IP address from a community string with a closed status, no SNMP management station can access the stack using that community string.

### Examples

The following command deletes the IP address 149.212.11.22 of a management station from the community string "private."

```
delete snmp community=private  
manager=149.212.11.22
```

The following command deletes the IP address 149.212.44.45 of a trap receiver from the community string “public.”

```
delete snmp community=public traphost=149.212.44.45
```

## DESTROY SNMP COMMUNITY

---

### Syntax

```
destroy snmp community="community"
```

### Parameter

community	Specifies an SNMP community string to delete from the stack. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character, such as an exclamation point. Otherwise, the quotes are optional.
-----------	--

### Description

This command deletes an SNMP community string from the stack. IP addresses of management stations and SNMP trap receivers assigned to the community string are deleted as well.

### Example

The following command deletes the community string "wind44":

```
destroy snmp community=wind44
```

## DISABLE SNMP

---

### Syntax

```
disable snmp
```

### Parameters

None.

### Description

This command disables SNMP on the stack. You cannot manage the unit from an SNMP management station when SNMP is disabled. The default setting for SNMP is disabled.

### Example

The following command disables SNMP on the stack:

```
disable snmp
```



## DISABLE SNMP AUTHENTICATETRAP

---

### Syntax

```
disable snmp authenticatetrap|authenticate_trap
```

### Parameters

None.

### Description

This command stops the stack from sending authentication failure traps to trap receivers. However, the stack will continue to send other system traps, such as alarm traps. The default setting for sending authentication failure traps is disabled.

The AUTHENTICATETRAP and AUTHENTICATE\_TRAP keywords are equivalent.

To activate the authentication failure trap, refer to “ENABLE SNMP AUTHENTICATETRAP” on page 116.

### Example

The following command instructs the stack not to send authentication failure traps to SNMP trap receivers:

```
disable snmp authenticatetrap
```

## DISABLE SNMP COMMUNITY

---

### Syntax

```
disable snmp community="community"
```

### Parameter

community	Specifies an SNMP community string to disable on the stack. This parameter is case sensitive. The string must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.
-----------	--

### Description

This command disables a community string on the stack, while leaving SNMP and all other community strings active. IP addresses of management stations or trap receivers assigned to the community string are also disabled. A disabled community string cannot be used by a management station to access the stack.

### Example

The following command deactivates the SNMP community string "sw1200" and the IP addresses of any management stations and trap receivers assigned to the community string:

```
disable snmp community=sw1200
```

## ENABLE SNMP

---

### Syntax

```
enable snmp
```

### Parameters

None.

### Description

This command activates SNMP on the stack so that you can remotely manage the unit with an SNMP application program from a management station on your network. It also enables the stack to send SNMP traps to trap receivers. The default setting for SNMP on the stack is disabled.

### Example

The following command activates SNMP on the stack:

```
enable snmp
```

## ENABLE SNMP AUTHENTICATETRAP

---

### Syntax

```
enable snmp authenticatetrap|authenticate_trap
```

### Parameters

None.

### Description

This command configures the stack to send authentication failure traps to trap receivers. The stack sends an authentication failure trap whenever a SNMP management station attempts to access the stack using an incorrect or invalid community string, or the management station's IP address has not been added to a community string that has a closed access status.

The default setting for sending authentication failure traps is disabled. Refer to "ADD SNMP COMMUNITY" on page 104 to enter the IP addresses of the SNMP trap receivers.

The AUTHENTICATETRAP and AUTHENTICATE\_TRAP keywords are equivalent.

### Example

The following command configures the stack to send authentication failure traps to SNMP trap receivers:

```
enable snmp authenticatetrap
```

## ENABLE SNMP COMMUNITY

---

### Syntax

```
enable snmp community="community"
```

### Parameter

community	Specifies an SNMP community string. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.
-----------	--

### Description

This command activates a community string on the stack. The default setting for a new community string is enabled. You can use this command to enable a community string that you disabled with the DISABLE SNMP COMMUNITY command.

### Example

The following command enables the SNMP community string "private":

```
enable snmp community=private
```

# SET SNMP COMMUNITY

---

### Syntax

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

### Parameters

community	Specifies the SNMP community string whose access level or access status is to be changed. This community string must already exist on the stack. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.
access	Specifies the new access level. Options are “read” for read only access and “write” for both read and write access. If no access level is specified, the default is “read.”
open	Specifies the open or closed access status of the community string. The options are: <div><div>yes, on, true      The community string is open, meaning that any management station can use the string to access the stack. These options are equivalent.</div><div>no, off, false     The community string is closed, meaning that only those management stations whose IP addresses are assigned to the string can use it to access the stack. To add IP addresses of management stations to a community string, refer to “ADD SNMP COMMUNITY” on page 104. The default setting for a community string is closed. These options are equivalent.</div></div>

### Description

This command changes the access level and access status of an existing SNMP community string.

## Examples

The following command changes the access status for the SNMP community string "sw44" to closed:

```
set snmp community=sw44 open=no
```

The following command changes the access level for the SNMP community string "serv12" to read and write with open access:

```
set snmp community=serv12 access=write open=yes
```

## SHOW SNMP

---

### Syntax

```
show snmp [community="community"]
```

### Parameter

community	Specifies a community string on the stack. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional. Default community strings are "public" and "private."
-----------	---

### Description

This command displays the following SNMP information:

- ❑ **SNMP status** - The status will be enabled or disabled. If enabled, you can manage the stack with an SNMP application program from a remote management station. If disabled, you cannot remotely manage the stack using SNMP. The default for SNMP is disabled. To enable SNMP, refer "ENABLE SNMP" on page 115. To disable SNMP, refer to "DISABLE SNMP" on page 112.
- ❑ **Authentication failure traps** - This status will be enabled or disabled. If enabled, the stack sends out authentication failure traps to trap receivers. If disabled, the stack will not send out authentication failure traps, but will send out other system traps. The stack sends an authentication failure trap whenever a SNMP management station attempts to access the stack using an incorrect or invalid community string, or the management station's IP address has not been added to a community string that has a closed access status. The default setting is enabled.

To enable authentication failure traps, refer to "ENABLE SNMP AUTHENTICATETRAPH" on page 116. To disable the sending of this trap, see "DISABLE SNMP AUTHENTICATETRAPH" on page 113. To add IP addresses of management stations to receive the trap, refer to the "ADD SNMP COMMUNITY" on page 104.

- ❑ **SNMP community strings** - The stack comes with the two default community strings public, which has read access, and private, which has read and write access. To add new community strings, see "CREATE SNMP COMMUNITY" on page 106. To delete community strings, refer to "DESTROY SNMP COMMUNITY" on page 111.
- ❑ **Management station IP addresses** - These are the IP addresses of management stations that can access the stack through a community



string that has a closed access status. (Management station IP addresses are displayed only when you specify a specific community string using the COMMUNITY parameter in this command.) To add IP addresses of management stations to a community string, refer to “ADD SNMP COMMUNITY” on page 104.

- ❑ Trap receiver IP addresses - These are the IP addresses of management stations to receive SNMP traps from the stack. (IP addresses or trap receivers are displayed only when you specify a specific community string using the COMMUNITY parameter in this command.) To add IP addresses to a community string, refer to “ADD SNMP COMMUNITY” on page 104.
- ❑ Access Status - If a community string shows an Open Access with Yes, the string has an open access status, meaning any management stations can use the string. A string with a Open Access of No has a closed access status; only those management stations whose IP addresses have been assigned to the string can use it. To change the access status, refer to “SET SNMP COMMUNITY” on page 118.

### Examples

The following command displays the SNMP status and the community strings on the stack:

```
show snmp
```

The following command displays specific information about the “private” community string. The information includes the IP addresses of management stations that can use the string and the IP addresses of SNMP trap receivers:

```
show snmp community=private
```



## Chapter 7

# Port Parameter Commands

---

This chapter contains the following commands:

- ❑ “DISABLE SWITCH PORT” on page 124
- ❑ “DISABLE SWITCH PORT FLOW” on page 125
- ❑ “ENABLE SWITCH PORT” on page 126
- ❑ “ENABLE SWITCH PORT FLOW” on page 127
- ❑ “PURGE SWITCH PORT” on page 128
- ❑ “RESET SWITCH PORT” on page 129
- ❑ “SET SWITCH PORT” on page 130
- ❑ “SET SWITCH PORT FILTERING” on page 134
- ❑ “SET SWITCH PORT RATELIMITING” on page 137
- ❑ “SHOW SWITCH PORT” on page 140

---

### **Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

## DISABLE SWITCH PORT

---

### Syntax

```
disable switch port=port
```

### Parameter

**port** Specifies the port to disable. You can specify more than one port at a time. Port numbers are entered in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command disables a port. A disabled port does not forward traffic. You might disable unused ports on the stack to prevent them from being used by unauthorized individuals. The default setting for a port is enabled.

### Example

This command disables ports 2.12 and 2.24:

```
disable switch port=2.12,2.24
```

### Equivalent Command

```
set switch port=port status=disable
```

For information, see “SET SWITCH PORT” on page 130.

## DISABLE SWITCH PORT FLOW

---

### Syntax

```
disable switch port=port flow=pause
```

### Parameter

**port** Specifies the port where flow control is to be disabled. You can specify more than one port at a time. Port numbers are entered in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command deactivates flow control on a port. Flow control only applies to ports operating in full duplex mode.

### Example

The following command deactivates flow control on port 4.6:

```
disable switch port=4.6 flow=pause
```

### Equivalent Command

```
set switch port=port flowcontrol=disable
```

For information, see “SET SWITCH PORT” on page 130.

## ENABLE SWITCH PORT

---

### Syntax

```
enable switch port=port
```

### Parameter

**port** Specifies the port to enable. You can specify more than one port at a time. Port numbers are specified in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command enables a port. When a port is enabled, it forwards traffic. The default setting for a port is enabled.

### Example

The following command enables ports 2.1 to 2.4:

```
enable switch port=2.1-2.4
```

### Equivalent Command

```
set switch port=port status=enable
```

For information, see “SET SWITCH PORT” on page 130.

## ENABLE SWITCH PORT FLOW

---

### Syntax

```
enable switch port=port flow=pause
```

### Parameter

**port** Specifies the port where you want to active flow control. You can specify more than one port at a time. Port numbers are specified in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command activates flow control on a port. Flow control applies to ports operating in full duplex mode. When flow control is activated, a port sends out a PAUSE packet whenever it wants the end node to stop sending packets.

### Example

The following command activates flow control on port 1.5:

```
enable switch port=1.5 flow=pause
```

### Equivalent Command

```
set switch port=port flowcontrol=enable
```

For information, see “SET SWITCH PORT” on page 130.

## PURGE SWITCH PORT

---

### Syntax

```
purge switch port=port
```

### Parameters

**port** Specifies the port whose parameter settings are to be returned to the default values. You can specify more than one port at a time. Port numbers are specified in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command returns all of the parameter settings of a port to the factory default values. To reset a port and retain its settings, use “RESET SWITCH PORT” on page 129.

### Example

This example resets the settings for port 2.10 to the factory default values:

```
purge switch port=2.10
```



## RESET SWITCH PORT

---

### Syntax

```
reset switch port=port
```

### Parameter

**port** Specifies the port to reset. You can specify more than one port at a time. Port numbers are specified in the following format:

`module ID.port number`

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command resets a port. The reset takes less than a second to complete. You might reset a port if it is experiencing a problem establishing a link with its end node. The port retains its current operating parameter settings. To reset a port to the factory default settings, use “PURGE SWITCH PORT” on page 128.

### Example

The following command resets ports 3.5 to 3.8:

```
reset switch port=3.5-3.8
```

### Equivalent Command

```
set switch port=port softreset
```

For information, see “SET SWITCH PORT” on page 130.

## SET SWITCH PORT

---

### Syntax

```
set switch port=port [description="description"]
[status=enabled|disabled]
[speed=autonegotiate|10mhalf|10mfull|100mhalf|100mfull|
1000mfull]
[mdimode=mdi|mdix|auto]
[flowcontrol=disable|enable|auto]
[fctrlimit=value]
[backpressure=yes|no|on|off|true|false|enabled|
disabled]
[bplimit=value]
[holbplimit=value]
[renegotiation=auto]
[softreset]
```

### Parameters

port	<p>Specifies the port to be configured. You can configure more than one port at a time. Port numbers are specified in the following format:</p> <p>module ID.port number</p> <p>For instructions, refer to “Port Numbers in Commands” on page 42.</p>				
description	<p>Specifies a description of up to 15 alphanumeric characters for the port. Spaces are allowed but not special characters. A name with spaces must be enclosed in double quotes. Otherwise, the quotes are optional. You cannot specify a description if you are configuring more than one port.</p>				
status	<p>Specifies the operating status of the port. The options are:</p> <table> <tr> <td>enabled</td><td>The port forwards network traffic. This is the default setting.</td></tr> <tr> <td>disabled</td><td>The port does not forward network traffic.</td></tr> </table>	enabled	The port forwards network traffic. This is the default setting.	disabled	The port does not forward network traffic.
enabled	The port forwards network traffic. This is the default setting.				
disabled	The port does not forward network traffic.				
speed	<p>Sets the speed and duplex mode of the port. The options are:</p> <table> <tr> <td>autonegotiate</td><td>The port uses Auto-Negotiation for both speed and duplex mode. This is the default setting.</td></tr> </table>	autonegotiate	The port uses Auto-Negotiation for both speed and duplex mode. This is the default setting.		
autonegotiate	The port uses Auto-Negotiation for both speed and duplex mode. This is the default setting.				

10mhalf	10 Mbps and half-duplex mode.
10mfull	10 Mbps and full-duplex mode.
100mhalf	100 Mbps and half-duplex mode.
100mfull	100 Mbps and full-duplex mode.
1000mfull	1000 Mbps and full-duplex mode. (Applies only to 1000Base SFP and GBIC modules. This selection should not be used. An SFP or GBIC module should use Auto-Negotiation to set its speed and duplex mode.)

**Note**

A 10/100/1000Base-T twisted pair port must be set to Auto-Negotiation to operate at 1000 Mbps.

mdimode	<p>Sets the wiring configuration of the port. This parameter applies to twisted pair ports, and only when a port's speed and duplex mode are set manually. If a port is auto-negotiating its speed and duplex mode, the MDI/MDIX setting is established automatically and cannot be changed. The options are:</p> <p>mdi     Sets the port's configuration to MDI.</p> <p>mdix    Sets the port's configuration to MDI-X.</p>
flowcontrol	<p>Specifies the flow control on the port. Flow control applies only to ports operating in full duplex mode. When flow control is activated, a port sends out a PAUSE packet whenever it wants the end node to stop sending packets. The options are:</p> <p>disabled    No flow control. This is the default setting.</p> <p>enabled     Flow control is activated.</p>
fctrlimit	<p>Specifies the number of cells for flow control. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.</p>

backpressure	Controls backpressure on the port. Backpressure applies only to ports operating in half-duplex mode. The options are:
	yes, on, true, enabled      Activates backpressure on the port. These options are equivalent.
	no, off, false, disabled      Deactivates backpressure on the port. This is the default. These options are equivalent.
bplimit	Specifies the number of cells for back pressure. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.
holbplimit	Specifies the threshold at which the stack signals a head of line blocking event on a port. The threshold is specified in cells. A cell is 128 bytes. The range is 1 to 61,440 cells; the default is 7,168.
renegotiation	Prompts the port to renegotiate its speed and duplex mode with the end node. This parameter only works when the port is using Auto-Negotiation. The only option is:
	auto      Renegotiates speed and duplex mode with the end node.
softreset	Resets the port. This parameter does not change any of a port's operating parameters.

### Description

This command configures the operating parameters of a port. You can set more than one parameter at a time.

### Examples

The following command disables ports 4.1 to 4.6:

```
set switch port=4.1-4.6 status=disabled
```

The following command configures port 3.8 to operate at 10 Mbps, half duplex:

```
set switch port=3.8 speed=10mhalf
```

The following command sets the speed on ports 1.2 to 1.6 to 100 Mbps, the duplex mode to full duplex, the wiring configuration to MDI-X, and flow control to enabled:

```
set switch port=1.2-1.6 speed=100mfull mdimode=mdix  
flowcontrol=enabled
```

The following command resets port 5.5:

```
set switch port=5.5 softreset
```

### **Equivalent Commands**

```
disable switch port=port
```

For information, see “DISABLE SWITCH PORT” on page 124.

```
disable switch port=port flow=pause
```

For information, see “DISABLE SWITCH PORT FLOW” on page 125.

```
enable switch port=port
```

For information, see “ENABLE SWITCH PORT” on page 126.

```
enable switch port=port flow=pause
```

For information, see “ENABLE SWITCH PORT FLOW” on page 127.

```
reset switch port=port
```

For information, see “RESET SWITCH PORT” on page 129.

## SET SWITCH PORT FILTERING

---

### Syntax

```
set switch port=port
[bcastfiltering=yes|no|on|off|true|false|enabled|
disabled]
[bcastegressfiltering=yes|no|on|off|true|false|enabled|
disabled]
[unkmcastfiltering=yes|no|on|off|true|false]
[unkmcastegressfiltering=yes|no|on|off|true|false]
[unkucastfiltering=yes|no|on|off|true|false]
[unkucastegressfiltering=yes|no|on|off|true|false]
```

### Parameters

port	<p>Specifies the port you want to configure. You can specify more than one port at a time. Port numbers are entered in the following format:</p> <pre>module ID.port number</pre> <p>For instructions, refer to “Port Numbers in Commands” on page 42.</p>				
bcastfiltering	<p>Controls the ingress broadcast frame filter. The options are:</p> <table> <tr> <td>yes, on, true, enabled</td><td>The port discards all ingress broadcast frames. These options are equivalent.</td></tr> <tr> <td>no, off, false, disabled</td><td>The port forwards all ingress broadcast frames. This is the default. These options are equivalent.</td></tr> </table>	yes, on, true, enabled	The port discards all ingress broadcast frames. These options are equivalent.	no, off, false, disabled	The port forwards all ingress broadcast frames. This is the default. These options are equivalent.
yes, on, true, enabled	The port discards all ingress broadcast frames. These options are equivalent.				
no, off, false, disabled	The port forwards all ingress broadcast frames. This is the default. These options are equivalent.				
bcastegressfiltering	<p>Controls the egress broadcast frame filter. The options are:</p> <table> <tr> <td>yes, on, true, enabled</td><td>The port discards all egress broadcast frames. These options are equivalent.</td></tr> <tr> <td>no, off, false, disabled</td><td>The port forwards all egress broadcast frames. This is the default. These options are equivalent.</td></tr> </table>	yes, on, true, enabled	The port discards all egress broadcast frames. These options are equivalent.	no, off, false, disabled	The port forwards all egress broadcast frames. This is the default. These options are equivalent.
yes, on, true, enabled	The port discards all egress broadcast frames. These options are equivalent.				
no, off, false, disabled	The port forwards all egress broadcast frames. This is the default. These options are equivalent.				

unkmcastfiltering	Controls the unknown ingress multicast frame filter. The options are:
yes, on, true, enabled	The port discards all unknown ingress multicast frames. These options are equivalent.
no, off, false, disabled	The port forwards all unknown ingress multicast frames. This is the default. These options are equivalent.
unkmcastegressfiltering	Controls the unknown egress multicast frame filter. The options are:
yes, on, true, enabled	The port discards all unknown egress multicast frames. These options are equivalent.
no, off, false, disabled	The port forwards all unknown egress multicast frames. These options are equivalent.
unkucastfiltering	Controls the unknown ingress unicast frame filter. The options are:
yes, on, true, enabled	The port discards all unknown ingress unicast frames. These options are equivalent.
no, off, false, disabled	The port forwards all unknown ingress unicast frames. This is the default. These options are equivalent.
unkucastegressfiltering	Controls the unknown egress unicast frame filter. The options are:
yes, on, true, enabled	The port discards all unknown egress unicast frames. These options are equivalent.

no, off, false, disabled    The port forwards all unknown egress unicast frames. This is the default. These options are equivalent.

### Description

This command discards ingress and egress broadcast packets as well as unknown unicast and multicast packets on a port. When you activate this feature on a port, the port discards all ingress or egress packets of the type specified. The default setting for each type of packet filter is disabled.

### Examples

This command activates the ingress broadcast filter on ports 2.4 and 2.23. The ports discard all ingress broadcast packets:

```
set switch port=2.4,2.23 bcastfiltering=yes
```

This command activates the unknown egress multicast and unicast filters on ports 3.3 and 3.6, causing the ports to discard all unknown egress multicast and unicast packets:

```
set switch port=3.3,3.6 unkmcastegressfiltering=yes
unkucastegressfiltering=yes
```

This command disables the unknown ingress unicast filter on port 2.24 so that the port again accepts all unknown ingress unicast packets:

```
set switch port=2.24 unkucastfiltering=no
```



## SET SWITCH PORT RATELIMITING

---

### Syntax

```
set switch port=port
[bcastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[bcastrate=value]
[mcastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[mcastrate=value]
[unkucastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[unkucastrate=value]
```

### Parameters

port	<p>Specifies the port to be configured. You can specify more than one port at a time, but the ports must be of the same medium type. For example, you cannot configure twisted pair and fiber optic ports with the same command. Port numbers are specified in the following format:</p> <pre>module ID.port number</pre> <p>For instructions, refer to “Port Numbers in Commands” on page 42.</p>					
bcastratelimiting	<p>Enables or disables rate limit for ingress broadcast packets. The options are:</p> <table><tr><td>yes, on, true, enabled</td><td>Activates broadcast packet rate limiting on the port. The options are equivalent. The rate limit is set with the BCASTRATE parameter.</td></tr><tr><td>no, off, false, disabled</td><td>Deactivates broadcast packet rate limit on the port. This is the default. The options are equivalent.</td></tr></table>	yes, on, true, enabled	Activates broadcast packet rate limiting on the port. The options are equivalent. The rate limit is set with the BCASTRATE parameter.	no, off, false, disabled	Deactivates broadcast packet rate limit on the port. This is the default. The options are equivalent.	
yes, on, true, enabled	Activates broadcast packet rate limiting on the port. The options are equivalent. The rate limit is set with the BCASTRATE parameter.					
no, off, false, disabled	Deactivates broadcast packet rate limit on the port. This is the default. The options are equivalent.					
bcastrate	<p>Specifies the maximum number of ingress broadcast packets a port accepts each second. The range is 0 to 262,134 packets. The default is 262,134 packets</p>					

mcastratelimiting	Enables or disables a rate limit for ingress multicast packets. The options are:	
	yes, on, true, enabled	Activates multicast packet rate limit on the port. The options are equivalent.
	no, off, false, disabled	Deactivates multicast packet rate limit on the port. This is the default. The options are equivalent.
mcastrate	Specifies the maximum number of ingress multicast packets a port accepts each second. The range is 0 to 262,134 packets. The default is 262,134 packets.	
unkucastratelimiting	Enables or disables rate limit for unknown ingress unicast packets. The options are:	
	yes, on, true, enabled	Activates unknown unicast packet rate limit on the port. The options are equivalent.
	no, off, false, disabled	Deactivates unknown unicast packet rate limit on the port. This is the default. The options are equivalent.
unkucastrate	Specifies the maximum number of ingress unknown unicast packets a port accepts each second. The range is 0 to 262,134 packets. The default is 262,134 packets.	

### Description

This command sets the maximum number of ingress packets a port accepts each second. Packets exceeding the threshold are discarded. You can enable the rate limiting threshold independently for broadcast, multicast and unknown unicast packets.

## Examples

This command activates rate limiting for ingress broadcast and multicast packets on port 1.6. It sets a threshold of 20,000 packets per second for broadcast packets and 100,000 for multicast packets:

```
set switch port=1.6 bcastratelimiting=yes bcastrate=20000  
mcastratelimiting=yes mcastrate=100000
```

This command sets a threshold of 150,000 packets per second for unknown ingress unicast packets on ports 2.15 and 2.17:

```
set switch port=2.15,2.17 unkucastratelimiting=yes  
unkucastrate=150000
```

This command disables the rate limiting feature for ingress broadcast packets on port 3.24:

```
set switch port=3.24 bcastratelimiting=no
```

## SHOW SWITCH PORT

---

### Syntax

```
show switch port[=port]
```

### Parameter

**port** Specifies the port whose parameter settings you want to view. You can specify more than one port at a time. Omitting this parameter displays all ports. Port numbers are entered in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command displays a port’s current operating specifications, such as speed and duplex mode. The command displays the following port information. (For an example of the information displayed by this command, see Figure 14 on page 144.)

- ❑ **Port Description** - Displays the name of the port. The default name is “Port\_” followed by the port number. To configure a port’s name, refer to “SET SWITCH PORT” on page 130.
- ❑ **Port Type** - Displays the IEEE standard of a port. For example, the port type for a twisted pair port on an AT-9424T/SP switch is 10/100/1000Base-T.
- ❑ **Status** - Displays whether the port is currently enabled or disabled. When disabled, a port does not forward network traffic. The default is enabled. To disable or enable a port, refer to “DISABLE SWITCH PORT” on page 124, “ENABLE SWITCH PORT” on page 126, or “SET SWITCH PORT” on page 130.
- ❑ **Link State** - Displays the current link state between the port and the end node. If the port has established a link with an end node, link state will be “Up.” If there is no link, link state will be “Down.”
- ❑ **Configured Speed/Duplex** - Displays the current configured settings for speed and duplex mode on the port. The setting of “Auto” indicates the port has been set to Auto-Negotiation, the default setting. To adjust a port’s speed and duplex mode, refer to “SET SWITCH PORT” on page 130.
- ❑ **Configured MDI Crossover** - Displays the current configured setting for MDI/MDIX on the port. If the port is set to Auto-Negotiation, this field

displays N/A, because the MDI/MDIX setting is set automatically on the port. A value only appears in this field if you disable Auto-Negotiation on a twisted pair port and set MDI/MDIX manually. This field does not apply to a fiber optic port. To adjust a port's MDI/MDIX setting, refer to "SET SWITCH PORT" on page 130.

- ❑ Actual Speed/Duplex - Displays the current operating speed and duplex mode of a port. This field displays no value (—) if the port does not have a link to an end node or has been disabled.
- ❑ Actual MDI Crossover- Displays the current operating MDI/MDIX setting of a twisted pair port. This field displays no value (—) if the port does not have a link to an end node or has been disabled. This field does not apply to a fiber optic port.
- ❑ Flow Control Status and Flow Control Threshold - Displays the status of flow control on a port. Flow control applies to ports operating in full duplex mode and is used by a port to stop an end node from sending packets when its ingress buffer is full. The default setting is disabled. The threshold marks the point at which flow control is activated. The threshold is measured in cells of 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells. To set flow control, refer to "DISABLE SWITCH PORT FLOW" on page 125, "ENABLE SWITCH PORT FLOW" on page 127, or "SET SWITCH PORT" on page 130.
- ❑ Backpressure Status and Backpressure Threshold - Displays the status of backpressure on a port. Backpressure applies to ports operating in half duplex mode. A port uses backpressure to stop an end node from sending packets when its ingress buffer is full. The default setting is disabled. The threshold marks the point at which backpressure is activated. The threshold is measured in cells of 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells. To set backpressure, refer to "SET SWITCH PORT" on page 130.
- ❑ HOL Blocking Prevention Threshold - Displays the threshold of a head of line blocking event. This event occurs when a port cannot forward packets to an egress queue of another stack port because the queue is full. The stack responds by instructing all ports to discard any packets in their ingress queues destined for the oversubscribed port. The threshold is measured in cells of 128 bytes. The range is 0 to 8191 cells. The default is 682.
- ❑ Broadcast Ingress Filtering - Displays the status of ingress broadcast filtering. The feature when enabled on a port discards all ingress broadcast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 134.
- ❑ Broadcast Egress Filtering - Displays the status of egress broadcast filtering. If enabled, the port discards all egress broadcast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 134.

- ❑ Unknown Multicast Ingress Filtering - Displays the status of unknown ingress multicast filtering. If enabled, the port discards all unknown ingress multicast packets. The default is disabled. To configure this parameter, refer to “SET SWITCH PORT FILTERING” on page 134.
- ❑ Unknown Multicast Egress Filtering - Displays the status of unknown egress multicast filtering. If enabled, the port discards all unknown egress multicast packets. The default is disabled. To configure this parameter, refer to “SET SWITCH PORT FILTERING” on page 134.
- ❑ Unknown Unicast Ingress Filtering - Displays the status of unknown ingress unicast filtering. If enabled, the port discards all unknown ingress unicast packets. The default is disabled. To configure this parameter, refer to “SET SWITCH PORT FILTERING” on page 134.
- ❑ Unknown Unicast Egress Filtering - Displays the status of unknown egress unicast filtering. If enabled, the port discards all unknown egress unicast packets. The default is disabled. To configure this parameter, refer to “SET SWITCH PORT FILTERING” on page 134.
- ❑ Broadcast Rate Limiting Status and Broadcast Rate - Displays the status of the broadcast rate limiting feature. If enabled, the port limits the number of ingress broadcast packets per second to the rate specified. Ingress broadcast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to “SET SWITCH PORT RATELIMITING” on page 137.
- ❑ Multicast Rate Limiting Status and Multicast Rate - Displays the status of the multicast rate limiting feature. If enabled, the port limits the number of ingress multicast packets per second to the rate specified. Ingress multicast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to “SET SWITCH PORT RATELIMITING” on page 137.
- ❑ Unknown Unicast Rate Limiting Status and Unknown Unicast Rate - Displays the status of the unicast rate limiting feature. If enabled, the port limits the number of unknown ingress unicast packets per second to the rate specified. Unknown ingress unicast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to “SET SWITCH PORT RATELIMITING” on page 137.
- ❑ PVID - Displays the port’s VLAN ID number. This number is equivalent to the VID of the VLAN where the port is currently an untagged member. The default is 1, the VID of the Default\_VLAN. To add a port to an existing VLAN or to create a new VLAN, refer to “ADD VLAN” on page 374 and “CREATE VLAN” on page 376.
- ❑ Port Priority - Displays the Class of Service priority assigned to the port. This priority level applies to all ingress untagged packets received on the port. The default setting is 0. At the default setting, all ingress untagged packets received on the port are stored in the egress port’s

Q1 egress queue. To set this parameter, refer to “SET SWITCH PORT PRIORITY OVERRIDEPRIORITY” on page 264.

- ❑ **Override Priority** - Displays whether the Class of Service priority level in ingress tagged packets is ignored when determining the egress queue for storing the packets. If this parameter is displaying Yes the stack ignores the priority level in tagged packets and uses the priority level assigned to the port to determine the egress queue. The default setting is No. At the default setting, the priority level in tagged packets is used to determine the appropriate egress queue. To set this parameter, refer to “SET SWITCH PORT PRIORITY OVERRIDEPRIORITY” on page 264.
- ❑ **Mirroring State** - Displays the state of port mirroring on the stack. If port mirroring has been activated on the stack, this field will contain Enabled. If port mirroring has not been activated on the stack, the default setting, this field will contain Disabled. To configure port mirroring, refer to “SET SWITCH MIRROR” on page 193 and “SET SWITCH PORT MIRROR” on page 194.
- ❑ **Is this mirror port mirror** - Displays whether the port is functioning as the destination port of a port mirror. This field only appears if port mirroring has been activated on the stack. This field displays No if the port is not the destination port and Yes if it is the destination port.

For further details on port parameters, refer to Chapter 6, “Port Parameters” in the *AT-S63 Management Software Menus Interface User's Guide*.

---

**Note**

The information for an SFP or GBIC module includes additional nonadjustable operating specifications of the module.

---

An example of the information displayed by this command is shown in Figure 14 on page 144.

**Port #11 Information:**

```

Port Description ..... Port_11
Port Type ..... 10/100/1000Base-T
Status ..... Enabled
Link State ..... Up
Configured Speed/Duplex ..... Auto
Configured MDI Crossover ..... N/A
Actual Speed/Duplex ..... 100 Mbps/Full Duplex
Actual MDI Crossover ..... MDIX
Flow Control Status ..... Disabled
Flow Control Threshold ..... 7935 cells
Backpressure Status ..... Disabled
Backpressure Threshold ..... 7935 cells
HOL Blocking Prevention Threshold .... 682 cells
Broadcast Ingress Filtering ..... Disabled
Broadcast Egress Filtering ..... Disabled
Unknown Multicast Ingress Filtering .. Disabled
Unknown Multicast Egress Filtering ... Disabled
Unknown Unicast Ingress Filtering .... Disabled
Unknown Unicast Egress Filtering ..... Disabled
Broadcast Rate Limiting Status ..... Disabled
Broadcast Rate ..... 262143 packet/second
Multicast Rate Limiting Status ..... Disabled
Multicast Rate ..... 262143 packet/second
Unknown Unicast Rate Limiting Status . Disabled
Unknown Unicast Rate ..... 262143 packet/second
PVID ..... 1
Port Priority (0-7) 0=Low 7=High..... 0
Override Priority ..... No
Mirroring State..... Disabled

```

Figure 14. SHOW SWITCH PORT Command

**Examples**

The following command displays the current settings for all of the ports in the stack:

```
show switch port
```

The following command displays the current settings for port 3.14:

```
show switch port=3.14
```



## Chapter 8

# Port Statistics Commands

---

This chapter contains the following commands:

- ❑ “RESET SWITCH PORT COUNTER” on page 146
- ❑ “SHOW SWITCH MODULE COUNTER” on page 147
- ❑ “SHOW SWITCH PORT COUNTER” on page 150

## RESET SWITCH PORT COUNTER

---

### Syntax

```
reset switch port=port counter
```

### Parameter

**port** Specifies the port whose statistics counters are to be returned to zero. You can specify more than one port at a time. Port numbers are specified in the following format:

`module ID.port number`

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command returns a port’s statistics counters to zero.

### Example

The following command returns to zero the counters on ports 1.14 to 1.22 and ports 2.1 to 2.5:

```
reset switch port=1.14-1.22,2.1-2.5 counter
```

## SHOW SWITCH MODULE COUNTER

### Syntax

```
show switch module=id counter
```

### Parameters

**id** Specifies the ID number of a switch in the stack. You can specify only one switch at a time. To view the ID numbers of the switches, refer to “SHOW STACK” on page 72.

### Description

This command displays the operating statistics, such as the number of ingress and egress packets, of a switch in a stack. An example is shown in Figure 15.

Module: 2 Port: All

Bytes Rx .....	983409801	Bytes Tx .....	965734443
Frames Rx .....	815423	Frames Tx .....	691396
Bcast Frames Rx...	107774	Bcast Frames Tx ..	1853
Mcast Frames Rx ..	11429	Mcast Frames Tx ..	0
Frames 64 .....	110509	Frames 65-127 ....	15192
Frames 128-255 ...	1928	Frames 256-511 ...	442
Frames 512-1023 ..	157796	Frames 1024-1518..	1221024
CRC Error .....	0	Jabber .....	0
No. of Rx Errors .	0	No. of Tx Errors .	0
UnderSize Frames .	0	OverSize Frames ..	0
Fragments .....	0	Collision .....	0
Frames 1519-1522 .	0	Dropped Frames ...	0

Figure 15. SHOW SWITCH COUNTER Command

The command provides the following information:

#### Bytes Rx

Number of bytes received by the switch.

#### Bytes Tx

Number of bytes transmitted by the switch.

#### Frames Rx

Number of frames received by the switch.

#### Frames Tx

Number of frames transmitted by the switch.

Bcast Frames Rx

Number of broadcast frames received by the switch.

Bcast Frames Tx

Number of broadcast frames transmitted by the switch.

Mcast Frames Rx

Number of multicast frames received by the switch.

Mcast Frames Tx

Number of multicast frames transmitted by the switch.

Frames 64

Frames 65-127

Frames 128-255

Frames 256-511

Frames 512-1023

Frames 1024-1518

Frames 1519-1522

Number of frames transmitted from the port, grouped by size.

CRC Error

Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received by the switch.

Jabber

Number of occurrences of corrupted data or useless signals appearing on the switch.

No. of Rx Errors

Number of receive errors.

No. of Tx Errors

Number of transmit errors.

Undersize Frames

Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received by the switch.

Oversize Frames

Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received by the switch.

Fragments

Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received by the switch.

Collision

Number of collisions that have occurred on the switch.

**Dropped Frames**

Number of frames successfully received and buffered by the switch, but discarded and not forwarded.

**Example**

The following command displays the operating statistics for a switch assigned module ID 4:

```
show switch module=4 counter
```

## SHOW SWITCH PORT COUNTER

---

### Syntax

```
show switch port[=port] counter
```

### Parameter

port

Specifies the port whose statistics you want to view. You can specify more than one port at a time. To view all ports, do not specify a port. Port numbers are entered in the following format:

module ID.port number

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command displays the operating statistics for a port on the switch. Examples of the statistics include the number of packets transmitted and received, and the number of CRC errors. For an example of the display and definitions of the statistics, refer to “SHOW SWITCH MODULE COUNTER” on page 147.

### Examples

The following command displays the operating statistics for port 4.14:

```
show switch port=4.14 counter
```

The following command displays the operating statistics for all ports in the stack:

```
show switch port counter
```

## Chapter 9

# MAC Address Table Commands

---

This chapter contains the following commands:

- ❑ “ADD SWITCH FDB|FILTER” on page 152
- ❑ “DELETE SWITCH FDB|FILTER” on page 154
- ❑ “RESET SWITCH FDB” on page 156
- ❑ “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 157
- ❑ “SHOW SWITCH AGINGTIMER|AGEINGTIMER” on page 158
- ❑ “SHOW SWITCH FDB” on page 159

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

# ADD SWITCH FDB|FILTER

---

## Syntax

```
add switch fdb|filter destaddress|macaddress=macaddress
port=port vlan=name|vid
```

---

**Note**  
The FDB and FILTER keywords are equivalent.

---

## Parameters

destaddress <i>or</i> macaddress	Specifies the static unicast or multicast address to be added to the stack’s MAC address table. The parameters are equivalent. The address can be entered in either of the following formats:  xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx
port	Specifies the port(s) for the MAC address. You can specify only one port when adding a unicast address, and more than one port when adding a multicast address. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
vlan	Specifies the name or VID of the VLAN where the node designated by the MAC address is a member.

## Description

This command adds static unicast and multicast MAC addresses to the stack’s MAC address table. A MAC address added with this command is never timed out from the MAC address table, even when the end node or, in the case of a multicast address, the multicast application is inactive.

If you are entering a static multicast address, the address must be assigned to the port when the multicast application is located and to the ports where the host nodes are connected. Assigning the address to only the port where the multicast application is located will result in the failure of the multicast packets to be properly forwarded to the host nodes.



## Examples

This command adds the static MAC address 00:A0:D2:18:1A:11 to port 1.7 in the Default\_VLAN:

```
add switch fdb macaddress=00A0D2181A11 port=1.7  
vlan=default_vlan
```

This command adds the multicast MAC address 01:00:51:00:00 10 to ports 2.1 to 2.5 in the Engineering VLAN:

```
add switch fdb macaddress=010051000010 port=2.1-2.5  
vlan=Engineering
```

# DELETE SWITCH FDB|FILTER

---

## Syntax

```
delete switch fdb|filter
macaddress|destaddress=macaddress vlan=name|vid
type|status=static|staticunicast|staticmulticast|dynamic|
dynamicunicast|dynamicmulticast
```

---

**Note**  
The FDB and FILTER keywords are equivalent.

---

## Parameters

macaddress <b>or</b> destaddress	Deletes a dynamic or static unicast or multicast MAC address from the MAC address table. The address can be entered in either of the following formats:  xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx  This parameter must be accompanied with the VLAN parameter.	
vlan	Specifies the VLAN containing the port(s) where the address was learned or assigned. The VLAN can be specified by name or VID. This parameter must be used with the MACADDRESS and DESTADDRESS parameters.	
type <b>or</b> status	Deletes specific types of MAC addresses. Options are:	
	static	Deletes all static unicast and multicast MAC addresses.
	staticunicast	Deletes all static unicast addresses.
	staticmulticast	Deletes all static multicast addresses.
	dynamic	Deletes all dynamic unicast and multicast MAC addresses.
	dynamicunicast	Deletes all dynamic unicast addresses.
	dynamicmulticast	Deletes all dynamic multicast addresses.

## Description

This command deletes dynamic and static unicast and multicast addresses from the stack's MAC address table.

---

### Note

You cannot delete a stack's MAC address, an STP BPDU MAC address, or a broadcast address.

---

## Examples

The following command deletes the static MAC address 00:A0:D2:18:1A:11 from the table. The port where the address was learned or assigned is part of the Default\_VLAN, which has a VID of 1:

```
delete switch fdb macaddress=00A0D2181A11 vlan=1
```

The following command deletes the MAC address 00:A0:C1:11:22:44 from the table. The port where the address was learned or assigned is part of the Sales VLAN:

```
delete switch fdb macaddress=00a0c1112244 vlan=sales
```

The following command deletes all dynamic MAC addresses learned on the ports of the Default\_VLAN:

```
delete switch fdb macaddress=dynamic vlan=default_vlan
```

The following command deletes all dynamic MAC addresses:

```
delete switch fdb type=dynamic
```

The following command deletes all static unicast MAC addresses:

```
delete switch fdb type=staticunicast
```

## RESET SWITCH FDB

---

### Syntax

```
reset switch fdb [port=port]
```

### Parameter

**port** Specifies the port whose dynamic MAC addresses are to be deleted from the MAC address table. You can specify more than one port at a time. Port numbers must be specified in the following format:

`module ID.port number`

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command deletes all of the dynamic MAC addresses learned by the entire stack or on a specific port. After a port’s dynamic MAC addresses have been deleted, the port begins to learn new addresses.

### Examples

The following command deletes all of the dynamic MAC addresses in the stack’s MAC address table:

```
reset switch fdb
```

The following command deletes all of the dynamic MAC addresses learned on port 2.5:

```
reset switch fdb port=2.5
```

## SET SWITCH AGINGTIMER|AGEINGTIMER

---

### Syntax

```
set switch agingtimer|ageingtimer=value
```

### Parameter

agingtimer <b>or</b> ageingtimer	Specifies the aging timer for the MAC address table. The value is in seconds. The range is 0 to 1048575. The default is 300 seconds (5 minutes). The parameters are equivalent.
-------------------------------------	---

### Description

The stack uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table in the master switch. When the stack detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, it deletes the address from the table. This prevents the table from becoming full of addresses of nodes that are no longer active.

Setting the aging timer to 0 disables the timer. No dynamic MAC addresses are aged out and the table stops learning new addresses after reaching its maximum capacity.

To view the current setting for the MAC address aging timer, refer to “SHOW SWITCH AGINGTIMER|AGEINGTIMER” on page 158.

### Example

The following command sets the aging timer to 120 seconds (2 minutes):

```
set switch agingtimer=120
```

## SHOW SWITCH AGINGTIMER|AGEINGTIMER

---

### Syntax

```
show switch agingtimer|ageingtimer
```

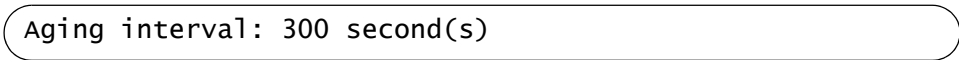
### Parameters

None.

### Description

This command displays the current setting for the aging timer. The stack uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. To set the aging timer, refer to “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 157.

Figure 16 illustrates the information displayed by this command.



```
Aging interval: 300 second(s)
```

Figure 16. SHOW SWITCH AGINGTIMER|AGEINGTIMER Command

### Example

The following command displays the current setting for the MAC address aging timer:

```
show switch agingtimer
```

## SHOW SWITCH FDB

---

### Syntax

```
show switch fdb [macaddress|destaddress=macaddress]  
[port=port] [type|status=static|staticunicast|  
staticmulticast|dynamic|dynamicunicast|dynamicmulticast]  
[vlan=name]
```

### Parameters

address	Specifies a MAC address. Use this parameter to determine the port on the stack where a particular MAC address was learned (dynamic) or assigned (static). The address can be entered in either of the following formats:  xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx	
port	Specifies a port on the stack. Use this parameter to view all addresses learned on a particular port. You can specify more than one port. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.	
type <i>or</i> status	Displays specific types of MAC addresses. Options are:	
	static	Displays all static unicast and multicast MAC addresses.
	staticunicast	Displays all static unicast addresses.
	staticmulticast	Displays all static multicast addresses.
	dynamic	Displays all dynamic unicast and multicast MAC addresses.
	dynamicunicast	Displays all dynamic unicast addresses.
	dynamicmulticast	Displays all dynamic multicast addresses.
vlan	Specifies a VLAN name. Use this parameter to view the MAC addresses learned or assigned to the ports of a particular VLAN on the stack.	

**Note**

You can specify more than one parameter at a time with this command.

**Description**

This command displays the unicast and multicast MAC addresses learned or assigned to the ports on the stack and stored in the stack's MAC address table. Figure 17 is an example.

Switch Forwarding Database			
Total Number of MAC Addresses: 121			
VLAN ID	MAC Address	Port	Status
0	01:80:c1:00:02:01	1.0	Static (fixed, non-aging)
1	00:a0:d2:18:1a:c8	1.1	Dynamic
1	00:a0:c4:16:3b:80	1.2	Dynamic
1	00:a0:12:c2:10:c6	1.3	Dynamic
1	00:a0:c2:09:10:d8	1.4	Dynamic
1	00:a0:33:43:a1:87	1.4	Dynamic
1	00:a0:12:a7:14:68	1.4	Dynamic
1	00:a0:d2:22:15:10	1.4	Dynamic
1	00:a0:d4:18:a6:89	1.4	Dynamic

Figure 17. SHOW SWITCH FDB Command - Unicast Addresses

**Note**

The first address in the unicast MAC address table is the address of the master switch of the stack.

The columns are defined here:

- ❑ VLAN ID - The ID number of the VLAN where the port is an untagged member.
- ❑ MAC - The dynamic or static unicast MAC address learned on or assigned to the port.
- ❑ Port - The port where the address was learned or assigned. The MAC address of port 1.0 is the switch's address.
- ❑ Status - The type of address: static or dynamic.



Figure 18 is an example of a multicast address.

```

Multicast Switch Forwarding Database
Total Number of MCAST MAC Addresses: 1
MAC Address          VLANID  Type      Port Maps (U:Untagged T:Tagged)
-----
01:00:51:00:00:01   1        Static    U:2.1-2.4
                                   T:

```

Figure 18. SHOW SWITCH FDB Command - Multicast Addresses

The columns are defined here:

- ❑ MAC Address - The static or dynamic unicast MAC address.
- ❑ VLAN ID - The ID number of the VLAN where the port is an untagged member.
- ❑ Type - The type of the address: static or dynamic.
- ❑ Port Maps - The tagged and untagged port members of the multicast group.

### Examples

The following command displays all the static and dynamic unicast MAC addresses in the switch's MAC address table:

```
show switch fdb
```

The following command displays just the static unicast MAC addresses:

```
show switch fdb type=static
```

The following command displays the static and dynamic multicast addresses:

```
show switch fdb type=multicast
```

The following command displays just the static multicast addresses:

```
show switch fdb type=staticmulticast
```

The following command displays the port where the MAC address 00:A0:D2:18:1A:11 was learned (dynamic) or added (static):

```
show switch fdb address=00A0D2181A11
```

The following command displays the MAC addresses learned on port 3.2:

```
show switch fdb port=3.2
```

The following command displays the MAC addresses learned on the ports in the Sales VLAN:

```
show switch fdb vlan=sales
```

The following command displays the static MAC addresses on port 2.17:

```
show switch fdb port=2.17 type=static
```

## Chapter 10

# Static Port Trunking Commands

---

This chapter contains the following commands:

- ❑ “Overview” on page 164
- ❑ “ADD SWITCH TRUNK” on page 166
- ❑ “CREATE SWITCH TRUNK” on page 168
- ❑ “DELETE SWITCH TRUNK” on page 170
- ❑ “DESTROY SWITCH TRUNK” on page 171
- ❑ “SET SWITCH TRUNK” on page 172
- ❑ “SHOW SWITCH TRUNK” on page 173

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

## Overview

---

A static port trunk is a group of two to eight ports that function as a single virtual link between the stack and another network device. A static port trunk distributes the traffic across its ports to improve performance and enhance reliability by reducing the reliance on a single physical link.

A static port trunk is easy to configure. You simply designate the ports of the trunk and the management software automatically groups them together. You can also control how traffic is distributed over the trunk ports by specifying the load distribution method. For an explanation of the load distribution methods, refer to the *AT-S63 Management Software Features Guide*.

Here are the guidelines to creating static port trunks on a stack:

- ❑ Since static port trunks are often implemented differently by network equipment vendors, Allied Telesis recommends using this feature only between Allied Telesis networking devices to ensure compatibility.
- ❑ A static trunk can contain up to eight ports.
- ❑ A stack can support up to six static port trunks.
- ❑ The ports of a static trunk must be of the same medium type. They can be all twisted pair ports or all fiber optic ports.
- ❑ The ports of a trunk can be either consecutive (for example, 1.5 to 1.8) or nonconsecutive (for example, 2.4, 2.8, 3.11, 4.20).
- ❑ The ports of a trunk can be located on different switches in a stack.
- ❑ Before creating a port trunk, examine the speed, duplex mode, flow control, and back pressure settings of the lowest number port to be in the trunk. Verify that its settings are correct for the device to which the trunk will be connected. When you create a static port trunk, the management software copies the current settings of the lowest numbered port in the trunk to the other ports, because all ports in a static trunk must have the same settings. For example, if you create a port trunk consisting of ports 2.5 to 2.8, the parameter settings for port 2.55 are copied to ports 2.6, 2.7, and 2.8 so that all the ports of the trunk have the same settings.
- ❑ After creating a port trunk, do not change the speed, duplex mode, flow control, or back pressure of any port in the trunk without also changing the other ports.
- ❑ A port can belong to only one static trunk at a time.
- ❑ A port cannot be a member of a static trunk and an LACP trunk at the same time.
- ❑ The ports of a static trunk must be untagged members of the same VLAN. The ports cannot be untagged members of different VLANs.

- ❑ The switch selects the lowest numbered port in the trunk to handle broadcast packets and packets of unknown destination. For example, a trunk of ports 2.11 to 2.15 would use port 2.11 for broadcast packets.

## ADD SWITCH TRUNK

---

### Syntax

```
add switch trunk=name [tgid=id_number] port=port
```

### Parameters

trunk	Specifies the name of the static port trunk to be modified.
tgid	Specifies the ID number of the static port trunk to be modified. The range is 1 to 6. This parameter is optional.
port	<p>Specifies the port to be added to the port trunk. You can add more than one port at a time. Port numbers are specified in the following format:</p> <pre>module ID.port number</pre> <p>For instructions, refer to “Port Numbers in Commands” on page 42.</p>

### Description

This command adds ports to an existing static port trunk. To initially create a static port trunk, refer to “CREATE SWITCH TRUNK” on page 168.



#### Caution

Disconnect all network cables from the ports of the trunk on the stack before using this command. Adding a port to a port trunk without first disconnecting the cables may result in loops in your network topology, which can produce broadcast storms and poor network performance.

---

#### Note

If the port being added will be the lowest numbered port in the trunk, its parameter settings will overwrite the settings of the existing ports in the trunk. Consequently, you should check to see if its settings are appropriate prior to adding it to the trunk. If the port will not be the lowest numbered port, its settings are adjusted to match the settings of the existing ports in the trunk.

---

---

**Note**

A port that already belongs to a static port trunk must be removed from its current assignment before it can be added to another port trunk. To remove a port from a trunk, see “DELETE SWITCH TRUNK” on page 170.

---

**Example**

The following command adds port 1.5 to a port trunk called load22:

```
add switch trunk=load22 port=1.5
```

## CREATE SWITCH TRUNK

---

### Syntax

```
create switch trunk=name port=ports
[select=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

### Parameters

trunk	Specifies the name of the trunk. The name can be up to 16 alphanumeric characters. No spaces or special characters are allowed.												
port	Specifies the ports to be added to the port trunk. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.												
select	Specifies the load distribution method. Options are: <table data-bbox="711 966 1364 1390"> <tr> <td>macsrc</td><td>Source MAC address.</td></tr> <tr> <td>macdest</td><td>Destination MAC address.</td></tr> <tr> <td>macboth</td><td>Source address/destination MAC address.</td></tr> <tr> <td>ipsrc</td><td>Source IP address.</td></tr> <tr> <td>ipdest</td><td>Destination IP address.</td></tr> <tr> <td>ipboth</td><td>Source address/destination IP address.</td></tr> </table>	macsrc	Source MAC address.	macdest	Destination MAC address.	macboth	Source address/destination MAC address.	ipsrc	Source IP address.	ipdest	Destination IP address.	ipboth	Source address/destination IP address.
macsrc	Source MAC address.												
macdest	Destination MAC address.												
macboth	Source address/destination MAC address.												
ipsrc	Source IP address.												
ipdest	Destination IP address.												
ipboth	Source address/destination IP address.												

### Description

This command creates a static port trunk. To create the trunk, you specify the stack ports and the load distribution method. For an explanation of the load distribution methods, refer to the *AT-S63 Management Software Features Guide*.



**Caution**

Do not connect the cables to the trunk ports on the devices until after you have created the trunk in the management software. Connecting the cables before configuring the software will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

**Note**

Before creating a static port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port to be in the trunk. Check to be sure that the settings are correct for the end node to which the trunk will be connected. When you create the trunk, the AT-S63 Management Software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

You should also check to be sure that the ports are untagged members of the same VLAN. You cannot create a trunk of ports that are untagged members of different VLANs.

**Note**

A port that already belongs to a static port trunk must be removed from its current assignment before it can be added to another port trunk. To remove ports from a static trunk, see “DELETE SWITCH TRUNK” on page 170.

**Examples**

The following command creates a static port trunk using ports 2.3 to 2.6. The command names the trunk “load22” and sets the load distribution method to destination MAC address.

```
create switch trunk=load22 port=2.3-2.6 select=macdest
```

The following command creates a port trunk consisting of ports 1.15, 4.17, and 4.22. The trunk is named “trunk4”. No load distribution method is specified, so the default setting, source and destination MAC addresses, is used:

```
create switch trunk=trunk4 port=1.15,4.17,4.22
```

## DELETE SWITCH TRUNK

---

### Syntax

```
delete switch trunk=name port=port
```

### Parameters

trunk	Specifies the name of the static port trunk to be modified.
port	Specifies the port to be removed from the existing port trunk. You can specify more than one port at a time. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command removes ports from a static port trunk. To completely remove a port trunk from a stack, see “DESTROY SWITCH TRUNK” on page 171.



#### Caution

Disconnect all data cables from the ports of the trunk on the stack before using this command. Removing a port from a port trunk without first disconnecting the cables may result in loops in your network topology, which can produce broadcast storms and poor network performance.

---

#### Note

You cannot remove ports from a trunk that has only two ports because a static trunk must have a minimum of two ports.

---

### Example

The following command removes port 4.11 from a port trunk called Dev\_trunk:

```
delete switch trunk=Dev_trunk port=4.11
```

## DESTROY SWITCH TRUNK

---

### Syntax

```
destroy switch trunk=name
```

### Parameter

trunk                      Specifies the name of the trunk to be deleted.

### Description

This command deletes a static port trunk from a stack. After a port trunk has been deleted, the ports that made up the trunk can be connected to different end nodes.



### Caution

Disconnect the cables from the port trunk on the stack before destroying the trunk. Deleting a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

---

### Example

The following command deletes the trunk called load22 from the stack:

```
destroy switch trunk=load22
```

## SET SWITCH TRUNK

---

### Syntax

```
set switch trunk=name  
select=macsrc|macdest|macboth|ipsrc|ipdest|ipboth
```

### Parameters

trunk	Specifies the name of the static port trunk.												
select	Specifies the load distribution method. Options are: <table><tr><td>macsrc</td><td>Source MAC address.</td></tr><tr><td>macdest</td><td>Destination MAC address.</td></tr><tr><td>macboth</td><td>Source address/destination MAC address.</td></tr><tr><td>ipsrc</td><td>Source IP address.</td></tr><tr><td>ipdest</td><td>Destination IP address.</td></tr><tr><td>ipboth</td><td>Source address/destination IP address.</td></tr></table>	macsrc	Source MAC address.	macdest	Destination MAC address.	macboth	Source address/destination MAC address.	ipsrc	Source IP address.	ipdest	Destination IP address.	ipboth	Source address/destination IP address.
macsrc	Source MAC address.												
macdest	Destination MAC address.												
macboth	Source address/destination MAC address.												
ipsrc	Source IP address.												
ipdest	Destination IP address.												
ipboth	Source address/destination IP address.												

### Description

This command changes the load distribution method of an existing static port trunk. For an explanation of the load distribution methods, refer to the *AT-S63 Management Software Features Guide*.

### Example

The following command changes the load distribution method of a trunk named "Load11" to source MAC address:

```
set switch trunk=Load11 select=macsrc
```

## SHOW SWITCH TRUNK

---

### Syntax

```
show switch trunk
```

### Parameters

None.

### Description

This command displays the names, ports, and load distribution methods of the static port trunks on the stack. An example of the command is shown in Figure 19.

```
Trunk group ID ..... 2
Trunk status ..... UP
Trunk group name ..... Server11
Trunk method ..... SRC/DST MAC
Ports ..... 2.12-2.16
```

Figure 19. SHOW SWITCH TRUNK Command

The command displays the following information:

- ❑ Trunk group ID - The ID number of the static port trunk.
- ❑ Trunk status - The operational status of the trunk. If the trunk has established a link with the other device, status will be UP. If the trunk has not establish a link or the ports in the trunk are disabled, status will be DOWN.
- ❑ Trunk group name - The name of the static port trunk.
- ❑ Trunk method - One of the following load distribution methods:
 

SRC MAC	Source MAC address.
DST MAC	Destination MAC address.
SRC/DST MAC	Source address/destination MAC address.
SRC IP	Source IP address.
DST IP	Destination IP address.
SRC/DST IP	Source address/destination IP address.
- ❑ Ports - The ports of the static port trunk.

### **Example**

The following command displays port trunking information:

```
show switch trunk
```

## Chapter 11

# LACP Port Trunking Commands

---

This chapter contains the following commands:

- ❑ “ADD LACP PORT” on page 176
- ❑ “CREATE LACP AGGREGATOR” on page 178
- ❑ “DELETE LACP PORT” on page 180
- ❑ “DESTROY LACP AGGREGATOR” on page 181
- ❑ “DISABLE LACP” on page 182
- ❑ “ENABLE LACP” on page 183
- ❑ “SET LACP AGGREGATOR” on page 184
- ❑ “SET LACP SYSPRIORITY” on page 186
- ❑ “SET LACP STATE” on page 187
- ❑ “SHOW LACP” on page 188

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

**Note**

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## ADD LACP PORT

---

### Syntax

```
add lacp aggregator=name port=port
```

### Parameters

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
port	Specifies the port(s) to be added to the aggregator. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command adds ports to an existing aggregator. You must identify the aggregator by its name. To display the names of the aggregators on the switch, refer to “SHOW LACP” on page 188. To create an aggregator, refer to “CREATE LACP AGGREGATOR” on page 178.

Review the following before adding a port to an aggregator:

- ❑ Verify that the port’s speed is set to Auto-Negotiation or 100 Mbps, full-duplex. Aggregate trunks do not support half-duplex mode.
- ❑ The ports of an aggregator must be untagged ports of the same VLAN.
- ❑ You cannot add a port to an aggregator that is below the lowest numbered port in the aggregator, also referred to as the base port. For example, if an aggregator consists of ports 7 to 12, you cannot add ports 1 to 6. To change the base port of an aggregator, you must delete and recreate the aggregator.



### Caution

A network cable should not be connected to a port on the switch until after the port is added to the aggregator. Connecting the cable before the port is a part of an aggregator could result in loops in your network topology, which can cause broadcast storms and poor network performance.

---



## Examples

The following command adds ports 1.8 and 2.22 to an aggregator named “agg\_1”:

```
add lacp aggregator=agg_1 port=1.8,2.22
```

## CREATE LACP AGGREGATOR

---

### Syntax

```
create lacp aggregator=name|adminkey=0xkey port=port
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

### Parameters

aggregator	Specifies a name for the new aggregator. The name can be up to 20 alphanumeric characters. No spaces or special characters are allowed. If no name is specified, the default name is DEFAULT_AGG followed by a number.												
adminkey	Specifies an adminkey number for the aggregator. This is a hexadecimal number in the range of 0x1 to 0xffff. If this parameter is omitted, the default adminkey of the lowest numbered port in the aggregator is used.												
port	Specifies the ports of the aggregator. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.												
distribution	Specifies the load distribution method, which can be one of the following: <table data-bbox="711 1249 1421 1648"> <tr> <td>macsrc</td><td>Source MAC address.</td></tr> <tr> <td>macdest</td><td>Destination MAC address.</td></tr> <tr> <td>macboth</td><td>Source and destination MAC addresses. This is the default.</td></tr> <tr> <td>ipsrc</td><td>Source IP address.</td></tr> <tr> <td>ipdest</td><td>Destination IP address.</td></tr> <tr> <td>ipboth</td><td>Source and destination IP addresses.</td></tr> </table> <p>If this parameter is omitted, the source and destination MAC addresses load distributed method is selected by default.</p>	macsrc	Source MAC address.	macdest	Destination MAC address.	macboth	Source and destination MAC addresses. This is the default.	ipsrc	Source IP address.	ipdest	Destination IP address.	ipboth	Source and destination IP addresses.
macsrc	Source MAC address.												
macdest	Destination MAC address.												
macboth	Source and destination MAC addresses. This is the default.												
ipsrc	Source IP address.												
ipdest	Destination IP address.												
ipboth	Source and destination IP addresses.												

## Description

This command creates an LACP aggregator. Note the following when creating a new aggregator:

- ❑ You can specify either a name or an adminkey but not both when creating a new aggregator.
- ❑ When you create a new aggregator by specifying a name, the adminkey is based on the operator key of the lowest numbered port in the aggregator.
- ❑ When you create an aggregator by specifying an adminkey, the aggregator's default name is DEFAULT\_AGG followed by the port number of the lowest numbered port in the aggregator. For instance, an aggregator of ports 1.12 to 1.16 would be given the name DEFAULT\_AGG12.
- ❑ Before creating an aggregator, you should verify that the ports that will be members of the aggregator are set to Auto-Negotiation or 100 Mbps, full-duplex. Aggregate trunks do not support half-duplex mode.
- ❑ All ports in an aggregator must be untagged ports of the same VLAN.
- ❑ You cannot change the name or adminkey of an existing aggregator. That function requires deleting the aggregator and recreating it.



### Caution

Do not connect the cables to the ports of the aggregator on the switch until after you have configured LACP and the aggregators on both devices that will be interconnected by the trunk. Connecting the cables before configuring the aggregators and activating the protocol will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

---

## Examples

The following command creates an LACP aggregator named "sw\_agg\_1" of ports 1.1 through 1.4. The load distribution method is source MAC address. Since the aggregator is being created by name, the default operator key for port 1, the lowest numbered port in the aggregator, becomes the adminkey:

```
create lacp aggregator=sw_agg_1 port=1.1-1.4
distribution=macsrc
```

The following command creates an LACP aggregator of ports 1.10, 2.12, 2.15 to 2.18 with an adminkey number of 0x7A. The default name for the aggregator is DEFAULT\_AGG10 because the command specifies an adminkey and because port 10 is the lowest numbered port in the aggregator. Since no load distribution method is specified, the source and destination MAC addresses load distributed method is used by default:

```
create lacp adminkey=0x7A port=1.10,2.12,2.15-2.18
```

## DELETE LACP PORT

---

### Syntax

```
delete lacp aggregator=name port=port
```

### Parameters

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
port	Specifies the port(s) to be removed from the aggregator. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command removes a port from an aggregator. You must identify the aggregator by its name. To display the names of the aggregators on the switch, refer to “SHOW LACP” on page 188. To completely remove an aggregator, see “DESTROY LACP AGGREGATOR” on page 181.



#### Caution

Disconnect the network cable from a port before removing the port from an aggregator. Removing a port without first disconnecting the cable might form loops in your network topology, which can cause broadcast storms and poor network performance.

---

#### Note

You cannot delete the lowest numbered port from an aggregator, also referred to as the base port. For example, if an aggregator consists of ports 7 to 12, you cannot delete port 7. You must delete and recreate an aggregator to remove the base port.

---

### Example

This command removes port 2.9 from the “lacp\_server” aggregator:

```
delete lacp aggregator=lacp_server port=2.9
```

## DESTROY LACP AGGREGATOR

---

### Syntax

```
destroy lacp aggregator=name|adminkey=0xkey
```

### Parameter

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
adminkey	Specifies the adminkey number of the aggregator. This is a hexadecimal number between 0x1 and 0xffff.

### Description

This command deletes an LACP aggregator from the switch. You can identify the aggregator by its name or adminkey number. To display the names and adminkeys of the aggregators on the switch, refer to “SHOW LACP” on page 188.



### Caution

Disconnect the network cables from the ports of the aggregator before performing this command. Deleting the aggregator without first disconnecting the cables can result in loops in your network topology, which can result in broadcast storms and poor network performance.

---

### Example

The following command deletes an aggregator named “agg\_15”:

```
destroy lacp aggregator=agg_15
```

The following command deletes an aggregator with an adminkey number of 0x1A:

```
destroy lacp adminkey=0x1a
```

## DISABLE LACP

---

### Syntax

```
disable lacp
```

### Parameters

None.

### Description

This command disables LACP on the switch. The default is disabled.



### Caution

Do not disable LACP if there are defined aggregators without first disconnecting all cables connected to the aggregate trunk ports. Otherwise, a network loop may occur, resulting in a broadcast storm and poor network performance.

---

### Example

The following command disables LACP on the switch:

```
disable lacp
```

### Equivalent Command

```
set lacp state=disable
```

For information, see “SET LACP STATE” on page 187.

## ENABLE LACP

---

### Syntax

```
enable lacp
```

### Parameters

None.

### Description

This command activates LACP on the switch. The default is disabled.

### Example

The following command activates LACP:

```
enable lacp
```

### Equivalent Command

```
set lacp state=enable
```

For information, see “SET LACP STATE” on page 187.

## SET LACP AGGREGATOR

---

### Syntax

```
set lacp aggregator=name|adminkey=key
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

### Parameters

aggregator	Specifies the name of the aggregator you want to modify. The name is case-sensitive.												
adminkey	Specifies the adminkey number of the aggregator you want to modify. This is a hexadecimal number between 0x1 and 0xffff.												
distribution	Specifies one of the following load distribution methods: <table data-bbox="711 829 1360 1247"> <tr> <td>macsrc</td><td>Source MAC address.</td></tr> <tr> <td>macdest</td><td>Destination MAC address.</td></tr> <tr> <td>macboth</td><td>Source address/destination MAC address. This is the default.</td></tr> <tr> <td>ipsrc</td><td>Source IP address.</td></tr> <tr> <td>ipdest</td><td>Destination IP address.</td></tr> <tr> <td>ipboth</td><td>Source address/destination IP address.</td></tr> </table>	macsrc	Source MAC address.	macdest	Destination MAC address.	macboth	Source address/destination MAC address. This is the default.	ipsrc	Source IP address.	ipdest	Destination IP address.	ipboth	Source address/destination IP address.
macsrc	Source MAC address.												
macdest	Destination MAC address.												
macboth	Source address/destination MAC address. This is the default.												
ipsrc	Source IP address.												
ipdest	Destination IP address.												
ipboth	Source address/destination IP address.												

### Description

This command modifies the load distribution method of an existing LACP aggregator. You can identify the aggregator by its name or adminkey. To display the names and adminkeys of the aggregators on the switch, refer to “SHOW LACP” on page 188.

---

#### Note

You cannot change the name or adminkey of an existing aggregator.

---

### Examples

The following command changes the load distribution method of an LACP aggregator titled “agg\_5” to the source MAC address method:

```
set lacp aggregator=agg_5 distribution=macsrc
```



The following command changes the load distribution method of an LACP aggregator with the adminkey 0x22 to the destination MAC address method:

```
set lacp adminkey=0x22 distribution=macdest
```

## SET LACP SYSPRIORITY

---

### Syntax

```
set lacp syspriority=0xpriority
```

### Parameters

syspriority	Specifies the LACP system priority value for a switch. This is a hexadecimal value from 0x1 to 0xffff. The lower the number, the higher the priority. The default is 0x0080.
-------------	--

### Description

This command sets the LACP priority of the switch. LACP uses the priority to resolve conflicts between two switches to decide which switch makes the decision about which ports to aggregate.

### Example

The following command sets the LACP priority on the switch to 0x8000:

```
set lacp syspriority=0x8000
```

## SET LACP STATE

---

### Syntax

```
set lacp state=enable|disable
```

### Parameters

state            Specifies the state of LACP on the switch. The options are:

enable	Enables LACP.
disable	Disables LACP. This is the default.

### Description

This command enables or disables LACP on the switch.



#### Caution

Do not disable LACP if there are defined aggregators without first disconnecting all cables connected to the aggregate trunk ports. Otherwise, a network loop might occur, resulting in a broadcast storm and poor network performance.

---

### Example

The following command activates LACP on the system:

```
set lacp state=enable
```

### Equivalent Commands

```
disable lacp
```

For information, see “DISABLE LACP” on page 182.

```
enable lacp
```

For information, see “ENABLE LACP” on page 183.

# SHOW LACP

---

**Syntax**

show lacp [port=*port*] [aggregator] [machine=*port*]

**Parameter**

port	Specifies the port(s) to display. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
aggregator	Displays information about the aggregators.
machine	Specifies the LACP machine state for a port or ports on the system.

**Description**

This command displays the configuration and/or machine states of the ports, and/or the aggregators. Entering the command without any parameters displays general LACP status information. Figure 20 illustrates the information displayed by this command.

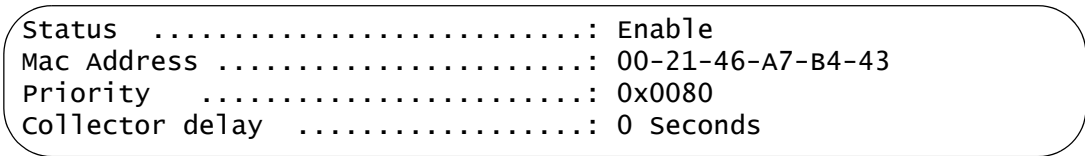


Figure 20. SHOW LACP Command

The command displayed the following information:

- ❑ Status - Whether the LACP protocol is enabled or disabled on the switch.
- ❑ MAC Address - The MAC address of the switch.
- ❑ Priority - The LACP system priority value assigned to the switch.

The PORT parameter displays LACP port information. Figure 21 illustrates the information displayed by this parameter. For definitions, refer to the IEEE 802.3ad standard.

```

Port ..... 05
Aggregator ..... LACP sw22
ACTOR
=====
Actor Port ..... 05
Selected ..... SELECTED
Oper Key ..... 0xf705
Oper Port Priority .... 0x0005
Individual ..... NO
Synchronized..... YES
Collecting ..... YES
Distributing ..... YES
Defaulted ..... NO
Expired ..... NO
Actor Churn ..... YES
PARTNER
=====
Partner Port ..... 00
Partner System ..... 00-30-84-AB-EF-CD
Oper Key ..... 0xff07
Oper Port Priority ... 0x0007
Individual ..... NO
Synchronized..... YES
Collecting ..... YES
Distributing ..... YES
Defaulted ..... NO
Expired ..... NO
Partner Churn ..... YES

```

Figure 21. SHOW LACP Command with the PORT Parameter

The AGGREGATOR parameter displays information about each existing aggregator. Figure 22 illustrates the information displayed by this parameter.

```

Aggregator # 1 ..... DEFAULT_AGG5
Admin Key ..... 0x0001
Oper Key ..... 0x0045
Speed ..... 1000 Mbps
Distribution Mode .. MACBoth
Ports configured ... 2.5-2.8
Ports in LAGID..... 2.5-2.8
Aggregated Port .... 2.5-2.8

```

Figure 22. SHOW LACP Command with the AGGREGATOR Parameter

## Examples

The following command displays general LACP status information:

```
show lacp
```

The following command displays the LACP configuration for ports 1.13 and 2.16:

```
show lacp port=1.13,2.16
```

The following command displays the configuration of the aggregators on the system:

```
show lacp aggregator
```

The following command displays the LACP machine states for each port on the system:

```
show lacp machine
```

## Chapter 12

# Port Mirroring Commands

---

This chapter contains the following commands:

- ❑ “Overview” on page 192
- ❑ “SET SWITCH MIRROR” on page 193
- ❑ “SET SWITCH PORT MIRROR” on page 194
- ❑ “SHOW SWITCH MIRROR” on page 195

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

## Overview

---

The port mirror feature allows you to unobtrusively monitor the ingress or egress traffic on one or more ports on a stack by copying the traffic to another stack port. By connecting a network analyzer to the port where the traffic is being copied to, you can monitor the traffic on the other ports without impacting network performance or speed.

The port(s) whose traffic you want to mirror is called the *source port(s)*. The port where the traffic will be copied to is called the *destination port*.

Observe the following guidelines when creating a port mirror:

- ❑ A stack can have only one destination port.
- ❑ You can mirror more than one source port at a time. However, the destination port may have to discard packets if the source ports are very active.
- ❑ The destination and source ports can be located on different switches in the stack.
- ❑ You can mirror the ingress or egress traffic of the source ports, or both.



## SET SWITCH MIRROR

---

### Syntax

```
set switch mirror=port
```

### Parameter

**mirror** Specifies the destination port for the port mirror, where the traffic from the source ports is copied. A stack can have only one destination port. To stop port mirroring and free the destination port for use as a normal networking port, specifying "0" (zero) as the destination port. Port numbers are specified in the following format:

`module ID.port number`

For instructions, refer to "Port Numbers in Commands" on page 42.

### Description

This command enables mirroring and specifies the destination port, or stops port mirroring. To select the source ports, refer to "SET SWITCH PORT MIRROR" on page 194.

### Examples

This command activates mirroring and designates port 2.11 as the destination port:

```
set switch mirror=2.11
```

This command stops port mirroring:

```
set switch mirror=0
```

## SET SWITCH PORT MIRROR

---

### Syntax

```
set switch port=port mirror=none|rx|tx|both
```

### Parameters

port	Specifies the source port of a port mirror. You can specify more than one port. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
mirror	Specifies which traffic on the source ports is to be mirrored to the destination port. The options are:  rx            Specifies ingress mirroring.  tx            Specifies egress mirroring.  both          Specifies both ingress and egress mirroring.  none          Removes a port as a source port.

### Description

This command specifies the source ports of a port mirror. If the port mirror already has source ports, the new source ports are added to the existing ports. You can also use the command to remove source ports.

You must set the destination port before you can select the source ports. To set the destination port, refer to “SET SWITCH MIRROR” on page 193.

### Examples

This command specifies ports 1.16 and 1.17 as source ports of the port mirror. The ingress traffic on the ports is copied to the destination port:

```
set switch port=1.16-1.17 mirror=rx
```

This command removes ports 2.5, 2.7, and 5.10 as source ports of a port mirror:

```
set switch port=2.5,2.7,5.10 mirror=none
```

## SHOW SWITCH MIRROR

---

### Syntax

```
show switch mirror
```

### Parameters

None.

### Description

This command displays the source and destination ports of a port mirror on the stack. An example is shown in Figure 23.

```
Port Mirroring:
Mirroring State ..... Enabled
Mirror-To (Destination) Port ..... 1.22
Ingress (Rx) Mirror (Source) Ports .. 2.1,2.3
Egress (Tx) Mirror (Source) Ports ... 2.1,2.3,5.11-5.13
```

Figure 23. SHOW SWITCH MIRROR Command

The command provides the following information about the port mirror:

- ❑ Mirroring State - The port mirroring status, Enabled or Disabled. If port mirroring is disabled on the stack, only this line is displayed by the command.
- ❑ Mirror-To (Destination) Port - The port functioning as the destination port.
- ❑ Ingress (Rx) Mirror (Source) Port - The port(s) whose ingress (received) traffic is mirrored.
- ❑ Egress (Tx) Mirror (Source) Port - The port(s) whose egress (transmitted) traffic is mirrored.

### Example

The following command displays the status and ports of a port mirror:

```
show switch mirror
```



## Section II

# Advanced Operations

---

The chapters in this section include:

- ❑ Chapter 13, “File System Commands” on page 199
- ❑ Chapter 14, “File Download and Upload Commands” on page 215
- ❑ Chapter 15, “Event Log and Syslog Client Commands” on page 235
- ❑ Chapter 16, “Class of Service (CoS) Commands” on page 263



## Chapter 13

# File System Commands

---

This chapter contains the following commands:

- ❑ “Overview” on page 200
- ❑ “COPY” on page 201
- ❑ “CREATE CONFIG” on page 203
- ❑ “DELETE FILE” on page 204
- ❑ “FORMAT DEVICE” on page 205
- ❑ “RENAME” on page 206
- ❑ “SET CFLASH DIR” on page 208
- ❑ “SET CONFIG” on page 209
- ❑ “SHOW CFLASH” on page 211
- ❑ “SHOW CONFIG” on page 212
- ❑ “SHOW FILE” on page 213
- ❑ “SHOW FLASH” on page 214

---

### **Note**

The master switch’s file system is the only active file system in a stack. The file systems on the member switches are not accessible.

---

## Overview

---

You can use the commands in this chapter to manage the files in the file system in the master switch of the stack. For example, you might create a backup copy of a configuration file or delete obsolete files.

The file systems on the member switches of a stack are inactive and cannot be accessed with these command.

For further information about the switch's file system, refer to the *AT-S63 Management Software Features Guide*.



# COPY

---

## Syntax

```
copy [cflash:]sourcefile.ext [cflash:]destinationfile.ext
```

## Parameters

<i>sourcefile.ext</i>	Specifies the name of the source file. If the file is stored on a compact memory flash card, precede the name with "cflash:". If the filename contains spaces, enclose it in double quotes. Otherwise, the quotes are optional.
<i>destinationfile.ext</i>	Specifies the name of the destination file. To store the copy on a compact memory flash card, precede the name with "cflash:". If the filename contains spaces, enclose it in double quotes.

## Description

This command creates a copy of an existing file in the file system of the master switch. It also copies files between the master switch's file system and a compact flash memory card, for those switches that support the card.

Note the following before using this command:

- ❑ This command does not accept a directory path. When copying a file to or from a compact flash card, you must first change to the appropriate directory on the card. For instructions, refer to "SET CFLASH DIR" on page 208. The default location is the root of the flash card.
- ❑ Files with the extension UKF are encryption key pairs. These files cannot be copied, renamed, or deleted from the file system.
- ❑ The new filename must be a valid filename from 1 to 16 alphanumeric characters. The name of the copy must be unique from the other files in the file system.
- ❑ *ext* is the three-letter file extension, and can be any of the types listed in Table 3. You must give the copy the same extension as the original file.

Table 3. File Extensions and File Types

Extension	File Type
.cfg	Configuration file
.cer	Certificate file

Table 3. File Extensions and File Types

Extension	File Type
.csr	Certificate enrollment request
.key	Public encryption key
.log	Event log

### Examples

The following command creates a copy of the configuration file “admin.cfg” in the master switch’s file system and names the copy “admin2.cfg”:

```
copy admin.cfg admin2.cfg
```

The following command creates a copy of the configuration file “stack 12.cfg” in the file system and names the copy “backup.cfg”:

```
copy "stack 12.cfg" backup.cfg
```

The following command copies the configuration file “b2\_stack.cfg” from the master switch’s file system to a compact flash card:

```
copy b2_stack.cfg cflash:b2_stack.cfg
```

The following command copies the configuration file “sales stack.cfg” from a compact flash card to the master switch’s file system and renames the file “presales\_4.cfg”:

```
copy cflash:"sales stack.cfg" presales_4.cfg
```

## CREATE CONFIG

---

### Syntax

```
create config=[cflash:] filename.cfg
```

### Parameter

config	Specifies the name of a new configuration file. If the filename contains spaces, enclose it in double quotes. Otherwise, the quotes are optional. To store the configuration file on a flash memory card, precede the name with "cflash:".
--------	--

### Description

This command creates a new configuration file in the file system of the master switch. The file contains all of the commands for recreating the current configuration settings on the switches in the stack.

The CONFIG parameter specifies the name for the configuration file. The file extension must be ".cfg". If the file already exists, it is replaced. If the file does not exist it is created.

The filename can be from 1 to 16 alphanumeric characters, not including the ".cfg" extension. Spaces are allowed. Be sure to enclose the name in double quotes if you include a space in the name. Wildcards are not allowed.

This command does not change the current assignment of the active boot configuration file, which the master switch uses to configure the stack. To change the active boot configuration file, refer to "SET CONFIG" on page 209.

### Examples

This command creates the new configuration file Stack1ab.cfg in the master switch's file system:

```
create config=Switch1ab.cfg
```

This command creates a configuration file named "sales stack.cfg" and stores it on a compact flash card:

```
create config=cflash:"sales stack.cfg"
```

## DELETE FILE

---

### Syntax

```
delete file=[cflash:] filename
```

### Parameter

file	Specifies the name of the file to be deleted. A name with spaces must be enclosed in double quotes. Otherwise, the quotes are optional. If the file is stored on a compact memory flash card, precede the name with "cflash:".
------	--

### Description

This command deletes a file from the file system or from a compact flash memory card in the master switch. Note the following before using this command:

- ❑ Deleting the active configuration file on the master switch causes the stack to return to its default settings after the next reboot or power cycle, unless you select another active boot configuration file. For instructions on how to change the active boot configuration file, refer to see "SET CONFIG" on page 209.
- ❑ This command does not accept a directory path. To delete a file on a compact flash card, you must first change to the directory where the file is stored. For instructions, refer to "SET CFLASH DIR" on page 208.
- ❑ Files with a ".ukf" extension cannot be deleted with this command. These files are encryption key pairs.

To list the files in the file system, refer to "SHOW FILE" on page 213.

### Examples

This command deletes the configuration file named "a12 stack.cfg" from a compact flash card in the master switch:

```
delete file=cflash:"a12 stack.cfg"
```

## FORMAT DEVICE

---

### Syntax

```
format device=flash
```

### Parameter

**device** Specifies the device to format. The only option is “Flash” for the master switch’s file system.

### Description

This command formats the flash memory in the master switch.



#### Caution

Formatting the flash memory deletes ALL files from the file system in the master switch, including the active configuration file and encryption keys. Only the image file of the AT-S63 Management Software in the application block is retained.

---



#### Caution

This procedure causes a stack reset. Some network traffic may be lost while the stack initializes the AT-S63 Management Software and performs the discovery process.

---

### Example

The following example formats the flash memory in the master switch:

```
format device=flash
```

## RENAME

---

### Syntax

```
rename [cflash:] filename1.ext [cflash:] filename2.ext
```

### Parameters

<code>filename1.ext</code>	Specifies the name of the file to be renamed. If the name contains spaces, enclose it in double quotes. Otherwise, the quotes are optional. If the file is stored on a compact memory card, precede the name with “cflash:”.
<code>filename2.ext</code>	Specifies the new name for the file. The filename can be from 1 to 16 alphanumeric characters, not including the filename extension. Spaces are allowed. If the name contains spaces, it must be enclosed in double quotes. The filename extension must be the same as in the original filename. The new name must be unique in the file system. If the file is stored on a compact memory card, precede the name with “cflash:”.

### Description

This command renames a file in the master switch’s file system or on a compact flash memory card. The source and destination file extensions must be the same. Note the following before using this command:

- ❑ Files with the extension UKF are encryption key pairs. They cannot be copied, renamed, or deleted with these commands.
- ❑ Renaming the active boot configuration file and then resetting the stack returns the stack parameter settings to the default values, unless you save the current configuration or select another active boot configuration file. For instructions on how to change the active boot configuration file, see “SET CONFIG” on page 209.
- ❑ The command does not accept a directory path. Renaming a file in a subdirectory on a compact flash card requires first changing to the subdirectory with “SET CFLASH DIR” on page 208.
- ❑ The source and destination locations must be the same.

### Examples

The following command renames the file “Stack12.cfg” in the switch’s file

system to "Stack 44a.cfg":

```
rename stack12.cfg "stack 44a.cfg"
```

This command renames the file "sales\_stack.cfg" on a flash memory card in the master switch to "sales 5 stack.cfg":

```
rename cflash:sales_stack.cfg cflash:"sales 5 stack.cfg"
```

## SET CFLASH DIR

---

### Syntax

```
set cflash dir=directory
```

### Parameter

dir                      Specifies the directory path.

### Description

This command changes the current directory on the compact flash card in the master switch.

---

#### Note

You cannot create directories on a compact flash card with the AT-S63 Management Software.

---

### Example

The following command changes the current directory on a compact flash card to “configs”:

```
set cflash dir=configs
```

This command changes the current directory back to the root on the compact flash card:

```
set cflash dir=\
```



## SET CONFIG

---

### Syntax

```
set config=[cflash:] filename.cfg | none
```

### Parameter

config	Specifies the name of the configuration file to act as the active configuration file on the stack. The name can be from 1 to 16 alphanumeric characters, not including the extension “.cfg”. If the filename contains spaces, enclose it in double quotes.
--------	--

### Description

This command specifies the active configuration file on the master switch. The master switch uses the active configuration file to save the stack parameter settings when the SAVE CONFIGURATION command is issued and to configure the settings whenever the stack performs the discovery process.

Before using this command, note the following:

- ❑ To view the name of the currently active configuration file, see “SHOW CONFIG” on page 212.
- ❑ The configuration file must already exist. To view the files, see “SHOW FILE” on page 213. Configuration files have a “.cfg” extension. To create an entirely new configuration file, refer to “CREATE CONFIG” on page 203.
- ❑ Changing the active boot configuration file does not change the current operating configuration of the stack. You must reset or power cycle the stack after specifying the new active boot configuration file if you want it to use the settings in the file.
- ❑ If you specify a new active configuration file and enter the SAVE CONFIGURATION command without resetting the stack, the current settings of the switch overwrite the settings in the file.
- ❑ The NONE option does the following:
  - It removes the currently active configuration file without assigning a new one.
  - The stack continues to operate with its existing configuration settings.
  - You may make further parameter changes, but you cannot save them.
  - If you reset the stack, it uses the STACK.CFG file to configure its settings.

- To be able to save configuration changes again, you must assign a new active boot configuration file.
- ❑ If the master switch has a flash memory card, you can specify a configuration file on a flash card as the active boot configuration file. However, the configuration file is not copied to the master switch's file system, but is instead used and updated directly from the card. If you remove the card and reset the stack, the management software uses its default settings.
- ❑ If the file is on a flash memory card, you must change to the directory where the file is stored before performing this command. The command does not accept a directory path. To change directories on a flash card, see "SET CFLASH DIR" on page 208. The default location is the root of the flash card.

### Examples

The following command selects the file `stack22.cfg` as the new active boot configuration file for the stack:

```
set config=stack22.cfg
```

If you want the stack to use the settings in the file, you must reset or power cycle the units. If, instead, you want to overwrite the settings in the file with the stack's current settings, enter the `SAVE CONFIGURATION` command.

The following command uses the `NONE` option to remove the current active boot configuration file without specifying a new one. After entering this command, you can continue to make changes to the parameter settings of the stack devices, but you will not be able to save them. If you reset the stack, the master switch uses the `STACK.CFG` file to configure the parameter settings:

```
set config=none
```

The following command selects the file `"sales stack.cfg"` on a flash memory card as the stack's active boot configuration file:

```
set config=cflash:"sales stack.cfg"
```

## SHOW CFLASH

---

### Syntax

```
show cflash
```

### Parameter

None

### Description

This command displays information about the compact flash card in the master switch. The information includes the current directory, the number of files, how much space is used, and amount of space available. An example is shown in Figure 24.

Compact Flash:

-----  
Current Directory: \

Number of files ..... 6

Number of directories ..... 3

Bytes used ..... 4468

Card Information:

Hardware detected ..... Yes

Serial Number ..... F000530211

Size ..... 124666 KB

Used ..... 22 KB (8 files)

Free ..... 124644 KB

Figure 24. SHOW CFLASH Command

### Example

```
show cflash
```

## SHOW CONFIG

---

### Syntax

```
show config [dynamic]
```

### Parameter

dynamic	Displays the stack's parameter settings in command line format.
---------	---

### Description

This command, when used without the DYNAMIC parameter, displays two pieces of information. An example is shown in Figure 25.



```
Boot configuration file ..... "SalesSt4a.cfg" (Exists)
Current configuration ..... "SalesSt4a.cfg"
```

Figure 25. SHOW CONFIG Command

The “Boot configuration file” field displays the name of the file that the master switch uses to store the parameter settings of the stack whenever the SAVE CONFIGURATION command is issued. This is also the file that the master switch will use during the reset or power cycle to configure the stack. To change the boot configuration file, refer to “SET CONFIG” on page 209.

The “Current Configuration” displays the name of the boot configuration file that the master switch used to configure the stack during the last discovery process.

The DYNAMIC parameter displays the parameter settings that have been changed from their default value, in command line format. An example is shown in Figure 12 on page 94.

### Example

This command displays the names of the active and current configuration files:

```
show config
```

This command displays the parameter settings of the stack in command line format:

```
show config dynamic
```

## SHOW FILE

---

### Syntax

```
show file[=[cflash:] filename.ext]
```

### Parameter

**file** Specifies the name of the file to be displayed. Use double quotes to enclose the name if it contains spaces. Otherwise, the quotes are optional. To view a file on a flash memory card, precede the name with "cflash".

If you do not specify a file name, the command displays a list of all files in flash memory as well as on the compact flash card.

### Description

This command displays a list of the files in the master switch's file system. You can use the wildcard "\*" to replace any part of the filename to allow a more selective display. You can also use this command to view the contents of a configuration file.

### Examples

This command displays all the files in the master switch's file system and the current directory of the flash memory card:

```
show file
```

This command displays just the configuration files on the master switch:

```
show file=*.cfg
```

This command displays the contents of the configuration file sw12.cfg in the master switch's file system:

```
show file=sw12.cfg
```

This command displays the contents of the configuration file boot.cfg on a compact flash card:

```
show file=cflash:boot.cfg
```

## SHOW FLASH

---

### Syntax

```
show flash
```

### Parameter

None

### Description

This command displays information about the file system in the master switch. The information includes the number of files, how much space is used, and the amount of space available. An example is shown in Figure 26.

Flash:

```
-----  
Files ..... 12288 bytes (5 files)  
Free ..... 8211456 bytes  
Total ..... 8223744 bytes  
-----
```

Figure 26. SHOW FLASH Command

### Example

```
show flash
```

## Chapter 14

# File Download and Upload Commands

---

This chapter contains the following commands:

- ❑ “LOAD METHOD=LOCAL” on page 216
- ❑ “LOAD METHOD=TFTP” on page 218
- ❑ “LOAD METHOD=XMODEM” on page 223
- ❑ “UPLOAD METHOD=LOCAL” on page 227
- ❑ “UPLOAD METHOD=TFTP” on page 229
- ❑ “UPLOAD METHOD=XMODEM” on page 232

## LOAD METHOD=LOCAL

---

### Syntax

```
load method=local destfile=appblock
srcfile|file=[cflash:] filename
```

### Parameters

method	Specifies a local download.
destfile	Specifies the application block (APPBLOCK) of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S63 image file.
srcfile or file	Specifies the filename of the AT-S63 image file in the file system to be downloaded into the application block. If the image file is stored on a compact flash card, precede the filename with "cflash:". If the filename contains a space, enclose it in double quotes. These parameters are equivalent.

### Description

This command downloads an AT-S63 image file from the switch's file system into the application block, which is the section of flash memory reserved for the active AT-S63 running image. This function makes the AT-S63 file the new active image file on the switch. This command assumes that at some earlier point you downloaded a new version of the AT-S63 image file into the file system of a switch and now want to copy it into application block so that it becomes the switch's active image file.

This command can also be used to download an AT-S63 image file from a compact flash card into the application block.

---

#### Note

Do not perform this command when the switch is part of a stack. Updates to the AT-S63 Management Software should only be performed when the switch is functioning as a standalone unit.

---

When performing a local download, note the following:

- ❑ The AT-S63 management image file must already be stored in the switch's file system or on a compact flash card.
- ❑ The command must include the DESTFILE parameter with the APPBLOCK option.



- ❑ Use the SRCFILE or FILE parameter to specify the name of the AT-S63 image file in the switch's file system or on the compact flash card.
- ❑ The current configuration of a switch is retained when a new AT-S63 software image is copied to the application block.
- ❑ After downloading an image file into the application block, you can delete the image file from the file system or compact flash card to free up space for other files.



### Caution

The switch, after downloading the AT-S63 image file into its application block, automatically resets to initialize the new management software. The entire process can take a minute or so to complete. The switch does not forward network traffic during the reset process. Some network traffic may be lost.

## Examples

This command downloads an AT-S63 image file stored in the switch's file system into the application block, the area of flash memory reserved for the active running image. This makes the file the active image file on the switch. The name of the image file in the file system in this example is "ats63v2.img":

```
load method=local destfile=appblock srcfile="ats63v2.img"
```

A confirmation prompt is displayed. Type **Y** for yes to transfer the file to the application block or **N** for no to cancel the procedure.

This command downloads an AT-S63 image file from a compact flash card to the switch's application block. The name of the image file on the compact flash card is "ats63v2.img":

```
load method=local destfile=appblock  
srcfile=cflash:"ats63v2.img"
```

## LOAD METHOD=TFTP

---

### Syntax

```
load method=tftp destfile=[cflash:] filename | appblock
server=ipaddress srcfile | file=filename
```

### Parameters

method	Specifies a TFTP download.
destfile	<p>Specifies the destination filename for the file. This is the name given to the file when it is stored in the switch's file system. The name can be from 1 to 15 alphanumeric characters, not including the three-letter extension. If the name includes spaces, enclose it in double quotes. The name must be unique from the files already stored in the file system. The command will not overwrite a preexisting file with the same name.</p> <p>To download a file onto a flash memory card in the switch rather than the file system, precede the name with "cflash:".</p> <p>The APPBLOCK option specifies the application block of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S63 image file. The APPBLOCK option is used to download a new AT-S63 image file from a TFTP server to the application block of the switch so that it functions as the new active image file on the switch.</p>
server	Specifies the IP address of the TFTP server on the network.
srcfile <b>or</b> file	Specifies the filename of the file on the TFTP server to download onto the switch. If the filename contains a space, enclose the name in double quotes. These parameters are equivalent.

### Description

A TFTP download uses the TFTP client software on the switch to download files onto the unit from a TFTP server on your network. For example, you might use the command to update a switch's AT-S63 image file, or to download a different boot configuration file or a SSL public key certificate. You can also use this command to download a file from a TFTP server to a flash memory card in the switch.

The DESTFILE parameter specifies a name for the file when it is stored in the file system or a flash memory card in the switch. Enclose the name in double quotes if it contains a space. When specifying the new name of a downloaded file, be sure to give it the correct three-letter extension that corresponds to its file type. The extensions are shown in Table 4.

Table 4. File Name Extensions - Downloading Files

Extension	File Type
.cfg	AT-S63 configuration file
.cer	CA certificate
.img	AT-S63 management software image (An AT-S63 image file is assigned a named only if you are downloading the file into the switch's file system instead of the application block.)

To store a file in a flash memory card, the destination filename must be preceded with "cflash:".

The APPBLOCK option of the DESTFILE parameter refers to the switch's application block, which is a portion of flash memory separate from the file system reserved for the active AT-S63 image. The APPBLOCK option downloads a new version of the AT-S63 image file into the application block, making it the active image file on the switch.

---

**Note**

The APPBLOCK option can only be used to download a new AT-S63 image file.

---



---

**Note**

To upgrade the AT-S63 Management Software on the switches of a stack, you must disconnect the stacking cables and upgrade the switches individually. Do not attempt to upgrade the AT-S63 Management Software while the switches are part of a stack.

---

The equivalent FILE and SCRFILE parameters specify the name of the file on the TFTP server to download onto the switch.

Before downloading a file onto a switch using TFTP, note the following:

- ☐ A TFTP download is supported from a local, Telnet or SSH management session.
- ☐ There must be a node on your network that contains TFTP server software and the file to be downloaded must be stored on the server.

- ❑ You should start the TFTP server software before performing the download command.
- ❑ For AT-9400 Switches running AT-S63 version 2.0.0 or later, the switch must have a routing interface on the local subnet from where it reaches the TFTP server. The switch uses the interface's IP address as its source address during the file transfer with the server. For AT-9400 Switches without a routing interface, you can perform an Xmodem download from a local management session.
- ❑ For AT-9400 Switches running AT-S63 version 1.3.0 or earlier, the switch must be able to access the TFTP server through its management VLAN.
- ❑ If you are upgrading the switch from AT-S63 version 1.3.0 or earlier and the switch has an IP address, the upgrade process automatically creates a routing interface on the switch to preserve the device's IP configuration. If the switch has a static address, the interface is assigned the same address. If the unit obtains its IP configuration from a DHCP or BOOTP server, the interface is created with its DHCP or BOOTP client activated. The interface is given the interface number 0 and assigned to the preexisting management VLAN. Furthermore, the interface is designated as the local interface on the switch.

For example, if the switch has the static IP address 149.44.44.44 and the management VLAN has a VID of 12, the upgrade process automatically creates a routing interface with the same IP address and names it VLAN12-0. It assigns the interface to the VLAN with the VID of 12 and designates it as the switch's local interface.

- ❑ If you are downloading a configuration file, the switch does not automatically designate it as its active boot configuration file. To designate a configuration file as the active boot file after you have downloaded it onto the switch, refer to "SET CONFIG" on page 209.
- ❑ The AT-S63 software image can be downloaded only onto an AT-9400 Switch.
- ❑ The current configuration of a switch is retained when a new AT-S63 software image is installed.
- ❑ The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- ❑ If you download a new AT-S63 image file and enter a filename for the DESTFILE parameter instead of APPBLOCK, the file is stored in the switch's file system. To copy the image file from the file system to the application block so that its used by the switch as its active image file, refer to "UPLOAD METHOD=LOCAL" on page 227.

---

**Note**

Downloading an AT-S63 image file into a switch's file system rather than into the application block should be performed with care. The file will take up 2 megabytes of space in the file system.

---

- ❑ If you download a file onto a flash memory card in the switch and later want to copy the file from the card to a switch's file system, refer to "COPY" on page 201.

**Examples**

The following command downloads a new version of the AT-S63 software image directly to the switch's application block, making it the active image file on the switch. The IP address of the TFTP server is 149.11.11.11 and the name of the image file on the server is "ats63v2.img":

```
load method=tftp destfile=appblock server=149.11.11.11
srcfile=ats63v2.img
```



---

**Caution**

After downloading an AT-S63 image file and writing it to the application block portion of flash memory, the switch resets and initializes its management software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

---

The following command downloads a new configuration file into the switch's file system using TFTP. The configuration file is stored as "sw 111.cfg" on the TFTP server and is given the name "sw56a.cfg" when stored in the switch's file system. The TFTP server has the IP address 149.55.55.55:

```
load method=tftp destfile=sw56a.cfg server=149.55.55.55
srcfile="sw 111.cfg"
```

The following command downloads an SSL certificate to the switch's file system. The name of the file on the TFTP server is "sw12\_ssl.cer". The same name is used for the file in the switch's file system:

```
load method=tftp destfile=sw12_ssl.cer server=149.44.44.44
srcfile=sw12_ssl.cer
```

The following command downloads a new version of the AT-S63 image file from a TFTP server to the switch's file system, changing the name from "ats63v1\_2\_0.img" to "ats63.img":

```
load method=tftp destfile=ats63.img server=149.11.11.11
srcfile=ats63v1_2_0.img
```

Since the file is downloaded to the switch's file system and not to the application block, it is not used as the switch's active image file. If at some point in the future you want to make it the active image file, refer to "UPLOAD METHOD=LOCAL" on page 227.

This command downloads a configuration file called "sw12.cfg" onto a flash memory card in the switch. The configuration file retains the same name when stored on the card. The TFTP server has the IP address 149.142.44.44:

```
load method=tftp destfile=cflash:sw12.cfg  
server=149.142.44.44 srcfile=sw12.cfg
```

This command downloads an AT-S63 image file from a TFTP server to a flash memory card in the switch:

```
load method=tftp destfile=cflash:ats63.img  
server=149.11.11.11 srcfile=ats63.img
```

## LOAD METHOD=XMODEM

---

### Syntax

```
load method=xmodem destfile=[cflash:] filename | appblock
```

### Parameters

method	Specifies an Xmodem download.
destfile	<p>Specifies the destination filename for the file. This is the name given to the file when it is stored in the switch's file system. The name can be from 1 to 15 alphanumeric characters, not including the three-letter extension. If the name includes spaces, enclose it in double quotes. The name must be unique from any files already stored in the file system. The command will not overwrite a preexisting file with the same name.</p> <p>To download a file onto a flash memory card in a switch rather than the file system, precede the name with "cflash:".</p> <p>The APPBLOCK option specifies the application block of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S63 image file. The APPBLOCK option is used to download a new AT-S63 image file into the application block so that it functions as the new active image file on the switch.</p>

### Description

An XMODEM download uses the XMODEM utility to download files onto a switch from a terminal or computer with a terminal emulator program connected to the switch's RS232 Terminal Port. You might use the command to update a switch's AT-S63 image file, or to download a different boot configuration file or a SSL public key certificate.

The DESTFILE parameter specifies a name for the file. This is the name the file will be stored as in the file system on the switch. Enclose the name in double quotes if it contains a space. When specifying the new name of a downloaded file, you must be sure to give it the correct three-letter extension, depending on the file type. The extensions are shown in Table 4 on page 219.

To download the file onto a flash memory card in the switch, precede the name with "cflash:".

The APPBLOCK option of the DESTFILE parameter refers to the switch's application block, which is the portion of flash memory reserved for the active AT-S63 image. This option downloads a new version of the AT-S63 image file into the application block, making it the active image file on the switch.

---

**Note**

The APPBLOCK option should only be used when downloading a new AT-S63 image file, and not with any other file type.

---



---

**Note**

To upgrade the AT-S63 Management Software on the switches of a stack, you must disconnect the stacking cables and upgrade the switches individually. Do not attempt to upgrade the AT-S63 Management Software while the switches are part of a stack.

---

Before downloading a file onto a switch using Xmodem, note the following:

- ❑ You must use a local management session to download a file using Xmodem.
- ❑ You can only use Xmodem to download a file onto the switch where you started the local management session.
- ❑ You must store the file to be downloaded on the computer or terminal connected to the RS232 Terminal Port on the switch.
- ❑ The transfer protocol can be Xmodem or 1K Xmodem.
- ❑ The switch does not automatically designate a newly downloaded configuration file as its active boot configuration file. To designate the active boot file, refer to “SET CONFIG” on page 209.
- ❑ The AT-S63 software image is only supported on AT-9400 Switches.
- ❑ The current configuration of a switch is retained when a new AT-S63 software image is installed.
- ❑ The AT-S63 image file also contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- ❑ If you download a new AT-S63 image file and enter a filename for the DESTFILE parameter instead of APPBLOCK, the file is stored in the switch's file system. To copy an image file from the file system to the switch's application block, refer to “LOAD METHOD=LOCAL” on page 216.
- ❑ If you download a file onto a flash memory card in the switch and later want to copy the file from the card to a switch's file system, refer to “COPY” on page 201.
- ❑ If you are upgrading the switch from AT-S63 version 1.3.0 or earlier and the switch has an IP address, the upgrade process automatically creates a routing interface on the switch to preserve the device's IP



configuration. If the switch has a static address, the interface is assigned the same address. If the unit obtained its IP configuration from a DHCP or BOOTP server, the interface is created with its DHCP or BOOTP client activated. The interface is given the interface number 0 and assigned to the preexisting management VLAN. Furthermore, the interface is designated as the local interface on the switch.

For example, if the switch has the static IP address 149.44.44.44 and the management VLAN has a VID of 12, the upgrade process automatically creates a routing interface with the same IP address and names it VLAN12-0. It assigns the interface to the VLAN with the VID of 12 and designates it as the switch's local interface.

## Examples

The following command uses the APPBLOCK option of the DESTFILE parameter to download a new version of the AT-S63 software image directly to the application block, making it the active image file on the switch:

```
load method=xmodem destfile=appblock
```



### Caution

After downloading an AT-S63 image file and writing it to the application block portion of flash memory, the switch resets itself and initializes the software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the reset process.

The following command downloads a new configuration file onto the switch. The configuration file is given the name "switch12.cfg" in the switch's file system:

```
load method=xmodem destfile=switch12.cfg
```

The source file is not specified when downloading a file using Xmodem. Rather, after you enter the command, the management software displays a confirmation prompt followed by another prompt instructing you to begin the file transfer. To start the transfer, you use your terminal emulation program to specify the file on your workstation that you want to download.

The following command uses Xmodem to download an SSL certificate into the switch's file system and assigns it the name sw12 ssl.cer:

```
load method=xmodem destfile="sw12 ssl.cer"
```

The following command downloads a configuration file onto a flash memory card in the switch. The configuration file is given the name "product\_sw.cfg" on the card:

```
load method=xmodem destfile=cflash:product_sw.cfg
```

The following command downloads a new version of the AT-S63 image file to the switch's file system instead of the application block. It does this by replacing the APPBLOCK option with a filename, in this case "ats63v1\_2\_0.img". The image file is stored in the switch's file system with this name:

```
load method=xmodem destfile=ats63v1_2_0.img
```

Since the file is stored in the switch's file system and not the application block, the switch does not use it as its active image file. If, at some point in the future, you want to make it the active image file, use "LOAD METHOD=LOCAL" on page 216.

## UPLOAD METHOD=LOCAL

---

### Syntax

```
upload method=local destfile=[cflash:] filename
srcfile|file=appblock
```

### Parameters

method	Specifies a local upload.
destfile	Specifies a filename for the AT-S63 image file. If the name contains spaces, enclose the name in quotes. To upload the active image file to a flash memory card in the switch, precede the name with "cflash:".
srcfile <i>or</i> file	Specifies the application block (APPBLOCK), where the active AT-S63 image file is stored.

### Description

This command copies the switch's active AT-S63 image file from the application block, where the active AT-S63 image is stored, into the switch's file system or to a flash memory card.

---

#### Note

You should never need to perform this command.

---

The DESTFILE parameter specifies a name for the AT-S63 image file when it is stored in the file system or on a compact flash memory card. The name should include the suffix ".img".

The equivalent SRCFILE and FILE parameters specify APPBLOCK, for application block.

### Examples

The following command uploads the active AT-S63 image from the switch's application block to the file system and assigns it the name "sw12 s63 image.img":

```
upload method=local destfile="sw12 s63 image.img"
srcfile=appblock
```

This command uploads the active AT-S63 image from the switch's application block to a flash memory card in the switch and assigns the name "s63.img" to the file:

```
upload method=local destfile=cflash:s63.img"  
srcfile=appblock
```

## UPLOAD METHOD=TFTP

---

### Syntax

```
upload method=tftp destfile=filename server=ipaddress
srcfile|file=switchcfg|[cflash:]filename|appblock
```

### Parameters

method	Specifies a TFTP upload.						
destfile	Specifies a filename for the uploaded file. This is the name given the file when it is stored on the TFTP server. If the name contains spaces, enclose it in quotes.						
server	Specifies the IP address of the network node containing the TFTP server software.						
srcfile <i>or</i> file	Specifies the file to be uploaded. Options are: <table data-bbox="737 892 1477 1226"> <tr> <td>switchcfg</td><td>Uploads the switch's active boot configuration file.</td></tr> <tr> <td><i>filename</i></td><td>Uploads a file from the switch's file system. If the file is stored on a compact flash card, precede the name with "cflash:".</td></tr> <tr> <td>appblock</td><td>Uploads the switch's active AT-S63 image file.</td></tr> </table>	switchcfg	Uploads the switch's active boot configuration file.	<i>filename</i>	Uploads a file from the switch's file system. If the file is stored on a compact flash card, precede the name with "cflash:".	appblock	Uploads the switch's active AT-S63 image file.
switchcfg	Uploads the switch's active boot configuration file.						
<i>filename</i>	Uploads a file from the switch's file system. If the file is stored on a compact flash card, precede the name with "cflash:".						
appblock	Uploads the switch's active AT-S63 image file.						

### Description

A TFTP upload uses the TFTP client software on the switch to upload files from the file system on the system to a TFTP server on the network. You can use the command to upload a switch's active boot configuration file or any other file from the file system, such as an SSL certificate enrollment request or a public encryption key. This command can also upload a file from a compact flash memory card in the switch to a TFTP server. You can also use the command to upload the switch's active AT-S63 software image from the application block to a TFTP server, though it is unlikely you would ever have need for that function.

When performing a TFTP upload, note the following:

- ☐ A TFTP upload is supported from a local, Telnet, or SSH management session.
- ☐ There must be a node on your network that contains the TFTP server software. The uploaded file will be stored on the server.

- ❑ Start the TFTP server software before you perform the command.
- ❑ The switch must have a routing interface on the local subnet from where it is reaching the TFTP server. The switch uses the interface's IP address as its source address during the file transfer with the server. The server can be located on any interface on the switch, not just the local interface. For a switch without a routing interface, you can perform an Xmodem upload from a local management session.

The DESTFILE parameter specifies a name for the file. This is a name for the file when it is stored on the TFTP server. The uploaded file should be given the same three-letter extension as the original file. The extensions are listed in Table 5.

Table 5. File Name Extensions - Uploaded Files

Extension	File Type
.cfg	Switch configuration file
.csr	CA certificate enrollment request
.log	Event log
.key	Public encryption key
.img	AT-S63 management software image

The SERVER parameter specifies the IP address of the network node with the TFTP server software where the uploaded file will be stored.

The equivalent SRCFILE and FILE parameters specify the name of the file to be uploaded from the switch. You have three options:

- ❑ SWITCHCFG - Uploads the switch's active boot configuration file to the TFTP server.
- ❑ *filename* - Uploads a file from the switch's file system to the TFTP server. This differs from the SWITCHCFG parameter in that the latter uploads just the active boot configuration file, while this parameter can upload any file in the file system. If the file to be uploaded is stored on a compact flash memory card in the switch, precede the name with "cflash:".
- ❑ APPBLOCK - Uploads the switch's active AT-S63 image file to the TFTP server.

---

**Note**

It is unlikely you will ever need to upload the active AT-S63 image file from a switch to a TFTP server.

---

## Examples

The following command uses TFTP to upload a configuration file called "sw22 boot.cfg" from the switch's file system to a TFTP server with an IP address of 149.88.88.88. The command stores the file on the server with the same name that it has on the switch:

```
upload method=tftp destfile="sw22 boot.cfg"
server=149.88.88.88 srcfile="sw22 boot.cfg"
```

The following command uses TFTP to upload the switch's active configuration file from the file system to a TFTP server with the IP address 149.11.11.11. The active boot file is signified with the SWITCHCFG option rather than by its filename. This option is useful in situations where you do not know the name of the active boot configuration file. The file is stored as "master112.cfg" on the TFTP server:

```
upload method=tftp destfile=master112.cfg
server=149.11.11.11 srcfile=switchcfg
```

The following command uploads a SSL certificate enrollment request form titled "sw12\_ssl\_enroll.csr" from the file system to the TFTP server. It changes the name of the file to "slave5b enroll.csr":

```
upload method=tftp destfile="slave5b enroll.csr"
server=149.11.11.11 srcfile=sw12_ssl_enroll.csr
```

The following command uploads a configuration file called "sales2.cfg" from a compact flash memory card in the switch to a TFTP server with an IP address of 149.124.88.88. The command stores the file on the server with the same name that it has on the card:

```
upload method=tftp destfile=sales2.cfg server=149.124.88.88
srcfile=cflash:sales2.cfg
```

The following command uploads the switch's active AT-S63 image file to a TFTP server with an IP addresses 149.55.55.55. The file is given the name "ats63 sw12.img":

```
upload method=tftp destfile="ats63 sw12.img"
server=149.55.55.55 srcfile=appblock
```

## UPLOAD METHOD=XMODEM

---

### Syntax

```
upload method=xmodem
srcfile|file=switchcfg|[cflash:]filename|appblock
```

### Parameters

method	Specifies an Xmodem upload.
srcfile or file	Specifies the file to be uploaded. Options are:
switchcfg	Uploads the switch's active boot configuration file.
filename	Specifies the name of a file to upload from the switch's file system or compact flash card. If the file is stored on a compact flash card, precede the name with "cflash:".
appblock	Uploads the switch's active AT-S63 image file.

### Description

An XMODEM upload uses the Xmodem utility to upload a file from the switch's file system to a terminal or computer with a terminal emulator program connected to the serial terminal port on the switch. You can use the command to upload a switch's active boot configuration file or any other file from the file system, such as an SSL certificate enrollment request or a public encryption key. You can also use this command to upload a file on a compact flash memory card to your workstation. The command also allows you to upload the switch's active AT-S63 software image from the application block to a your terminal or workstation, though it is unlikely you would ever have need for that function.

When performing an Xmodem upload, note the following:

- ❑ An Xmodem upload must be performed from a local management session.
- ❑ Xmodem can only upload a file from the switch where you started the local management session.

The equivalent SRCFILE and FILE parameters specify the name of the file to upload from the switch. You have three options:

- ❑ SWITCHCFG - Uploads the switch's active boot configuration file.



- ❑ *filename* - Uploads a file from the switch's file system or a compact flash memory card. This differs from the SWITCHCFG parameter in that the latter can upload just the active boot configuration file, while this parameter can upload any file on the switch. If the file is stored on a flash memory card in the switch, precede the filename with "cflash:".
- ❑ APPBLOCK - Uploads the switch's active AT-S63 image file.

---

**Note**

It is unlikely you will ever need to upload the active AT-S63 image file from a switch to your workstation.

---

## Examples

The following command uses Xmodem to upload a configuration file called "sw22 boot.cfg" from the switch's file system to your workstation:

```
upload method=xmodem srcfile="sw22 boot.cfg"
```

An Xmodem upload command does not include a destination filename. After entering the command, use your terminal emulator program to indicate where to store the file on your workstation and its filename.

The following command uploads the switch's active configuration file from the file system to your workstation. The active boot file is signified with the SWITCHCFG option rather than by its filename. This option is useful in situations where you do not know the name of the active boot configuration file:

```
upload method=xmodem srcfile=switchcfg
```

The following command uploads a SSL certificate enrollment request named "sw12\_ssl\_enroll.csr" from the switch's file system to the workstation:

```
upload method=xmodem srcfile=sw12_ssl_enroll.csr
```

The following command uses Xmodem to upload a configuration file called "pre10.cfg" from a flash memory card to the workstation where you are running the local management session:

```
upload method=xmodem srcfile=cflash:pre10.cfg
```

The following command uploads the switch's active AT-S63 image file to the workstation:

```
upload method=xmodem srcfile=appblock
```



## Chapter 15

# Event Log and Syslog Client Commands

---

This chapter contains the following commands:

- ❑ “ADD LOG OUTPUT” on page 236
- ❑ “CREATE LOG OUTPUT” on page 238
- ❑ “DESTROY LOG OUTPUT” on page 242
- ❑ “DISABLE LOG” on page 243
- ❑ “DISABLE LOG OUTPUT” on page 244
- ❑ “ENABLE LOG” on page 245
- ❑ “ENABLE LOG OUTPUT” on page 246
- ❑ “PURGE LOG” on page 247
- ❑ “SAVE LOG” on page 248
- ❑ “SET LOG FULLACTION” on page 250
- ❑ “SET LOG OUTPUT” on page 251
- ❑ “SHOW LOG” on page 254
- ❑ “SHOW LOG OUTPUT” on page 259
- ❑ “SHOW LOG STATUS” on page 261

---

### Note

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

### Note

The event logs on the master switch are the only active logs in the stack. The event logs on the member switches are inactive. For background information about event logs and the syslog client, refer to the *AT-S63 Management Software Features Guide*.

---

# ADD LOG OUTPUT

---

### Syntax

```
add log output=output-id module=[all | module]  
severity=[all | severity]
```

### Parameters

output	Specifies the output definition ID number.
module	Specifies what AT-S63 events to filter. The available options are:  <div><div>all</div><div>Sends events for all modules. This is the default.</div></div> <div><div>module</div><div>Sends events for specific module(s). You can select more than one module at a time, for example, MAC,PACCESS. For a list of modules, see Table 8, “AT-S63 Modules” on page 255.</div></div>
severity	Specifies the severity of events to be sent. The options are:  <div><div>all</div><div>Sends events of all severity levels.</div></div> <div><div>severity</div><div>Sends events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 9, “Event Log Severity Levels” on page 257. The default is I, E, and W.</div></div>

### Description

This command configures an output definition.

---

**Note**  
This version of the AT-S63 Management Software supports only syslog servers as output definitions.

---

There are two steps to creating a output definition from the command line interface. The first is to create the definition with “CREATE LOG OUTPUT” on page 238. This command assigns the definition an ID number, the IP address of the syslog server, and other information.

The second step is to customize the definition by specifying which event messages are to be sent. This is accomplished with this command. You can customize the definition so that the stack sends all of its event messages or just events from particular modules in the AT-S63 Management Software. An alternative method to configuring a definition is with “SET LOG OUTPUT” on page 251.

---

**Note**

The default configuration for a new output definition is no event messages. The stack does not send any events until you customize the definition with this command or “SET LOG OUTPUT” on page 251.

---

The OUTPUT parameter specifies the ID number of the output definition you want to configure. The range is 2 to 20. The definition must already exist on the stack. To view the existing definitions and their ID numbers, refer to “SHOW LOG OUTPUT” on page 259.

The MODULE parameter specifies the modules whose events you want the stack to send. The AT-S63 Management Software consists of a number of modules. Each module is responsible for a different part of stack operation and generates its own events. The MODULE parameter's ALL option sends the events from all the modules. You can also specify individual modules, which are listed in Table 8 on page 255.

The SEVERITY parameter specifies the severity of the events to be sent. For example, you might configure the stack to send only error events of all the modules. Or, you might configure a definition so that the stack sends only warning events from a couple of the modules, such as the spanning tree protocol and the MAC address table. For a list of severity levels, refer to Table 9 on page 257.

**Examples**

The following command configures output definition 5 to send event messages from all modules and all severity levels:

```
add log output=3 module=all severity=all
```

The following command configures output definition 3 to send only messages related to the event log and the MAC address table with an error severity level:

```
add log output=3 module=evtlog,mac severity=e
```

# CREATE LOG OUTPUT

---

### Syntax

```
create log output=output-id destination=syslog
server=ipaddress
[facility=default|local1|local2|local3|local4|local5|local6
|local7] [syslogformat=extended|normal]
```

### Parameters

output	Specifies an ID number that identifies the output definition. The possible output IDs are:	
	0	Reserved for permanent (nonvolatile) storage. You cannot change or delete this ID.
	1	Reserved for temporary (dynamic) storage. You cannot change or delete this ID.
	2 - 20	Available to be used for other outputs.
destination	Specifies the destination for the log messages. The only option currently supported is:	
	syslog	Forwards log messages in syslog format to a syslog server.
server	Specifies the IP address of the syslog server.	
facility	Specifies a facility level to be added to the events.	
	default	Adds a facility level based on the functional groupings defined in the RFC 3164 standard. The codes applicable to the AT-S63 Management Software and its modules are shown in Table 6 on page 240. This is the default setting.
	local1 to local7	Adds a set facility code of 17 (LOCAL1) to 23 (LOCAL7) to all event messages. For a list of the levels and their corresponding codes, refer to Table 7 on page 241.

syslogformat	Specifies the format of the generated messages. The possible options are:
extended	Messages include the date, time, and system name. This is the default.
normal	Messages do not include the date, time, and system name.

## Description

This command creates a new output definition. The stack uses the definition to send event messages to a device on your network. You can create up to nineteen output definitions.

---

### Note

This version of the AT-S63 Management Software supports only syslog servers as output definitions.

---



---

### Note

The stack must communicate with a syslog server through a local network or subnet that has a routing interface. The stack uses the IP address of the interface as its source address when sending packets to the server. For instructions on how to add a routing interface to the stack, refer to “ADD IP INTERFACE” on page 392.

---

After creating a output definition with this command, you must customize it by defining which event messages you want the stack to send. You can customize a definition so that the stack sends all of its event messages or limit it to just a selection of events from particular modules in the AT-S63 Management Software. Customizing a definition is accomplished with “ADD LOG OUTPUT” on page 236 or “SET LOG OUTPUT” on page 251.

---

### Note

The default configuration for a new output definition is no event messages. The stack does not send events until you customize the definition.

---

The OUTPUT parameter specifies the ID number for the new output definition. The range is 2 to 20. Every definition must have a unique ID number.

The SERVER parameter specifies the IP address of the syslog server.

The FACILITY parameter adds a numerical code to the entries as they are sent to the syslog server so that the entries are grouped on the server according to the source device. This is of particular value when a syslog server is collecting events from several different network devices. You can specify only one facility level for a syslog server definition.

There are two approaches to using this parameter. The first is to use the DEFAULT option. This setting determines the codes of the messages based on the functional groupings in the RFC 3164 standard. For example, encryption key events and port mirroring events would be assigned codes 4 and 22, respectively. The codes that are applicable to the AT-S63 Management Software and its modules are shown in Table 6.

Table 6. Default Syslog Facilities

Facility Number	Syslog Protocol Definition	Mapped Event Log Modules and Events
4	Security/ authorization messages	Security and authorization messages from the following modules: DOS, ENCO, PACCESS (802.1x), PKI, PSEC (port security), RADIUS, SSH, SSL, TACACS+, and system events such as user login and logout.
9	Clock daemon	Time-based activities and events from the following modules: TIME, SNTP, and RTC.
16	Local use 0	All other modules and events.
22	Local use 6	Physical interface and data link events from the following modules: PCFG (port configuration), PMIRR (port mirroring), PTRUNK (port trunking), STP, and VLANs.
23	Local use 7	System events related to major exceptions.

Another approach is assign the same numerical code to all of the events using the LOCAL1 to LOCAL7 options, each of which represents a predefined RFC 3164 numerical code, as listed in Table 7. For example, the facility level LOCAL2 assigns the numerical code 18 to all of the events sent by the stack to the syslog server.



Table 7. Numerical Code and Facility Level Mappings

Facility Level Setting	Numerical Code
LOCAL1	17
LOCAL2	18
LOCAL3	19
LOCAL4	20
LOCAL5	21
LOCAL6	22
LOCAL7	23

The SYSLOGFORMAT parameter defines the content of the events.

### Examples

The following command creates a definition for a syslog server with the IP address 149.65.10.22. The definition, which is given the ID 10, sends the messages in normal format with a facility level setting of LOCAL6:

```
create log output=10 destination=syslog server=149.65.10.22
facility=local6 syslogformat=normal
```

The following command creates a definition for a syslog server with the IP address 149.65.10.101. Because the SYSLOGFORMAT option is omitted from the command, the messages are sent in extended format, which is the default:

```
create log output=18 destination=syslog server=149.65.10.101
```

## DESTROY LOG OUTPUT

---

### Syntax

```
destroy log output=output-id
```

### Parameters

output                      Specifies the output definition ID number.

### Description

This command deletes an output definition. To disable the output definition without deleting it, see “DISABLE LOG OUTPUT” on page 244.

### Example

This command deletes output definition number 3:

```
destroy log output=3
```

## DISABLE LOG

---

### Syntax

```
disable log
```

### Parameters

None.

### Description

This command disables the event log module. When the log module is disabled, the AT-S63 Management Software stops storing events in the event logs and sending events to output definitions. The default setting for the event logs is enabled.

---

#### Note

The event log module, even when disabled, still logs all AT-S63 initialization events that occur when the stack is reset or power cycled. Any events that occur after AT-S63 initialization are recorded only if the event log module is enabled.

---

### Examples

The following command disables the event log on the switch:

```
disable log
```

## DISABLE LOG OUTPUT

---

### Syntax

```
disable log output[=output-id]
```

### Parameters

output	Specifies the output definition ID number to disable. Not specifying an output definition disables all definitions.
--------	---

### Description

This command disables an output definition. When disabled, no event messages are sent to the specified device, although the definition still exists. To permanently remove an output definition, see “DESTROY LOG OUTPUT” on page 242. To enable the output definition again, see “ENABLE LOG OUTPUT” on page 246.

### Example

The following command disables (but does not delete) output definition number 7:

```
disable log output=7
```

The following command disables all configured definitions:

```
disable log output
```

## ENABLE LOG

---

### Syntax

```
enable log
```

### Parameters

None.

### Description

This command activates the event logs. After the log is activated, the switch immediately starts to store events in the event logs and send events to defined outputs. The default setting for the event log is enabled.

### Example

The following command activates the event log module on the switch:

```
enable log
```

## ENABLE LOG OUTPUT

---

### Syntax

```
enable log output[=output-id]
```

### Parameters

output	Specifies the output definition ID number to enable. The range is 2 to 20.
--------	---

### Description

This command enables an output definition that was disabled using “DISABLE LOG OUTPUT” on page 244.

### Example

The following command enables output definition number 4:

```
enable log output=4
```

The following command enables all output definitions:

```
enable log output
```

## PURGE LOG

---

### Syntax

```
purge log[=permanent|temporary]
```

### Parameter

log	Specifies the event log to be purged. The options are:	
	permanent	Permanent (nonvolatile) memory. Deletes all of the events in the event log in nonvolatile memory, which can contain up to 2,000 events.
	temporary	Temporary memory. Deletes all of the events in the event log in temporary memory, which can contain up to 4,000 events. This is the default if you do not specify the “permanent” option.

### Description

This command deletes all the entries stored in an event log.

### Example

The following command deletes all the entries in the event log stored in temporary memory:

```
purge log=temporary
```

The following command deletes all the entries in both event logs:

```
purge log
```

## SAVE LOG

---

### Syntax

```
save log[=permanent|temporary] filename=filename.log [full]
[module=module] [reverse] [severity=all|severity]
[overwrite]
```

### Parameters

log	Specifies the source of the events you want to save to the log file. The options are:
permanent	Permanent (nonvolatile) memory. Saves events stored in nonvolatile memory, which can contain up to 2,000 events.
temporary	Temporary memory. Saves events stored in temporary memory, which can contain up to 4,000 events. This is the default.
filename	Specifies the filename for the log. The name can be up to 16 alphanumeric characters, followed by the extension ".log." Spaces are allowed. The filename must be enclosed in quotes if it contains spaces. Otherwise, the quotes are optional.
full	Specifies the amount of information saved to the log. Without this option, the log saves only the time, module, severity, and description for each entry. With it, the log also saves the filename, line number, and event ID.
module	Specifies the AT-S63 module whose events are to be saved. For a list of modules, refer to Table 8 on page 255. Omitting this parameter saves the events from all the modules.
reverse	Specifies the order of the events in the log. Without this option, the events are saved oldest to newest. With this option, the events are saved newest to oldest.
severity	Specifies the severity of events to be saved. The options are:
all	Saves events of all severity levels.



severity	Saves events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 9, “Event Log Severity Levels” on page 257. The default is E, W, I.
overwrite	Overwrites the file if it already exists. Without this option, the command displays an error if a file with the same name already exists in the master switch’s file system.

## Description

This command saves the current entries in an event log to a file in the file system. The parameters in the command allow you to specify which events you want saved in the log file.

## Examples

The following command saves the event messages stored in the permanent event log to a file called “stack2.log”. Because the MODULE and SEVERITY parameters are not included in the command, the defaults are used, which is events from all modules with an informational, error, or warning severity level:

```
save log=permanent filename=stack2.log
```

The following command saves the error messages of the VLAN module stored in the temporary event log in a file called “sw14.log.”:

```
save log=temporary filename=sw14.log module=vlan severity=e
```

The following command saves informational messages from all modules in a file called “sw56.log” and overwrites the file of the same name if it already exists in the file system:

```
save log=permanent filename=sw56.log severity=i overwrite
```

## SET LOG FULLACTION

---

### Syntax

```
set log fullaction [temporary=halt|wrap]  
[permanent=halt|wrap]
```

### Parameters

fullaction	Specifies what happens when a log reaches maximum capacity. You can set the action separately for each log. The possible actions are:
halt	The log stops storing new events.
wrap	The log deletes the oldest entries as new ones are added. This is the default.

### Description

This command defines the action of an event log when it has stored its maximum number of entries. The HALT option instructs the log to stop storing new entries. If the event log has already reached its maximum capacity, it immediately stops entering new entries. The WRAP option instructs the log to delete the oldest entries as new entries are added.

To view the current actions of the event logs, refer to “SHOW LOG OUTPUT” on page 259.

### Example

The following command configures the event log in permanent memory to stop storing new entries after it has stored the maximum number of allowed entries:

```
set log fullaction permanent=halt
```

## SET LOG OUTPUT

---

### Syntax

```
set log output=output-id [destination=syslog]
server=ipaddress
[facility=default|local1|local2|local3|local4|local5|local6
|local7] [syslogformat=extended|normal] [module=all|module]
[severity=all|severity-list]
```

### Parameters

output	Specifies an ID number that identifies the output definition to be modified. The possible output IDs are:	
	0	Reserved for permanent (nonvolatile) storage. You cannot change or delete this ID.
	1	Reserved for temporary (dynamic) storage. You cannot change or delete this ID.
	2 - 20	Available to be used for other outputs.
destination	Specifies the destination for the log messages. The only option currently supported is:	
	syslog	Forwards log messages in syslog format to a syslog server.
server	Specifies a new IP address for the syslog server.	
facility	Specifies a facility level to be added to the events.	
	default	Adds a facility level based on the functional groupings defined in the RFC 3164 standard. The codes applicable to the AT-S63 Management Software and its modules are shown in Table 6 on page 240. This is the default setting.
	local1 to local7	Adds a set facility code of 17 (LOCAL1) to 23 (LOCAL7) to all event messages. For a list of the levels and their corresponding codes, refer to Table 7 on page 241.

syslogformat	Specifies the format of the generated messages. The possible options are:
extended	Messages include the date, time, and system name. This is the default.
normal	Messages do not include the date, time, and system name.
module	Specifies what AT-S63 events to filter. The available options are:
all	Sends events for all modules. This is the default.
module	Sends events for specific module(s). You can select more than one module at a time, for example, MAC,PACCESS. For a list of modules, see Table 8, “AT-S63 Modules” on page 255.
severity	Specifies the severity of events to be sent. The options are:
all	Sends events of all severity levels.
severity	Sends events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 9, “Event Log Severity Levels” on page 257. The defaults are I, E, and W.

### Description

This command modifies an existing output definition. For further information on the FACILITY and SYSLOGFORMAT parameters, see “CREATE LOG OUTPUT” on page 238. For further information about the MODULE and SEVERITY parameters, see “ADD LOG OUTPUT” on page 236.

---

#### Note

This version of the AT-S63 Management Software supports only syslog servers as output definitions.

---

## Examples

The following command changes the IP address for output definition number 5 to 149.55.55.55:

```
set log output=5 server=149.55.55.55
```

The following command modifies output definition number 6 to only send messages from the RADIUS module of all severity levels:

```
set log output=6 module=radius severity=all
```

The following command changes the facility level and message format for output definition 4. The facility level is changed to LOCAL1 (numerical code 17) and the format to normal so that the messages include only severity, module, and description:

```
set log output=11 facility=local1 syslogformat=normal
```

The following command changes syslog server definition 11 to send only spanning tree and IGMP snooping events with a severity level of error or warning:

```
set log output=11 module=stp,igmpsnooping severity=e,w
```

## SHOW LOG

---

### Syntax

```
show log[=permanent|temporary] [full] [module=module]
[reverse] [severity=severity]
```

### Parameters

log	Specifies which of the two event logs you want to view. The options are:
permanent	Displays the events stored in permanent memory.
temporary	Displays the events stored in temporary memory. This is the default.
full	Specifies the amount of information displayed by the log. Without this option, the log displays the time, module, severity, and description for each entry. With it, the log also displays the filename, line number, and event ID.
module	Specifies the AT-S63 module whose events you want displayed. For a list of modules, refer to Table 8 on page 255.
reverse	Specifies the order of the events in the log. Without this option, the events are displayed oldest to newest. With this option, the events are displayed newest to oldest.
severity	Specifies the severity of events to be displayed. The options are:
all	Displays events of all severity levels.
severity	Displays events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 9, “Event Log Severity Levels” on page 257. The defaults are I, E, and W.

## Description

This command displays the entries stored in an event log.

An event log can display entries in two modes: normal and full. In the normal mode, a log displays the time, module, severity, and description for each entry. In the full mode, a log also displays the filename, line number, and event ID. If you want to view the entries in the full mode, use the FULL parameter. To view entries in the normal mode, omit the parameter.

The MODULE parameter displays entries generated by a particular AT-S63 module. You can specify more than one module at a time. If you omit this parameter, the log displays the entries for all the modules. Table 8 lists the modules and their abbreviations.

Table 8. AT-S63 Modules

Module Name	Description
ALL	All modules
ACL	Port access control list
CFG	Stack configuration
CLASSIFIER	Classifiers used by ACL and QoS
CLI	Command line interface commands
DOS	Denial of service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP GVRP
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	System IP configuration
LACP	Link Aggregation Control Protocol
MAC	MAC address table
MGMTACL	Management access control list
MLDSNOOP	MLD snooping
PACCESS	802.1x port-based access control

Table 8. AT-S63 Modules (Continued)

Module Name	Description
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	MAC address-based port security
PTRUNK	Static port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RPS	Redundant power supply
RRP	RRP snooping
RTC	Real time clock
SNMP	SNMP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; manager and operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	Telnet
TFTP	TFTP
TIME	System time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes
WATCHDOG	Watchdog timer

The log can display its entries in chronological order (oldest to newest), or reverse chronological order. The default is chronological order. To reverse the order, use the REVERSE parameter.

The SEVERITY parameter displays entries of a particular severity. Table 9 defines the different severity levels. You can specify more than one severity level at a time. The default is to display error, warning, and informational messages.



Table 9. Event Log Severity Levels

Value	Severity Level	Description
E	Error	Stack operation is severely impaired.
W	Warning	An issue may require manager attention.
I	Informational	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for technical support and software development.

An example of the event log is shown in Figure 27. The example uses the full display mode.

S	Date	Time	EventID Event	Source File:Line Number
I	2/01/04	09:11:02	073001	garpmain.c:259
			garp: GARP initialized	
I	2/01/04	09:55:15	083001	portconfig.c:961
			pcfg: PortConfig initialized	
I	2/01/04	10:22:11	063001	vlanapp.c:444
			vlan: VLAN initialization succeeded	
I	2/01/04	12:24:12	093001	mirrorapp.c:158
			pmirr: Mirror initialization succeeded	
I	2/01/04	12:47:08	043016	macapp.c:1431
			mac: Delete Dynamic MAC by Port[2] succeeded	

Figure 27. Event Log Example

The columns in the log are described below:

- ❑ S (Severity) - The event's severity. Refer to Table 9 on page 257.
- ❑ Date/Time - The date and time the event occurred.
- ❑ Event - The module within the AT-S63 software that generated the event followed by a brief description of the event. For a list of the AT-S63 modules, see Table 8 on page 255.
- ❑ Event ID - A unique number that identifies the event. (Displayed only in the full display mode.)
- ❑ Filename and Line Number - The subpart of the AT-S63 module and the line number that generated the event. (Displayed only in the full display mode.)

## Examples

The following command displays all the entries in the event log stored in permanent memory:

```
show log=permanent
```

The following command displays the events stored in temporary memory in the full display mode, which adds more information:

```
show log=temporary full
```

The following command displays only those entries stored in temporary memory and associated with the AT-S63 modules FILE and QOS:

```
show log=permanent module=file,qos
```

The following command displays the error and warning entries for the AT-S63 module VLAN. Because the log is not specified, the temporary log is displayed by default:

```
show log module=vlan severity=e,w
```

## SHOW LOG OUTPUT

### Syntax

```
show log output[=output-id] [full]
```

### Parameters

output	Specifies the output definition ID number. If an output ID number is not specified, all output definitions on the stack are displayed.
full	Displays the details of the output definition. If not specified, only a summary is displayed.

### Description

This command displays output definition details. An example of the information displayed by this command is shown in Figure 28.

OutputID	Type	Status	Details
0	Permanent	Enabled	Wrap on Full
1	Temporary	Enabled	Wrap on Full
2	Syslog	Enabled	169.55.55.55
3	Syslog	Enabled	149.88.88.88

Figure 28. SHOW LOG OUTPUT Command

The columns in the display are described below:

- ❑ Output ID - The ID number of the output definition. The permanent event log has the ID 0 and the temporary log has the ID 1. Syslog server definitions start with ID 2.
- ❑ Type - The type of output definition. Permanent is the permanent event log and Temporary is the temporary event log. Syslog indicates a syslog server definition.
- ❑ Status - The status of the output definition, which can be enabled or disabled.
- ❑ Details - The event log full action or a syslog server's IP address. For an event log, this column contains the log's full action. Wrap on Full indicates that the log adds new entries by deleting old entries when it reaches maximum capacity. Halt on Full means the log stops adding entries after reaching maximum capacity. To configure the full action for an event log, refer to "SET LOG FULLACTION" on page 250. For a syslog definition, this column contains the IP address of the syslog server.

An example of the information displayed by this command with the FULL parameter is shown in Figure 29.

```
Output ID ..... 2
Output Type ..... Syslog
Status ..... Enabled
Server IP Address ..... 149.88.88.88
Message Format ..... Extended
Facility Level ..... DEFAULT
Event Severity ..... E,W,I
Event Module ..... All
```

Figure 29. SHOW LOG OUTPUT Command with the FULL Parameter

For definitions of the parameters, refer to “SET LOG OUTPUT” on page 251.

### Examples

The following command lists all the output definitions:

```
show log output
```

The following command displays the details of output definition number 5:

```
show log output=5 full
```

## SHOW LOG STATUS

---

### Syntax

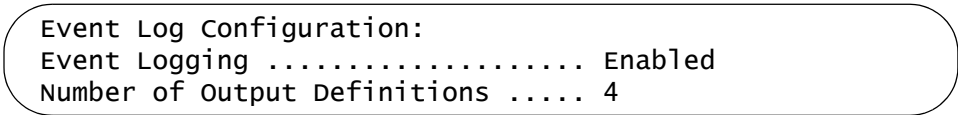
```
show log status
```

### Parameter

None.

### Description

This command displays information about the event log feature. Figure 30 is an example of the information displayed by this command.



```
Event Log Configuration:  
Event Logging ..... Enabled  
Number of Output Definitions ..... 4
```

Figure 30. SHOW LOG STATUS Command

The Event Logging field indicates whether the feature is enabled or disabled. If enabled, the stack stores events in the event logs and sends events to defined outputs. If disabled, no events are stored in the event logs or sent to defined outputs. To enable and disable the event logs, refer to “ENABLE LOG” on page 245 and “DISABLE LOG” on page 243.

The Number of Output Definitions is the sum of the two event logs plus any output definitions that you might have created. For instance, the number 4 for Number of Output Definitions in the above example indicates the existence of two output definitions in addition to the two event logs. To create new output definitions, refer to “CREATE LOG OUTPUT” on page 238 and “ADD LOG OUTPUT” on page 236.

### Example

The following command displays event log status information:

```
show log status
```



## Chapter 16

# Class of Service (CoS) Commands

---

This chapter contains the following command:

- “SET SWITCH PORT PRIORITY OVERRIDE PRIORITY” on page 264

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

**Note**

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## SET SWITCH PORT PRIORITY OVERRIDEPRIORITY

---

### Syntax

```
set switch port=port [priority=value]  
[overridepriority=yes|no|on|off|true|false]
```

### Parameters

port	Specifies the port to be configured. You can specify more than one port at a time, but the ports must be of the same medium type (either all twisted pair ports or all fiber optic ports). Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
priority	Specifies a temporary priority level for all ingress untagged packets received on the port. If you include the OVERRIDEPRIORITY parameter, the temporary priority level also applies to all ingress tagged packets. The range is 0 to 7; 0 is the lowest priority, and 7 is the highest.
overridepriority	Determines if a port should ignore the priority level in tagged packets and instead use the temporary priority level assigned to the port with the PRIORITY parameter. The options are:  yes, on, true Overrides the priority level in tagged packets and uses the temporary priority level. This is the default. The options are equivalent.  no, off, false Does not override the priority in tagged packets. The options are equivalent.

### Description

This command can change a port’s temporary priority level. It can also be used to determine whether a port receiving tagged packets should use the priority level in the frames or a temporary priority level assigned to the port.



This command allows you to override the priority level mappings at the port level by assigning the packets a temporary priority. Note that this assignment is made when a packet is received on the ingress port and before the frame is forwarded to the egress port. Consequently, you need to configure this feature on the ingress port.

For example, you can configure a port so that all ingress frames are assigned a temporary priority level of 5, regardless of the actual priority levels in the frames themselves.

A temporary priority level applies only while a frame traverses the switching matrix of the stack. Tagged frames leave the stack with the same priority level they had upon entering the stack.

### **Examples**

This command sets the temporary priority level to 5 on ports 1.5, 1.8, and 2.12 to 2.15:

```
set switch port=1.5,1.8,2.12-2.15 priority=5
```

This command activates the priority override feature on port 5.6 so that the port applies its temporary priority level to all ingress tagged packets:

```
set switch port=5.6 overridepriority=yes
```



## Section III

# Snooping Protocol

---

This section has the following chapter:

- ❑ Chapter 17, "IGMP Snooping Commands" on page 269



# IGMP Snooping Commands

---

This chapter contains the following commands:

- ❑ “DISABLE IGMP Snooping” on page 270
- ❑ “ENABLE IGMP Snooping” on page 271
- ❑ “SET IP IGMP” on page 272
- ❑ “SHOW IGMP Snooping” on page 275
- ❑ “SHOW IP IGMP” on page 277

---

**Note**

Remember to save your changes with the `SAVE CONFIGURATION` command.

---

---

**Note**

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## DISABLE IGMPSNOOPING

---

### Syntax

```
disable igmpsnooping
```

### Parameters

None.

### Description

This command deactivates IGMP snooping on the stack.

### Example

The following command deactivates IGMP snooping:

```
disable igmpsnooping
```

### Equivalent Command

```
set ip igmp snoopingstatus=disabled
```

For information, refer to “SET IP IGMP” on page 272.

## ENABLE IGMPSNOOPING

---

### Syntax

```
enable igmpsnooping
```

### Parameters

None.

### Description

This command activates IGMP snooping on the stack.

### Example

The following command activates IGMP snooping:

```
enable igmpsnooping
```

### Equivalent Command

```
set ip igmp snoopingstatus=enabled
```

For information, refer to “SET IP IGMP” on page 272.

## SET IP IGMP

---

### Syntax

```
set ip igmp [snoopingstatus=enabled|disabled]
[hoststatus=singlehost|multihost] [timeout=value]
[numbermulticastgroups=value]
[routerport=port|all|none|auto]
```

### Parameters

snoopingstatus	<p>Activates and deactivates IGMP snooping on the stack. The options are:</p> <p>enabled      Activates IGMP snooping.</p> <p>disabled      Deactivates IGMP snooping. This is the default setting.</p>
hoststatus	<p>Specifies the IGMP host node topology. Options are:</p> <p>singlehost    Activates the Single-Host/Port setting, which is appropriate when there is only one host node connected to a port on the stack. This is the default setting.</p> <p>multihost     Activates the Multi-Host setting, which is appropriate if there is more than one host node connected to a stack port.</p>
timeout	<p>Specifies the time period in seconds used by the stack to identify inactive host nodes. A host node is inactive if it has not sent an IGMP report during the specified time interval. The range is from 0 second to 86,400 seconds (24 hours). The default is 260 seconds. If you set the timeout to zero (0), the timer never times out, and the timeout interval is essentially disabled.</p> <p>This parameter also controls the time interval used in determining whether or not a multicast router is still active. The stack makes the determination by watching for queries from the router. If the stack does not detect any queries from a multicast router</p>



during the specified time interval, the router is assumed to be no longer active on the port.

The actual timeout may be ten seconds less than the specified value. For example, at a setting of 25 seconds host nodes or multicast routers could be labeled as inactive after just 15 seconds. A setting of 10 seconds or less could result in the immediate timeout of inactive host nodes or routers.

`numbermulticastgroups`

Specifies the maximum number of multicast addresses the stack can learn. Useful in networks with large numbers of multicast groups, this parameter can be used to protect a stack's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 0 to 255 addresses; the default is 64 addresses.

`routerport`

Specifies the port(s) on the stack connected to a multicast router. Options are:

`port` Specifies the router port(s) manually. Port numbers are specified in the following format:

`module ID.port number`

For instructions, refer to "Port Numbers in Commands" on page 42.

`all` Specifies all of the stack's ports.

`none` Sets the mode to manual without any router ports specified.

`auto` Activates auto-detect, where the stack automatically determines the ports with multicast routers.

## Description

This command configures the IGMP snooping parameters.

### **Examples**

The following command activates IGMP snooping, sets the IGMP topology to Multi-Host, and sets the timeout value to 120 seconds:

```
set ip igmp snoopingstatus=enabled hoststatus=multihost  
timeout=120
```

The following command changes the topology to Single-Host:

```
set ip igmp hoststatus=singlehost
```

The following command disables IGMP snooping:

```
set ip igmp snoopingstatus=disabled
```

### **Equivalent Commands**

```
disable igmpsnooping
```

For information, refer to “DISABLE IGMP SNOOPING” on page 270.

```
enable igmpsnooping
```

For information, refer to “ENABLE IGMP SNOOPING” on page 271.

## SHOW IGMP Snooping

### Syntax

```
show igmpsnooping
```

### Parameters

None.

### Description

This command displays the IGMP parameters. Figure 31 illustrates the information that is displayed by this command.

```
IGMP Snooping Configuration:
IGMP Snooping Status ..... Disabled
Host Topology ..... Single-Host/Port (Edge)
Host/Router Timeout Interval ..... 260 seconds
Maximum IGMP Multicast Groups ..... 64
Router Port(s) ..... Auto Detect

Router List:

VLAN  Port/
ID    Trunk ID          RouterIP      IGMP    Exp.
-----
1     14/-              172.16.01.1  Ver.    time

Host List:
Number of IGMP Multicast Groups: 4

MulticastGroup      VLAN  Port/
ID                  ID    TrunkID  HostIP      IGMP    Exp.
-----
01:00:5E:00:01:01   1     6/-     172.16.10.51 v2        21
01:00:5E:7F:FF:FA   1     5/-     149.35.200.75 v2        11
                   149.35.200.65 v2        65
01:00:5E:00:00:02   1    17/-     149.35.200.69 v2        34
01:00:5E:00:00:09   1    14/-     172.16.10.51 v2        32
```

Figure 31. SHOW IGMP Snooping Command

For an explanation of these parameters, refer to “SET IP IGMP” on page 272 and “SHOW IP IGMP” on page 277.

### **Examples**

The following command displays the current IGMP parameter settings:

```
show igmpsnooping
```

### **Equivalent Command**

```
show ip igmp
```

For information, see “SHOW IP IGMP” on page 277.

## SHOW IP IGMP

---

### Syntax

```
show ip igmp [hostlist] [routerlist]
```

### Parameters

hostlist	Displays a list of the multicast groups the stack has learned, and the stack ports that are connected to host nodes. For this parameter to display information there have to be active host nodes.
routerlist	Displays the ports on the stack where multicast routers are detected. This parameter displays information only when there are active multicast routers.

### Description

This command displays the settings of the IGMP parameters. Figure 32 illustrates the information when the command is entered without the optional parameters.

```
IGMP Snooping Configuration:
IGMP Snooping Status ..... Disabled
Host Topology ..... Single-Host/Port (Edge)
Host/Router Timeout Interval ..... 260 seconds
Maximum IGMP Multicast Groups ..... 64
Router Port(s) ..... Auto Detect
```

Figure 32. SHOW IP IGMP Command

For an explanation of these parameters, refer to “SET IP IGMP” on page 272.

An example of the information displayed by the HOSTLIST parameter is shown in Figure 33.

Number of IGMP Multicast Groups: 4					
MulticastGroup	VLAN ID	Port/TrunkID	HostIP	IGMP Ver	Exp. Time
01:00:5E:00:01:01	1	6/-	172.16.10.51	v2	21
01:00:5E:7F:FF:FA	1	5/-	149.35.200.75	v2	11
			149.35.200.65	v2	65
01:00:5E:00:00:02	1	17/-	149.35.200.69	v2	34
01:00:5E:00:00:09	1	14/-	172.16.10.51	v2	32

Figure 33. SHOW IP IGMP Command with HOSTLIST Parameter

The HOSTLIST parameter displays the following information:

- ❑ Number of IGMP Multicast Groups - The number of IGMP multicast groups with active host nodes on the stack.
- ❑ Multicast Group - The multicast address of the group.
- ❑ VLAN - The VID of the VLAN where the port or trunk is an untagged member.
- ❑ Port/Trunk - The port on the stack where the host node is connected. If the host node is connected to the stack through a trunk, the trunk ID number instead of the port number is displayed.
- ❑ HostIP - The IP address of the host node connected to the port.
- ❑ IGMP Ver. - The version of IGMP being used by the host.
- ❑ Exp. Time - The number of seconds remaining before the host is timed out if no further IGMP reports are received from it.

An example of the information displayed by the ROUTERLIST parameter is shown in Figure 34.

VLAN	Port/Trunk ID	RouterIP
1	14/-	172.16.01.1

Figure 34. SHOW IP IGMP Command with ROUTERLIST Parameter

The ROUTERLIST parameter displays the following information:

- ❑ VLAN - The VID of the VLAN in which the port is an untagged member.
- ❑ Port/Trunk ID - The port on the stack where the multicast router is connected. If the stack learned the router on a port trunk, the trunk ID number instead of the port number is displayed.
- ❑ Router IP - The IP address of the multicast router.

## Examples

The following command displays the current IGMP parameter settings:

```
show ip igmp
```

The following command displays a list of active host nodes connected to the stack:

```
show ip igmp hostlist
```

The following command displays a list of active multicast routers:

```
show ip igmp routerlist
```

## Equivalent Command

```
show igmpsnooping
```

This command does not display the router and host lists. For information, see “SHOW IGMP Snooping” on page 275.





## Section IV

# SNMPv3

---

This section has the following chapter:

- ❑ Chapter 18, "SNMPv3 Commands" on page 283



# SNMPv3 Commands

---

This chapter contains the following commands:

- ❑ “ADD SNMPV3 USER” on page 285
- ❑ “CREATE SNMPV3 ACCESS” on page 287
- ❑ “CREATE SNMPV3 COMMUNITY” on page 290
- ❑ “CREATE SNMPV3 GROUP” on page 292
- ❑ “CREATE SNMPV3 NOTIFY” on page 294
- ❑ “CREATE SNMPV3 TARGETADDR” on page 296
- ❑ “CREATE SNMPV3 TARGETPARAMS” on page 298
- ❑ “CREATE SNMPV3 VIEW” on page 300
- ❑ “DELETE SNMPV3 USER” on page 302
- ❑ “DESTROY SNMPv3 ACCESS” on page 303
- ❑ “DESTROY SNMPv3 COMMUNITY” on page 305
- ❑ “DESTROY SNMPv3 GROUP” on page 306
- ❑ “DESTROY SNMPv3 NOTIFY” on page 307
- ❑ “DESTROY SNMPv3 TARGETADDR” on page 308
- ❑ “DESTROY SNMPv3 TARGETPARMS” on page 309
- ❑ “DESTROY SNMPV3 VIEW” on page 310
- ❑ “PURGE SNMPV3 ACCESS” on page 311
- ❑ “PURGE SNMPV3 COMMUNITY” on page 312
- ❑ “PURGE SNMPV3 NOTIFY” on page 313
- ❑ “PURGE SNMPV3 TARGETADDR” on page 314
- ❑ “PURGE SNMPV3 VIEW” on page 315
- ❑ “SET SNMPV3 ACCESS” on page 316
- ❑ “SET SNMPV3 COMMUNITY” on page 318
- ❑ “SET SNMPV3 GROUP” on page 320
- ❑ “SET SNMPV3 NOTIFY” on page 322
- ❑ “SET SNMPV3 TARGETADDR” on page 324
- ❑ “SET SNMPV3 TARGETPARAMS” on page 326
- ❑ “SET SNMPV3 USER” on page 328
- ❑ “SET SNMPV3 VIEW” on page 330

- ❑ “SHOW SNMPV3 ACCESS” on page 332
- ❑ “SHOW SNMPV3 COMMUNITY” on page 333
- ❑ “SHOW SNMPv3 GROUP” on page 334
- ❑ “SHOW SNMPV3 NOTIFY” on page 335
- ❑ “SHOW SNMPV3 TARGETADDR” on page 336
- ❑ “SHOW SNMPV3 TARGETPARAMS” on page 337
- ❑ “SHOW SNMPV3 USER” on page 338
- ❑ “SHOW SNMPV3 VIEW” on page 339

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

**Note**

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## ADD SNMPV3 USER

---

### Syntax

```
add snmpv3 user=user [authentication=md5|sha]
authpassword=password privpassword=password
[storagetype=volatile|nonvolatile]
```

### Parameters

user	Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.				
authentication	<p>Specifies the authentication protocol that is used to authenticate this user with an SNMP entity (manager or NMS). If you do not specify an authentication protocol, this parameter is automatically set to None. The options are:</p> <table> <tr> <td>md5</td><td>The MD5 authentication protocol. SNMPv3 Users are authenticated with the MD5 authentication protocol after a message is received.</td></tr> <tr> <td>sha</td><td>The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.</td></tr> </table> <p>Note: You must specify the authentication protocol before you specify the authentication password.</p>	md5	The MD5 authentication protocol. SNMPv3 Users are authenticated with the MD5 authentication protocol after a message is received.	sha	The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.
md5	The MD5 authentication protocol. SNMPv3 Users are authenticated with the MD5 authentication protocol after a message is received.				
sha	The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.				
authpassword	Specifies a password of up to 32 alphanumeric characters for the authentication protocol. If you specify an authentication protocol, then you must configure an authentication protocol password.				
privpassword	<p>Specifies a password for the 3DES privacy, or encryption protocol, up to 32 alphanumeric characters. This is an optional parameter.</p> <p>Note: If you specify a privacy password, the privacy protocol is set to DES. You must also specify an authentication protocol and password.</p>				
storagetype	<p>Specifies the storage type of this table entry. This is an optional parameter. The options are:</p> <table> <tr> <td>volatile</td><td>Does not allow you to save the table</td></tr> </table>	volatile	Does not allow you to save the table		
volatile	Does not allow you to save the table				

entry to the configuration file on the master switch. This is the default.

**nonvolatile** Allows you to save the table entry to the configuration file on the stack.

### Description

This command creates an SNMPv3 User Table entry.

### Examples

The following command creates an SNMPv3 user with the name “steven142” with an authentication protocol of MD5, an authentication password of “99doublesecret12”, a privacy password of “encrypt178” and a storage type of nonvolatile.

```
add snmpv3 user=steven142 authentication=md5
authpassword=99doublesecret12 privpassword=encrypt178
storagetype=nonvolatile
```

The following command creates an SNMPv3 user with the name “77hoa” an authentication protocol of SHA, an authentication password of “youvegottobekidding88” and a storage type of nonvolatile.

```
add snmpv3 user=77hoa authentication=sha
authpassword=youvegottobekidding88 storagetype=nonvolatile
```

## CREATE SNMPV3 ACCESS

---

### Syntax

```
create snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] readview=readview writeview=writeview
notifyview=notifyview [storagetype=volatile|nonvolatile]
```

### Parameters

access	Specifies the name of the security group, up to 32 alphanumeric characters.
securitymodel	Specifies the security model. The options are: <ul style="list-style-type: none"> <li>v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.</li> <li>v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.</li> <li>v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.</li> </ul>
securitylevel	Specifies the security level. The options are: <ul style="list-style-type: none"> <li>noauthentication This option provides no authentication protocol and no privacy protocol.</li> <li>authentication This option provides an authentication protocol, but no privacy protocol.</li> </ul>
privacy	This option provides an authentication protocol and the privacy protocol.
readview	Specifies a Read View Name that allows the users assigned to this Group Name to view the information specified by the View Table entry. This is an optional parameter. If you do not assign a value to this parameter, then the readview parameter defaults to none.
writeview	Specifies a Write View Name that allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This is an optional parameter. If you do not assign a value to this parameter, then the writeview parameter defaults to none.

notifyview	Specifies a Notify View Name that allows the users assigned to this Group Name to send traps permitted in the specified View. This is an optional parameter. If you do not assign a value to this parameter, then the notifyview parameter defaults to none.	
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the stack.

### Description

This command creates an SNMPv3 Access Table entry.

### Examples

The following command creates a security group called “testengineering” with a security model of SNMPv3 and a security level of privacy. The security group has a read view named “internet,” a write view named private, and a notify view named “internet.” The storage type is nonvolatile storage.

```
create snmpv3 access=testengineering securitymodel=v3
securitylevel=privacy readview=internet writeview=private
notifyview=internet storage=nonvolatile
```

The following command creates a security group called “swengineering” with a security model of SNMPv3 and a security level of authentication. In addition, the security group has a read view named “internet,” a write view named experimental, and a notify view named “mgmt” (management). The storage type group is nonvolatile storage.

```
create snmpv3 access=swengineering securitymodel=v3
securitylevel=authentication readview=internet
writeview=experimental notifyview=mgmt storage=nonvolatile
```

The following command creates a security group called “hwengineering” with a security model of SNMPv3 and a security level of noauthentication. In addition, the security group has a read view named “internet.”

```
create snmpv3 access=hwengineering securitymodel=v3
securitylevel=authentication readview=internet
```



---

**Note**

In the above example, the storage type has not been specified. As a result, the storage type for the hwengineering security group is volatile storage.

---

## CREATE SNMPV3 COMMUNITY

---

### Syntax

```
create snmpv3 community index=index
communityname=communityname securityname=securityname
transporttag=transporttag
[storagetype=volatile|nonvolatile]
```

### Parameters

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.				
communityname	Specifies a password for this community entry, up to 32 alphanumeric characters.				
securityname	Specifies the name of an SNMPv1 and SNMPv2 user, up to 32 alphanumeric characters.				
transporttag	Specifies the transport tag, up to 32 alphanumeric characters. This is an optional parameter.				
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <table data-bbox="760 1087 1429 1289"> <tr> <td>volatile</td><td>Does not allow you to save the table entry to the configuration file on the stack. This is the default.</td></tr> <tr> <td>nonvolatile</td><td>Allows you to save the table entry to the configuration file on the stack.</td></tr> </table>	volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.	nonvolatile	Allows you to save the table entry to the configuration file on the stack.
volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.				
nonvolatile	Allows you to save the table entry to the configuration file on the stack.				

### Description

This command creates an SNMPv3 Community Table entry.

### Examples

The following command creates an SNMP community with an index of 1213 and a community name of “sunnyvale145.” The user is “chitra34” and the transport tag is “testengtag.” The storage type for this community is nonvolatile storage.

```
create snmpv3 community index=1213
communityname=sunnyvale145 securityname=chitra34
transporttag=testengtag storagetype=nonvolatile
```

The following command creates an SNMP community with an index of 95 and a community name of "12sacramento49." The user is "regina" and the transport tag "trainingtag." The storage type for this community is nonvolatile storage.

```
create snmpv3 community index=95  
communityname=12sacramento49 securityname=regina  
transporttag=trainingtag storagetype=nonvolatile
```

## CREATE SNMPV3 GROUP

---

### Syntax

```
create snmpv3 group username=username
[securitymodel=v1|v2c|v3] groupname=groupname
[storagetype=volatile|nonvolatile]
```

### Parameter

username	Specifies a user name configured in the SNMPv3 User Table.						
securitymodel	Specifies the security model of the above user name. The options are: <table> <tr> <td>v1</td><td>Associates the Security Name, or User Name, with the SNMPv1 protocol.</td></tr> <tr> <td>v2c</td><td>Associates the Security Name, or User Name, with the SNMPv2c protocol.</td></tr> <tr> <td>v3</td><td>Associates the Security Name, or User Name, with the SNMPv3 protocol.</td></tr> </table>	v1	Associates the Security Name, or User Name, with the SNMPv1 protocol.	v2c	Associates the Security Name, or User Name, with the SNMPv2c protocol.	v3	Associates the Security Name, or User Name, with the SNMPv3 protocol.
v1	Associates the Security Name, or User Name, with the SNMPv1 protocol.						
v2c	Associates the Security Name, or User Name, with the SNMPv2c protocol.						
v3	Associates the Security Name, or User Name, with the SNMPv3 protocol.						
groupname	Specifies a group name configured in the SNMPv3 Access Table with the access parameter. See “CREATE SNMPV3 ACCESS” on page 287.						
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <table> <tr> <td>volatile</td><td>Does not allow you to save the table entry to the configuration file on the stack. This is the default.</td></tr> <tr> <td>nonvolatile</td><td>Allows you to save the table entry to the configuration file on the stack.</td></tr> </table>	volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.	nonvolatile	Allows you to save the table entry to the configuration file on the stack.		
volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.						
nonvolatile	Allows you to save the table entry to the configuration file on the stack.						

### Description

This command creates an SNMPv3 SecurityToGroup Table entry.

### Examples

The following command creates the SNMPv3 SecurityToGroup Table entry for a user named Nancy. The security model is set to the SNMPv3 protocol. The group name, or security group, for this user is the “admin” group. The storage type is set to nonvolatile storage.

```
create snmpv3 group username=Nancy securitymodel=v3  
groupname=admin storagetype=nonvolatile
```

The following command creates the SNMPv3 SecurityToGroup Table entry for a user named princess. The security model is set to the SNMPv3 protocol. The group name, or security group, for this user is the “training” group. The storage type is set to nonvolatile storage.

```
create snmpv3 group username=princess securitymodel=v3  
groupname=training storagetype=nonvolatile
```

## CREATE SNMPV3 NOTIFY

---

### Syntax

```
create snmpv3 notify=notify tag=tag [type=trap|inform]
[storagetype=volatile|nonvolatile]
```

### Parameters

notify	Specifies the name of an SNMPv3 Notify Table entry, up to 32 alphanumeric characters.				
tag	Specifies the notify tag name, up to 32 alphanumeric characters. This is an optional parameter.				
type	Specifies the message type. This is an optional parameter. The options are: <table data-bbox="760 856 1429 1102"> <tr> <td>trap</td><td>Trap messages are sent, with no response expected from another entity (NMS or manager). This is the default.</td></tr> <tr> <td>inform</td><td>Inform messages are sent, with a response expected from another entity (NMS or manager).</td></tr> </table>	trap	Trap messages are sent, with no response expected from another entity (NMS or manager). This is the default.	inform	Inform messages are sent, with a response expected from another entity (NMS or manager).
trap	Trap messages are sent, with no response expected from another entity (NMS or manager). This is the default.				
inform	Inform messages are sent, with a response expected from another entity (NMS or manager).				
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <table data-bbox="760 1218 1429 1428"> <tr> <td>volatile</td><td>Does not allow you to save the table entry to the configuration file on the stack. This is the default.</td></tr> <tr> <td>nonvolatile</td><td>Allows you to save the table entry to the configuration file on the stack.</td></tr> </table>	volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.	nonvolatile	Allows you to save the table entry to the configuration file on the stack.
volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.				
nonvolatile	Allows you to save the table entry to the configuration file on the stack.				

### Description

This command creates an SNMPv3 Notify Table entry.

### Examples

The following command creates the SNMPv3 Notify Table entry called “testengtrap1” and the notify tag is “testengtag1.” The message type is defined as a trap message and the storage type for this entry is nonvolatile storage.

```
create snmpv3 notify=testengtrap1 tag=testengtag1 type=trap
storagetype=nonvolatile
```

The following command creates the SNMPv3 Notify Table entry called “testenginform5” and the notify tag is “testenginformtag5.” The message type is defined as an inform message and the storage type for this entry is nonvolatile storage.

```
create snmpv3 notify=testenginform5 tag=testenginformtag5  
type=inform storagetype=nonvolatile
```

## CREATE SNMPV3 TARGETADDR

---

### Syntax

```
create snmpv3 targetaddr=targetaddr params=params
ipaddress=ipaddress udpport=udpport timeout=timeout
retries=retries taglist=taglist
[storagetype=volatile|nonvolatile]
```

### Parameters

targetaddr	Specifies the name of the SNMP manager, or host, that manages the SNMP activity on the stack, up to 32 alphanumeric characters.				
params	Specifies the target parameters name, up to 32 alphanumeric characters.				
ipaddress	Specifies the IP address of the host.				
udpport	Specifies the UDP port in the range of 0 to 65535. The default UDP port is 162. This is an optional parameter.				
timeout	Specifies the timeout value in milliseconds. The range is 0 to 2,147,483,647 milliseconds, and the default is 1500 milliseconds. This is an optional parameter.				
retries	Specifies the number of times the stack resends an inform message. The default is 3. This is an optional parameter.				
taglist	Specifies a tag or list of tags, up to 256 alphanumeric characters. Use a space to separate entries. This is an optional parameter.				
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <table data-bbox="760 1556 1437 1757"> <tr> <td>volatile</td><td>Does not allow you to save the table entry to the configuration file on the stack. This is the default.</td></tr> <tr> <td>nonvolatile</td><td>Allows you to save the table entry to the configuration file on the stack.</td></tr> </table>	volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.	nonvolatile	Allows you to save the table entry to the configuration file on the stack.
volatile	Does not allow you to save the table entry to the configuration file on the stack. This is the default.				
nonvolatile	Allows you to save the table entry to the configuration file on the stack.				

### Description

This command creates an SNMPv3 Target Address Table entry.



## Examples

In the following command, the name of the Target Address Table entry is "snmphost1." In addition, the params parameter is assigned to "snmpv3manager" and the IP address is 198.1.1.1. The tag list consists of "swengtag," "hwengtag," and "testengtag." The storage type for this table entry is nonvolatile storage.

```
create snmpv3 targetaddr=snmphost1 params=snmpv3manager  
ipaddress=198.1.1.1 taglist=swengtag hwengtag testengtag  
storagetype=nonvolatile
```

In the following command, the name of the Target Address Table entry is snmphost99. The params parameter is "snmpmanager7" and the IP address is 198.1.2.2. The tag list is "trainingtag." The storage type for this table entry is nonvolatile storage.

```
create snmpv3 targetaddr=snmphost99 params=snmpmanager7  
ipaddress=198.1.2.2 taglist=trainingtag  
storagetype=nonvolatile
```

## CREATE SNMPV3 TARGETPARAMS

---

### Syntax

```
create snmpv3 targetparams=targetparams username=username
[securitymodel=v1|v2c|v3] [messageprocessing=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] [storagetype=volatile|nonvolatile]
```

### Parameters

targetparams	Specifies the name of the SNMPv3 Target Parameters Table entry, up to 32 alphanumeric characters.
username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are: <ul style="list-style-type: none"> <li>v1 Associates the User Name, or Security Name, with the SNMPv1 protocol.</li> <li>v2c Associates the User Name, or Security Name, with the SNMPv2c protocol.</li> <li>v3 Associates the User Name, or Security Name, with the SNMPv3 protocol.</li> </ul>
messageprocessing	Specifies the SNMP protocol that is used to process, or send messages. Configure this parameter only if you have selected the SNMPv1 or SNMPv2c protocols as the security model. If you have selected the SNMPv3 protocol as the security model, message processing is automatically set to the SNMPv3 protocol. The options are: <ul style="list-style-type: none"> <li>v1 Messages are processed with the SNMPv1 protocol.</li> <li>v2c Messages are processed with the SNMPv2c protocol.</li> <li>v3 Messages are processed with the SNMPv3 protocol.</li> </ul>

securitylevel	Specifies the security level. The options are:	
	noauthentication	This option provides no authentication protocol and no privacy protocol.
	authentication	This option provides an authentication protocol, but no privacy protocol.
	privacy	This option provides an authentication protocol and the privacy protocol.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the master switch.

## Description

This command creates an SNMPv3 Target Parameters Table entry.

## Examples

In the following command, the Target Parameters Table entry is called "snmpv3mgr13" and user name is "user444." The security model is set to the SNMPv3 protocol. In addition, the security level is set to privacy and the storage type is nonvolatile.

```
create snmpv3 targetparams=snmpv3mgr13 username=user444
securitymodel=v3 securitylevel=privacy
storagetype=nonvolatile
```

In the following command, the Target Parameters Table entry is called "snmpmanager" and the user name is "pat365." The security model is set to SNMPv3 protocol. In addition, the security level is set to authentication and the storage type is nonvolatile.

```
create snmpv3 targetparams=snmpmanager username=pat365
securitymodel=v3 securitylevel=authentication
storagetype=nonvolatile
```

# CREATE SNMPV3 VIEW

---

## Syntax

```
create snmpv3 view=view [subtree=OID|text] mask=mask  
[type=included|excluded]  
[storagetype=volatile|nonvolatile]
```

## Parameters

view	Specifies the name of the view, up to 32 alphanumeric characters.	
subtree	Specifies the view of the MIB Tree. The options are:	
	OID	A numeric value in hexadecimal format.
	text	Text name of the view.
mask	Specifies the subtree mask, in hexadecimal format.	
type	Specifies the view type. This is an optional parameter. The options are:	
	included	Permits a user to view the specified subtree. This is the default.
	excluded	Does not permit a user to view the specified subtree.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the master switch.

## Description

This command creates an SNMPv3 View Table entry.

## Examples

The following command creates an SNMPv3 View Table entry called “internet1” with a subtree value of the Internet MIBs and a view type of

included. The storage type for this table entry is nonvolatile storage.

```
create snmpv3 view=internet1 subtree=internet type=included  
storagetype=nonvolatile
```

The following command creates an SNMPv3 View Table entry called "tcp1" with a subtree value of the TCP/IP MIBs and a view type of excluded. The storage type for this table entry is nonvolatile storage.

```
create snmpv3 view=tcp1 subtree=tcp type=excluded  
storagetype=nonvolatile
```

## DELETE SNMPV3 USER

---

### Syntax

```
delete snmpv3 user=user
```

### Parameters

user	Specifies the name of an SNMPv3 user to delete from the stack.
------	--

### Description

This command deletes an SNMPv3 User Table entry. After you delete an SNMPv3 user from the stack, you cannot recover it.

### Examples

The following command deletes the user named “wilson890.”

```
delete snmpv3 user=wilson890
```

The following command deletes the user named “75murthy75.”

```
delete snmpv3 user=75murthy75
```

## DESTROY SNMPv3 ACCESS

---

### Syntax

```
destroy snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy]
```

### Parameter

access	Specifies an SNMPv3 Access Table entry.
securitymodel	Specifies the security model of the user name specified above. The options are: <ul style="list-style-type: none"> <li>v1      Associates the Security Name, or User Name, with the SNMPv1 protocol.</li> <li>v2c     Associates the Security Name, or User Name, with the SNMPv2c protocol.</li> <li>v3      Associates the Security Name, or User Name, with the SNMPv3 protocol.</li> </ul>
securitylevel	Specifies the security level. The options are: <ul style="list-style-type: none"> <li>noauthentication    This option provides no authentication protocol and no privacy protocol.</li> <li>authentication     This option provides an authentication protocol, but no privacy protocol.</li> <li>privacy              This option provides an authentication protocol and the privacy protocol.</li> </ul>

### Description

This command deletes an SNMPv3 Access Table entry. After you delete an SNMPv3 Access Table entry, you cannot recover it.

### Examples

The following command deletes the SNMPv3 Access Table entry called "swengineering" with a security model of the SNMPv3 protocol and a security level of authentication.

```
destroy snmpv3 access=swengineering securitymodel=v3  
securitylevel=authentication
```

The following command deletes the SNMPv3 Access Table entry called “testengineering” with a security model of the SNMPv3 protocol and a security level of privacy.

```
destroy snmpv3 access=testengineering securitymodel=v3  
securitylevel=privacy
```



## DESTROY SNMPv3 COMMUNITY

---

### Syntax

```
destroy snmpv3 community index=index
```

### Parameter

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.
-------	--

### Description

This command deletes an SNMPv3 Community Table entry. After you delete an SNMPv3 Community Table entry, you cannot recover it.

### Examples

The following command deletes an SNMPv3 Community Table entry with an index of 1001.

```
destroy snmpv3 community index=1001
```

The following command deletes an SNMPv3 Community Table entry with an index of 5.

```
destroy snmpv3 community index=5
```

## DESTROY SNMPv3 GROUP

---

### Syntax

```
destroy snmpv3 group username=username  
[securitymodel=v1|v2c|v3]
```

### Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are: <ul style="list-style-type: none"><li>v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.</li><li>v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.</li><li>v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.</li></ul>

### Description

This command deletes an SNMPv3 SecurityToGroup Table entry. After you delete an SNMPv3 SecurityToGroup Table entry, you cannot recover it.

### Examples

The following command deletes an SNMPv3 User Table entry for a user called Dave with an security model of the SNMPv3 protocol:

```
destroy snmpv3 group username=Dave securitymodel=v3
```

The following command deletes an SNMPv3 User Table entry for a user called May with an security model of the SNMPv3 protocol:

```
destroy snmpv3 group username=May securitymodel=v3
```

## DESTROY SNMPv3 NOTIFY

---

### Syntax

```
destroy snmpv3 notify=notify
```

### Parameter

notify                      Specifies an SNMPv3 Notify Table entry.

### Description

This command deletes an SNMPv3 Notify Table entry. After you delete an SNMPv3 Notify Table entry, you cannot recover it.

### Examples

The following command deletes an SNMPv3 Notify Table entry called "systemtestnotifytrap."

```
destroy snmpv3 notify=systemtestnotifytrap
```

The following command deletes an SNMPv3 Notify Table entry called "engineeringinform1."

```
destroy snmpv3 notify=engineeringinform1
```

## DESTROY SNMPv3 TARGETADDR

---

### Syntax

```
destroy snmpv3 targetaddr=target
```

### Parameter

targetaddr                      Specifies an SNMPv3 Target Address table entry.

### Description

This command deletes an SNMPv3 Target Address Table entry. After you delete an SNMPv3 Target Address Table entry, you cannot recover it.

### Example

The following command deletes an SNMPv3 Address Table entry called “snmpmanager.”

```
destroy snmpv3 targetaddr=snmpmanager
```

## DESTROY SNMPv3 TARGETPARMS

---

### Syntax

```
destroy snmpv3 targetparams=targetparams
```

### Parameter

targetparams	Specifies an SNMPv3 Target Parameters table entry.
--------------	--

### Description

This command deletes an SNMPv3 Target Parameters Table entry. After you delete an SNMPv3 Target Parameters Table entry, you cannot recover it.

### Examples

The following command deletes the SNMPv3 Target Parameters Table entry called "targetparameter1."

```
destroy snmpv3 targetparams=targetparameter1
```

The following command deletes the SNMPv3 Target Parameters Table entry called "snmpmanager."

```
destroy snmpv3 targetparams=snmpmanager
```

## DESTROY SNMPV3 VIEW

---

### Syntax

```
destroy snmpv3 view=view [subtree=OID|text]
```

### Parameters

view	Specifies the name of the view, up to 32 alphanumeric characters.
subtree	Specifies the view subtree view. The options are:  OID    A numeric value in hexadecimal format.  text    Text name of the view.

### Description

This command deletes an SNMPv3 View Table entry. After you delete an SNMPv3 View Table entry, you cannot recover it.

### Examples

The following command deletes the SNMPv3 View Table entry named “experimental.” The subtree value of this table entry is experimental.

```
destroy snmpv3 view=experimental subtree=experimental
```

The following command deletes the SNMPv3 View Table entry named “directory.” The subtree value of this table entry is 1.3.6.1.3.

```
destroy snmpv3 view=directory subtree=1.3.6.1.3
```

## PURGE SNMPV3 ACCESS

---

### Syntax

```
purge snmpv3 access
```

### Parameters

None

### Description

This command resets the SNMPv3 Access Table to its default value by removing all the access table entries. To remove a single entry, use “DESTROY SNMPv3 ACCESS” on page 303.

### Example

The following example removes all the SNMPv3 Access Table entries:

```
purge snmpv3 access
```

## PURGE SNMPV3 COMMUNITY

---

### Syntax

```
purge snmpv3 community
```

### Parameters

None

### Description

This command resets the SNMPv3 Community Table to its default value by removing all the community table entries. To remove a single entry, use “DESTROY SNMPv3 COMMUNITY” on page 305.

### Example

The following example removes all the SNMPv3 Community Table entries:

```
purge snmpv3 community
```



## PURGE SNMPV3 NOTIFY

---

### Syntax

```
purge snmpv3 notify
```

### Parameters

None

### Description

This command resets the SNMPv3 Notify Table to its default value by removing all the notify table entries. To remove a single entry, use “DESTROY SNMPv3 NOTIFY” on page 307.

### Example

The following example removes all the entries from the SNMPv3 Notify Table:

```
purge snmpv3 notify
```

## PURGE SNMPV3 TARGETADDR

---

### Syntax

```
purge snmpv3 targetaddr
```

### Parameters

None

### Description

This command resets the SNMPv3 Target Address Table to its default values by removing all the target address table entries. To remove a single entry, use “DESTROY SNMPv3 TARGETADDR” on page 308.

### Example

The following example removes all the entries from the SNMPv3 Target Address Table:

```
purge snmpv3 targetaddr
```

## PURGE SNMPV3 VIEW

---

### Syntax

```
purge snmpv3 view
```

### Parameters

None

### Description

This command resets the SNMPv3 View Table to its default values by removing all the view table entries. To remove a single entry, use “DESTROY SNMPV3 VIEW” on page 310.

### Example

The following example removes all the entries from the SNMPv3 View Table:

```
purge snmpv3 view
```

## SET SNMPV3 ACCESS

---

### Syntax

```
set snmpv3 access=access [securitymodel=v1|v2c|v3]  
[securitylevel=noauthentication|authentication|  
privacy] readview=readview writeview=writeview  
notifyview=notifyview [storagetype=volatile|nonvolatile]
```

### Parameters

access	Specifies the name of the group, up to 32 alphanumeric characters.
securitymodel	Specifies the security model. Options are: <ul style="list-style-type: none"> <li>v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.</li> <li>v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.</li> <li>v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.</li> </ul>
securitylevel	Specifies the security level. The options are: <ul style="list-style-type: none"> <li>noauthentication This option provides no authentication protocol and no privacy protocol.</li> <li>authentication This option provides an authentication protocol, but no privacy protocol.</li> <li>privacy This option provides an authentication protocol and the privacy protocol.</li> </ul>
readview	Specifies a Read View Name that allows the users assigned to this Group Name to view the information specified by the View Table entry.
writeview	Specifies a Write View Name that allows the users assigned to this Security Group to write, or modify, the information in the specified View Table.
notifyview	Specifies a Notify View Name that allows the users assigned to this Group Name to send traps permitted in the specified View.

storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the master switch.

### Description

This command modifies an SNMPv3 Access Table entry.

### Examples

The following command modifies the group called engineering. The new read view is the Internet MIBs and the storage type is volatile storage.

```
set snmpv3 access=engineering securitymodel=v3
securitylevel=authentication readview=internet
storagetype=volatile
```

The following command modifies the group called training. The read view, write view, and notify view are set to the Internet MIBs. The storage type is nonvolatile storage.

```
set snmpv3 access=training securitymodel=v3
securitylevel=privacy readview=internet writeview=internet
notifyview=internet storagetype=nonvolatile
```

## SET SNMPV3 COMMUNITY

---

### Syntax

```
set snmpv3 community index=index communityname=communityname
securityname=securityname transporttag=transporttag
[storagetype=volatile|nonvolatile]
```

### Parameters

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.				
communityname	Specifies a password of this community, up to 32 alphanumeric characters.				
securityname	Specifies the name of an SNMPv1 and SNMPv2 user, up to 32 alphanumeric characters.				
transporttag	Specifies the transport tag, up to 32 alphanumeric characters.				
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <table data-bbox="760 1050 1429 1287"> <tr> <td>volatile</td><td>Does not allow you to save the table entry to the configuration file on the master switch. This is the default.</td></tr> <tr> <td>nonvolatile</td><td>Allows you to save the table entry to the configuration file on the master switch.</td></tr> </table>	volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.	nonvolatile	Allows you to save the table entry to the configuration file on the master switch.
volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.				
nonvolatile	Allows you to save the table entry to the configuration file on the master switch.				

### Description

This command modifies an SNMPv3 Community Table entry.

### Examples

The following command modifies the community table entry with an index of 1001. The community has a password of “secretpassword98” and a security name of “user451.” The transport tag is set to “sampletag4” and the storage type is set to nonvolatile storage.

```
set snmpv3 community index=1001
communityname=secretpassword98 securityname=user451
transporttag=sampletag4 storagetype=nonvolatile
```

The following command modifies the community table entry with an index of 52. The community has a password of “oldmiss71” and a security name of “jjhuser234.” The transport tag is set to “testtag40.”

```
set snmpv3 community index=52 communityname=oldmiss71  
securityname=jjhuser234 transporttag=testtag40
```

## SET SNMPV3 GROUP

---

### Syntax

```
set snmpv3 group username=username [securitymodel=v1|v2c|v3]
groupname=groupname [storagetype=volatile|nonvolatile]
```

### Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are: <ul style="list-style-type: none"> <li>v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.</li> <li>v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.</li> <li>v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.</li> </ul>
groupname	Specifies a group name configured in the SNMPv3 Access Table.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:
volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the master switch.

### Description

This command modifies an SNMPv3 SecurityToGroup Table entry.

### Examples

The following command modifies the SecurityToGroup Table entry with a user name of “nancy28.” The security model is the SNMPv3 protocol. and the group name is set to engineering.

```
set snmpv3 group username=nancy28 securitymodel=v3
groupname=engineering
```



The following command modifies the SecurityToGroup Table entry with a user name of "nelvid." The security model is the SNMPv3 protocol and the group name "systemtest."

```
set snmpv3 group username=nelvid securitymodel=v3  
groupname=systemtest
```

## SET SNMPV3 NOTIFY

---

### Syntax

```
set snmpv3 notify=notify tag=tag [type=trap|inform]
[storagetype=volatile|nonvolatile]
```

### Parameters

notify	Specifies the name associated with the trap message, up to 32 alphanumeric characters.	
tag	Specifies the notify tag name, up to 32 alphanumeric characters.	
type	Specifies the message type. Options are:	
	trap	Trap messages are sent, with no response expected from the host.
	inform	Inform messages are sent, with a response expected from the host.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the master switch.

### Description

This command modifies an SNMPv3 Notify Table entry.

### Examples

The following command modifies an SNMPv3 Notify Table entry called “systemtesttrap2.” The notify tag is “systemtesttag2” and the message type is a trap message.

```
set snmpv3 notify=systemtesttrap2 tag=systemtesttag2
type=trap
```

The following command modifies an SNMPv3 Notify Table entry called "systemtestinform5." The notify tag is "systemtestinform5tag" and the message type is an inform message.

```
set snmpv3 notify=systemtestinform5 tag=systemtestinform5tag  
type=inform
```

## SET SNMPV3 TARGETADDR

---

### Syntax

```
set snmpv3 targetaddr=targetaddr params=params
ipaddress=ipaddress udpport=udpport timeout=timeout
retries=retries taglist=taglist
[storagetype=volatile|nonvolatile]
```

### Parameters

targetaddr	Specifies the name of the SNMP entity (NMS or manager) that manages the SNMP activity on the stack, up to 32 alphanumeric characters.				
params	Specifies the target parameters name, up to 32 alphanumeric characters. This is an optional parameter.				
ipaddress	Specifies the IP address of the host. This is an optional parameter.				
udpport	Specifies the UDP port in the range of 0 to 65535. The default UDP port is 162. This is an optional parameter.				
timeout	Specifies the timeout value in milliseconds. The range is 0 to 2,147,483,647 milliseconds, and the default is 1500 milliseconds. This is an optional parameter.				
retries	Specifies the number of times the stack retries to send an inform message. The default is 3. This is an optional parameter.				
taglist	Specifies a tag or list of tags, up to 256 alphanumeric characters. Use a space to separate entries. This is an optional parameter.				
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <table data-bbox="760 1625 1429 1856"> <tr> <td>volatile</td><td>Does not allow you to save the table entry to the configuration file on the master switch. This is the default.</td></tr> <tr> <td>nonvolatile</td><td>Allows you to save the table entry to the configuration file on the master switch.</td></tr> </table>	volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.	nonvolatile	Allows you to save the table entry to the configuration file on the master switch.
volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.				
nonvolatile	Allows you to save the table entry to the configuration file on the master switch.				

## Description

This command modifies an SNMPv3 Target Address Table entry.

## Examples

The following command modifies the Target Address Table entry with a value of "snmphost." The params parameter is set to "targetparameter7" and the IP address is 198.1.1.1. The taglist is set to "systemtesttraptag" and "systemtestinformtag."

```
set snmpv3 targetaddr=snmphost params=targetparameter7  
ipaddress=198.1.1.1 taglist=systemtesttraptag  
systemtestinformtag
```

The following command modifies the Target Address Table entry with a value of "host." The params parameter is set to "targetparameter22" and the IP address is 198.1.1.198. The taglist is set to "engineeringtraptag" and "engineeringinformtag."

```
set snmpv3 targetaddr=host params=targetparameter22  
ipaddress=198.1.1.198 taglist=engineeringtraptag  
engineeringinformtag
```

## SET SNMPV3 TARGETPARAMS

---

### Syntax

```
set snmpv3 targetparams=targetparams username=username
[securitymodel=v1|v2c|v3] [messageprocessing=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] [storagetype=volatile|nonvolatile]
```

### Parameters

targetparams	Specifies the target parameters name, up to 32 alphanumeric characters.
username	Specifies the user name.
securitymodel	Specifies the security model of the above user name. The options are: <ul style="list-style-type: none"> <li>v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.</li> <li>v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.</li> <li>v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.</li> </ul>
messageprocessing	Specifies the SNMP protocol that is used to process, or send messages. Configure this parameter only if you have selected the SNMPv1 or SNMPv2c protocols as the security model. If you have selected the SNMPv3 protocol as the security model, message processing is automatically set to the SNMPv3 protocol. The options are: <ul style="list-style-type: none"> <li>v1 Messages are processed with the SNMPv1 protocol.</li> <li>v2c Messages are processed with the SNMPv2c protocol.</li> <li>v3 Messages are processed with the SNMPv3 protocol.</li> </ul>
securitylevel	Specifies the security level. The options are: <ul style="list-style-type: none"> <li>noauthentication This option provides no authentication protocol and no privacy protocol.</li> </ul>

authentication	This option provides an authentication protocol, but no privacy protocol.
privacy	This option provides an authentication protocol and the privacy protocol.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:
volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the master switch.

### Description

This command modifies a Target Parameters Table entry.

### Examples

The following command modifies the Target Parameters Table entry called "host23." The user name is "user7990" and the security model is the SNMPv3 protocol. The security level is set to the privacy level.

```
set snmpv3 targetparams=host23 username=loan1
securitymodel=v3 securitylevel=privacy
```

The following command modifies the Target Parameters Table entry called "manager9". The user name is "loan1" and the security model is the SNMPv3 protocol. The security level is set to the authentication protocol.

```
set snmpv3 targetparams=manager9 username=loan1
securitymodel=v3 securitylevel=authentication
```

## SET SNMPV3 USER

---

### Syntax

```
set snmpv3 user=user [authentication=md5|sha]
authpassword=password privpassword=password
[storagetype=volatile|nonvolatile]
```

### Parameters

user	Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.				
authentication	Specifies the authentication protocol that is used to authenticate this user with an SNMPv3 entity (or NMS). The default is no authentication. The options are: <table> <tr> <td>md5</td><td>The MD5 authentication protocol. Users are authenticated with the MD5 authentication protocol after a message is received.</td></tr> <tr> <td>sha</td><td>The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.</td></tr> </table>	md5	The MD5 authentication protocol. Users are authenticated with the MD5 authentication protocol after a message is received.	sha	The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.
md5	The MD5 authentication protocol. Users are authenticated with the MD5 authentication protocol after a message is received.				
sha	The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.				
authpassword	Specifies a password for the authentication protocol, up to 32 alphanumeric characters.				
privpassword	Specifies a password for the 3DES privacy, or encryption protocol, up to 32 alphanumeric characters. Configuring a privacy protocol password, turns on the DES privacy protocol.				
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <table> <tr> <td>volatile</td><td>Does not allow you to save the table entry to the configuration file on the master switch. This is the default.</td></tr> <tr> <td>nonvolatile</td><td>Allows you to save the table entry to the configuration file on the master switch.</td></tr> </table>	volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.	nonvolatile	Allows you to save the table entry to the configuration file on the master switch.
volatile	Does not allow you to save the table entry to the configuration file on the master switch. This is the default.				
nonvolatile	Allows you to save the table entry to the configuration file on the master switch.				



## Description

This command modifies an SNMPv3 User Table entry.

## Examples

The following command modifies a User Table entry called "atiuser104". The authentication protocol is set to the MD5 protocol and the authentication password is "atlanta45denver." The DES privacy protocol is on and the privacy password is "denvertoatlanta3."

```
set snmpv3 user=atiuser104 authentication=md5  
authpassword=atlanta45denver privpassword=denvertoatlanta3
```

The following command modifies a User Table entry called "atiuser104." The authentication protocol is set to the MD5 protocol and the authentication password is "nycbostonwash56." The privacy protocol is on and the privacy password is "bostontoamherst7." The storage type is set to nonvolatile storage.

```
set snmpv3 user=atiuser104 authentication=md5  
authpassword=nycbostonwash56 privpassword=bostontoamherst7  
storagetype=nonvolatile
```

## SET SNMPV3 VIEW

---

### Syntax

```
set snmpv3 view=view [subtree=OID|text] mask=mask
[type=included|excluded]
[storagetype=volatile|nonvolatile]
```

### Parameters

view	Specifies the name of the view, up to 32 alphanumeric characters.
subtree	Specifies the view subtree view. Options are: <ul style="list-style-type: none"> <li>OID    A numeric value in hexadecimal format.</li> <li>text    Text name of the view.</li> </ul>
mask	Specifies the subtree mask, in hexadecimal format.
type	Specifies the view type. Options are: <ul style="list-style-type: none"> <li>included    Permits the user assign to this View Name to see the specified subtree.</li> <li>excluded    Does not permit the user assigned to this View Name to see the specified subtree.</li> </ul>
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: <ul style="list-style-type: none"> <li>volatile    Does not allow you to save the table entry to the configuration file on the master switch. This is the default.</li> <li>nonvolatile    Allows you to save the table entry to the configuration file on the master switch.</li> </ul>

### Description

This command modifies an SNMPv3 View Table entry.

### Examples

The following command modifies the view called “internet1.” The subtree is set to the Internet MIBs and the view type is included.

```
set snmpv3 view=internet1 subtree=internet type=included
```

The following command modifies the view called system. The subtree is set to 1.3.6.1.2.1 (System MIBs) and the view type is excluded.

```
set snmpv3 view=system subtree=1.3.6.1.2.1 type=excluded
```

## SHOW SNMPV3 ACCESS

---

### Syntax

```
show snmpv3 access=access
```

### Parameter

**access** Specifies an SNMPv3 Access Table entry.

### Description

This command displays the SNMPv3 Access Table. You can display one or all of the table entries.

### Examples

The following command displays the SNMPv3 Access Table entry called “production.”

```
show snmpv3 access=production
```

The following command displays all of the SNMPv3 Access Table entries:

```
show snmpv3 access
```

## SHOW SNMPV3 COMMUNITY

---

### Syntax

```
show snmpv3 community index=index
```

### Parameter

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.
-------	--

### Description

This command displays the SNMPv3 Community Table. You can display one or all of the SNMPv3 Community Table entries.

### Examples

The following command displays the Community Table entry with an index of 246:

```
show snmpv3 community index=246
```

The following command displays all of the Community Table entries:

```
show snmpv3 community
```

## SHOW SNMPv3 GROUP

---

### Syntax

```
show snmpv3 group username=username  
[securitymodel=v1|v2c|v3]
```

### Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are: <ul style="list-style-type: none"><li>v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.</li><li>v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.</li><li>v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.</li></ul>

### Description

This command displays SNMPv3 SecurityToGroup Table entries. You can display one or all of the table entries.

### Example

The following command displays the SNMPv3 SecurityToGroup Table entry for a user named Dave who is assigned a security model of the SNMPv3 protocol.

```
show snmpv3 group username=Dave securitymodel=v3
```

The following command displays all of the SNMPv3 SecurityToGroup Table entries:

```
show snmpv3 group
```

## SHOW SNMPV3 NOTIFY

---

### Syntax

```
show snmpv3 notify=notify
```

### Parameter

notify                      Specifies an SNMPv3 Notify Table entry.

### Description

This command displays SNMPv3 Notify Table entries. You can display one or all of the table entries.

### Examples

The following command displays the SNMPv3 Notify Table entry called "testengtrap1":

```
show snmpv3 notify=testengtrap1
```

The following command displays all of the SNMPv3 Notify Table entries:

```
show snmpv3 notify
```

## SHOW SNMPV3 TARGETADDR

---

### Syntax

```
show snmpv3 targetaddr=targetaddr
```

### Parameter

targetaddr                      Specifies an SNMPv3 Target Address Table entry.

### Description

This command displays SNMPv3 Target Address Table entries. You can display one or all of the table entries.

### Examples

The following command displays the SNMPv3 Target Address Table entry called “snmpv3host55”:

```
show snmpv3 targetaddr=snmpv3host55
```

The following command displays all of the SNMPv3 Target Address Table entries:

```
show snmpv3 targetaddr
```



## SHOW SNMPV3 TARGETPARAMS

---

### Syntax

```
show snmpv3 targetparams=targetparams
```

### Parameter

**targetparams** Specifies an SNMPv3 Target Parameters Table entry.

### Description

This command displays SNMPv3 Target Parameters Table entries. You can display one or all of the table entries.

### Examples

The following command displays the SNMPv3 Target Parameters Table entry called "snmpv3manager95":

```
show snmpv3 targetparams=snmpv3manager95
```

The following command displays all of the SNMPv3 Target Parameters Table entries:

```
show snmpv3 targetparams
```

## SHOW SNMPV3 USER

---

### Syntax

```
show snmpv3 user=user
```

### Parameters

*user* Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.

### Description

This command displays SNMPv3 User Table entries. You can display one or all of the table entries.

### Examples

The following command displays the SNMPv3 User Table entry for a user name of Robert:

```
show snmpv3 user=Robert
```

The following command displays all of the SNMPv3 User Table entries:

```
show snmpv3 user
```

## SHOW SNMPV3 VIEW

---

### Syntax

```
show snmpv3 view=view [subtree=OID|text]
```

### Parameter

view	Specifies an SNMPv3 View Table entry.
subtree	Specifies the view subtree view. Options are:  OID    A numeric value in hexadecimal format.  text    Text name of the view.

### Description

This command displays the SNMPv3 View Table entries. You can display one or all of the table entries.

### Examples

The following command displays the SNMPv3 View Table entry called "snmpv3manager95":

```
show snmpv3 targetparams=snmpv3manager95
```

The following command displays all the SNMPv3 View Table entries:

```
show snmpv3 targetparams
```



## Section V

# Spanning Tree Protocols

---

The chapters in this section contain the commands for the spanning tree protocols. The chapters include:

- ❑ Chapter 19, “Spanning Tree Protocol Commands” on page 343
- ❑ Chapter 20, “Rapid Spanning Tree Protocols Commands” on page 357



## Chapter 19

# Spanning Tree Protocol Commands

---

This chapter contains the following commands:

- ❑ “ACTIVATE STP” on page 344
- ❑ “DISABLE STP” on page 345
- ❑ “ENABLE STP” on page 346
- ❑ “PURGE STP” on page 347
- ❑ “SET STP” on page 348
- ❑ “SET STP PORT” on page 351
- ❑ “SET SWITCH MULTICASTMODE” on page 353
- ❑ “SHOW STP” on page 355

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

**Note**

For overview information on the spanning tree protocol (STP), refer to the *AT-S63 Management Software Features Guide*.

---

## ACTIVATE STP

---

### Syntax

```
activate stp
```

### Parameters

None.

### Description

This command designates STP as the active spanning tree on the stack. You cannot enable STP or configure its parameters until you have designated it as the active spanning tree with this command. Only one spanning tree protocol, STP, RSTP, or MSTP, can be active on the stack at a time.

### Example

```
activate stp
```



## DISABLE STP

---

### Syntax

```
disable stp
```

### Parameters

None.

### Description

This command disables the Spanning Tree Protocol on the stack. The default setting for STP is disabled. To view the current status of STP, refer to “SHOW STP” on page 355.

### Example

```
disable stp
```

## ENABLE STP

---

### Syntax

```
enable stp
```

### Parameters

None.

### Description

This command enables the Spanning Tree Protocol on the stack. The default setting for STP is disabled. To view the current status of STP, refer to “SHOW STP” on page 355.

---

#### Note

You cannot enable STP until after you have activated it with “ACTIVATE STP” on page 344.

---

### Example

```
enable stp
```

## PURGE STP

---

### Syntax

```
purge stp
```

### Parameters

None.

### Description

This command returns all STP bridge and port parameters to the default settings. STP must be disabled in order for you to use this command. To disable STP, see “DISABLE STP” on page 345.

### Example

```
purge stp
```

### Equivalent Command

```
set stp default
```

For information, see “SET STP” on page 348.

## SET STP

---

### Syntax

```
set stp [default] [priority=priority] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
```

### Parameters

**default** Disables STP and returns all bridge and port STP settings to the default values. This parameter cannot be used with any other command parameter and can only be used when STP is disabled. (This parameter performs the same function as the PURGE STP command.)

**priority** Specifies the priority number for the bridge. This number is used in determining the root bridge for STP. 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. The range is divided into sixteen increments, as shown in Table 10. You specify the increment that represents the desired bridge priority value. The default value is 32,768 (increment 8).

Table 10. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

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, all links may not have had time to adapt to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.
maxage	Specifies the length of time 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 20, all bridges delete current configuration messages after 20 seconds. 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  $(2 \times (\text{forwarddelay} - 1))$ .

---

**Description**

This command sets the following STP parameters:

- ☐ Bridge priority
- ☐ Hello time
- ☐ Forwarding delay
- ☐ Maximum age time

This command can also disable STP and return the STP parameters to their default settings.

---

**Note**

You can use this command only if STP is designated as the active spanning tree protocol on the stack. See "ACTIVATE STP" on page 344.

---

### **Examples**

This command sets the stack's bridge priority value to 45,056 (increment 11):

```
set stp priority=11
```

This command sets the hello time to 7 seconds and the forwarding delay to 25 seconds:

```
set stp hellotime=7 forwarddelay=25
```

This command returns all of the stack's STP parameters to the default values:

```
set stp default
```

### **Equivalent Command**

```
purge stp
```

For information, see "PURGE STP" on page 347.

## SET STP PORT

---

### Syntax

```
set stp port=port [pathcost|portcost=auto|portcost]
[portpriority=portpriority]
```

### Parameters

port	Specifies the port you want to configure. You can configure more than one port at a time. Port numbers must be specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
pathcost <b>or</b> portcost	Specifies the port’s cost. The parameters are equivalent. The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost to the root bridge for that LAN. This parameter can take the range of 1 to 65,535, or AUTO. The default setting is AUTO, for Automatic Update, which automatically sets port cost according to the speed of the port. Table 11 lists the STP port costs with Auto-Detect.

Table 11. STP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	100
100 Mbps	10
1000 Mbps	4

Table 12 lists the STP port costs with Auto-Detect when a port is part of a port trunk.

Table 12. Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	4
100 Mbps	4
1000 Mbps	1

**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 13. You specify the increment of the desired value. The default is 128 (increment 8).

Table 13. Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

### Description

This command configures the following STP parameter settings for a stack port:

- ☐ Port cost
- ☐ Port priority

### Examples

This command sets the port cost to 15 and the port priority to 192 (increment 12) for port 2.6:

```
set stp port=2.6 portcost=15 portpriority=12
```

This command sets the port cost to auto-detect on ports 4.7 to 4.10:

```
set stp port=4.7-4.10 portcost=auto
```



## SET SWITCH MULTICASTMODE

---

### Syntax

```
set switch multicastmode=[a|b|c|d]
```

### Parameter

multicast mode	Specifies the multicast mode. The options are:
a	Discards all ingress spanning tree BPDU and 802.1x EAPOL packets on all ports.
b	Forwards ingress spanning tree BPDU and 802.1x EAPOL packets across all VLANs and ports.
c	Forwards ingress BPDU and EAPOL packets only among the untagged ports of the VLAN where the ingress port is a member.
d	Forwards ingress BPDU and EAP packets on both tagged and untagged ports of the VLAN where the ingress port is a member.

### Description

This command controls the behavior of the stack when forwarding ingress spanning tree BPDU packets and 802.1x port-based access control EAPOL packets when these features are disabled on the stack. Note the following when setting this parameter:

- ☐ The mode is set at the stack level. You cannot configure it on a per-switch or per-port basis.
- ☐ A stack can have only one mode active at a time.
- ☐ The mode setting applies to spanning tree protocol BPDUs when STP, RSTP, and MSTP are disabled on the stack.
- ☐ The mode setting applies to 802.1x port-based access control EAPOL packets when 802.1x is disabled.
- ☐ There are four possible states: A, B, C, and D:

**A** - Discards all ingress spanning tree BPDU and 802.1x EAPOL packets on all ports. The stack behaves as follows:

- ☐ If STP, RSTP, and MSTP are disabled, all ingress BPDUs are discarded.
- ☐ If 802.1x port-based access control is disabled, all ingress EAPOL packets are discarded.

**B** - Forwards ingress spanning tree BPDU and 802.1x EAPOL packets across all VLANs and ports. This is the default setting. The stack behaves as follows:

- ❑ If STP, RSTP, and MSTP are disabled, ingress BPDUs are flooded on all ports.
- ❑ If STP, RSTP, MSTP, and 802.1x are disabled on the stack, BPDUs and EAPOL packets are flooded on all ports.
- ❑ If the stack is running STP or RSTP and 802.1x is disabled, EAPOL packets are flooded on all ports, except ports in the blocking state.
- ❑ If the stack is running MSTP and 802.1x is disabled, EAPOL packets are flooded on all ports, including ports in the blocking state.

**C** - Forwards ingress BPDU and EAPOL packets only on untagged ports of the VLAN where the ingress port is a member. Packets are not forwarded from tagged ports. The VLAN is identified by the PVID assigned to the ingress port.

**D** - Forwards ingress BPDU and EAP packets from both tagged and untagged ports of the VLAN where the ingress port is a member. The VLAN is identified by the PVID assigned to the ingress port.

### Example

The following command sets the stack's mode to A, blocking all ingress BPDUs and 802.1 EAPOL packets:

```
set switch multicastmode=a
```

## SHOW STP

---

### Syntax

```
show stp [port=port]
```

### Parameter

**port** Specifies the port whose STP parameters you want to view. You can view more than one port at a time. Port numbers must be specified in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command displays the current values for the STP parameters. An example of the display is shown in Figure 35.

```
Status ..... Enabled
Bridge Priority ..... 32768 (In multiples of 4096: 8)
Bridge Hello Time ..... 2/2 (Configured/Actual)
Bridge Forwarding Delay ..... 15/15 (Configured/Actual)
Bridge Max Age ..... 20/20 (Configured/Actual)
Bridge Identifier ..... 32768/00:21:46:A7:B4:11
Root Bridge ..... 32768/00:21:46:A7:B4:11
Root Path Cost ..... 0
```

Figure 35. SHOW STP Command

The bridge priority, bridge hello time, and bridge max age parameters display two values when STP is enabled on the stack (for example, Bridge Forwarding Delay .. 15/15). The first number is the configured value on the stack for the parameter and the second is the value the stack obtained from the root bridge and is actually using for the parameter. The stack displays only the configured values when spanning tree is not activated on the stack.

The Status parameter displays whether STP is enabled or disabled on the stack.

For definitions of the bridge priority, hello time, forwarding delay, and max age parameters, refer to “SET STP” on page 348.

The bridge Identifier parameter consists of the stack's bridge priority value and MAC address, separated by a slash (/). To change the stack's priority value, refer to “SET STP” on page 348. The MAC address of the stack cannot be changed.

The root bridge parameter specifies the bridge identifier of the root bridge of the spanning tree domain. The identifier consists of the bridge priority value and MAC address of the root switch, separated by a slash (/). This parameter only appears when STP is activated on the stack.

The root path cost parameter displays the path cost from the stack to the root bridge of the spanning tree domain. If the stack is the root bridge, the path cost is 0. This parameter only appears when STP is activated on the stack.

The PORT parameter allows you to view the STP parameter settings for the stack ports: An example of the display is shown in Figure 36.

Port	State	Cost	Priority
1.1	Forwarding	4	128
1.2	Forwarding	4	128
1.3	Forwarding	4	128
1.4	Forwarding	4	128
1.5	Forwarding	4	128
1.6	Forwarding	4	128
1.7	Forwarding	4	128
1.8	Forwarding	4	128
1.9	Forwarding	4	128
1.10	Forwarding	4	128
1.11	Forwarding	4	128

Figure 36. SHOW STP PORT Command

The columns are defined here:

- ❑ Port is the port number.
- ❑ State is the current state of a port. The possible states are Listening, Learning, Forwarding, or Blocking when spanning tree is enabled on the stack. When spanning tree is not enabled on the stack or if a port is not being used, its state will be disabled.
- ❑ Cost is the port cost of the port.
- ❑ Priority is the port's priority value. The number is used as a tie breaker when two or more ports have equal costs to the root bridge.

### Examples

This command displays the stack's STP settings:

```
show stp
```

This command displays the STP settings for ports 2.1 to 2.4:

```
show stp port=2.1-2.4
```

## Chapter 20

# Rapid Spanning Tree Protocols Commands

---

This chapter contains the following commands:

- ❑ “ACTIVATE RSTP” on page 358
- ❑ “DISABLE RSTP” on page 359
- ❑ “ENABLE RSTP” on page 360
- ❑ “PURGE RSTP” on page 361
- ❑ “SET RSTP” on page 362
- ❑ “SET RSTP PORT” on page 365
- ❑ “SHOW RSTP” on page 368

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

**Note**

For overview information on the rapid spanning tree protocol (RSTP), refer to the *AT-S63 Management Software Features Guide*.

---

## ACTIVATE RSTP

---

### Syntax

```
activate rstp
```

### Parameters

None.

### Description

This command designates RSTP as the active spanning tree on the stack. After selecting RSTP as the active spanning tree, you can enable or disable it with the ENABLE RSTP and DISABLE RSTP commands. RSTP is active on a stack only after you have designated it as the active spanning tree with this command and enabled it with the ENABLE RSTP command.

Only one spanning tree protocol, STP, RSTP, or MSTP, can be active on the stack at a time.

### Example

```
activate rstp
```

## DISABLE RSTP

---

### Syntax

```
disable rstp
```

### Parameters

None.

### Description

This command disables the Rapid Spanning Tree Protocol on the stack. To view the current status of RSTP, use “SHOW RSTP” on page 368.

### Example

The following command disables RSTP:

```
disable rstp
```

## ENABLE RSTP

---

### Syntax

```
enable rstp
```

### Parameters

None.

### Description

This command enables the Rapid Spanning Tree Protocol on the stack. The default setting for RSTP is disabled. To view the current status of RSTP, use “SHOW RSTP” on page 368.

You cannot enable RSTP until you have activated it with the ACTIVATE RSTP command.

### Example

The following command enables RSTP:

```
enable rstp
```



## PURGE RSTP

---

### Syntax

```
purge rstp
```

### Parameters

None.

### Description

This command returns all 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 RSTP” on page 359.

### Example

The following command resets RSTP:

```
purge rstp
```

### Equivalent Command

```
set rstp default
```

For information, refer to “SET RSTP” on page 362.

## SET RSTP

---

### Syntax

```
set rstp [default] [priority=priority] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
[rstptype|forceversion=stpcompatible|
forcestpcompatible|normalrstp]
```

### Parameters

- 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 RSTP command.)
- 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. The range is divided into sixteen increments, as shown in Table 14. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 14. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

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.
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  $(2 \times (\text{forwarddelay} - 1))$ .

rstptype <i>or</i> forceversion	Sets the RSTP mode. The parameters are equivalent. The options are:
stpcompatible <i>or</i> forcestpcompatible	The bridge uses the RSTP parameter settings, but transmits only STP BPDU packets from the ports. These options are equivalent.
normalrspt	The bridge uses RSTP. It transmits RSTP BPDU packets, except on ports connected to bridges running STP. This is the default setting.

**Description**

This command configures the following RSTP parameter settings.

- ☐ Bridge priority
- ☐ Hello time

- ☐ Forwarding delay
- ☐ Maximum age time
- ☐ Port priority
- ☐ Force version of STP or normal RSTP

This command can also return the RSTP parameters to their default settings.

---

**Note**

You can use this command only if RSTP is the active spanning tree protocol on the stack. See “ACTIVATE RSTP” on page 358.

---

**Examples**

The following command sets the bridge priority to 20480 (increment 5), the hello time to 5 seconds, and the forwarding delay to 20 seconds:

```
set rstp priority=5 hellotime=5 forwarddelay=20
```

The following command uses the FORCEVERSION parameter to configure the bridge to use the RSTP parameters but to transmit only STP BPDU packets:

```
set rstp forceversion=stpcompatible
```

The following command returns all RSTP parameter settings to their default values:

```
set rstp default
```

**Equivalent Command**

```
purge rstp
```

For information, see “PURGE RSTP” on page 361.

## SET RSTP PORT

---

### Syntax

```
set rstp port=port [pathcost|portcost=cost|auto]
[portpriority=portpriority]
[edgeport=yes|no|on|off|true|false]
[ptp|pointtopoint=yes|no|on|off|true|false|autoupdate]
[migrationcheck=yes|no|on|off|true|false]
```

### Parameters

**port** Specifies the port you want to configure. You can specify more than one port at a time. Port numbers are specified in the following format:

`module ID.port number`

For instructions, refer to “Port Numbers in Commands” on page 42.

**pathcost *or* portcost** Specifies the port’s cost. The parameters are equivalent. 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 number 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 15 lists the port cost with auto-detect.

Table 15. RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 16 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 16. RSTP Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
1000 Mbps	2,000

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 17. You specify the increment that corresponds to the desired value. The default is 128, which is increment 8.

Table 17. Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

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. This is the default. |
| no, off, false | The port is not an edge port. The options are equivalent.                  |

ptp <i>or</i> pointtopoint	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.
autoupdate	The port's status is determined automatically. This is the default.
migrationcheck	Enables and disables migration check. The purpose of this feature is to change from the RSTP mode to the STP mode if STP BPDU packets are received on the selected port. When you enable this option, the bridge will send out RSTP BPDU packets from the selected port until STP BPDU packets are received. The port will remain in the RSTP mode until it receives an STP BPDU packet. The options are:
yes, on, true	Enable migration check. The options are equivalent.
no, off, false	Disable migration check. The options are equivalent.

## Description

This command sets a port's RSTP settings.

## Examples

This command sets the port cost to 1,000,000 and port priority to 224 (increment 14) on port 2.4:

```
set rstp port=2.4 portcost=1000000 portpriority=14
```

This command specifies ports 1.6 to 1.8 as not edge ports:

```
set rstp port=1.6-1.8 edgeport=no
```

## SHOW RSTP

---

### Syntax

```
show rstp [portconfig=port|portstate=port]
```

### Parameters

portconfig	Displays the RSTP port settings. You can specify more than one port at a time.
portstate	Displays the RSTP port status. You can specify more than one port at a time.

### Description

You can use this command to display the RSTP parameter settings. An example of the display is shown in Figure 37.

```
Status ..... Enabled
Force Version ..... NormalRSTP
Bridge Priority ..... 32768 (In multiples of 4096: 8)
Bridge Hello Time ..... 2/2 (Configured/Actual)
Bridge Forward Delay ..... 15/15 (Configured/Actual)
Bridge Max Age ..... 20/20 (Configured/Actual)
Bridge Identifier ..... 32768/00:21:46:A7:B4:11
Root Bridge Identifier ..... 32768/00:21:46:A7:B4:11
Root Path Cost ..... 0
```

Figure 37. Example of the SHOW RSTP Command

The bridge priority, bridge hello time, and bridge max age parameters will have two values if RSTP is enabled on the stack (for example, Bridge Forwarding .. 15/15). The first number is the configured value on the stack for the parameter and the second is the value the stack obtained from the root bridge and is currently using for the parameter. The stack displays only the configured values for these parameters if spanning tree is not enabled on the stack.

The Status parameter displays whether STP is enabled or disabled on the stack.

For definitions of the force version, bridge priority, hello time, forward delay, and max age parameters, refer to “SET RSTP” on page 362.

The bridge Identifier parameter consists of the stack’s bridge priority value and MAC address, separated by a slash (/). To change the stack’s priority value, refer to “SET RSTP” on page 362. The MAC address of the stack cannot be changed.



The root bridge identifier parameter displays the bridge priority value and MAC address of the root switch of the spanning tree domain. The values are separated by a slash (/). This parameter only appears when RSTP is activated on the stack.

The root path cost parameter displays the path cost from the stack to the root bridge of the spanning tree domain. If the stack is the root bridge, the path cost is 0. This parameter only appears when RSTP is activated on the stack.

The PORTCONFIG parameter displays the current RSTP parameter settings for the ports. An example is shown in Figure 38.

Port	Edge-Port	Point-to-Point	Cost	Priority
1.1	Yes	Auto Update	Auto Update	128
1.2	Yes	Auto Update	Auto Update	128
1.3	Yes	Auto Update	Auto Update	128
1.4	Yes	Auto Update	Auto Update	128
1.5	Yes	Auto Update	Auto Update	128
1.6	Yes	Auto Update	Auto Update	128
1.7	Yes	Auto Update	Auto Update	128
1.8	Yes	Auto Update	Auto Update	128
1.10	Yes	Auto Update	Auto Update	128
1.11	Yes	Auto Update	Auto Update	128

Figure 38. Example of the SHOW RSTP PORTCONFIG Command

For definitions of these parameters, refer to “SET RSTP PORT” on page 365.

The PORTSTATE parameter displays the current operating settings and status of the ports. An example is shown in Figure 39.

Port	State	Role	Edge	P2P	Version	Port-Cost
1.1	Disabled	-----				
1.2	Forwarding	Designated	No	Yes	RSTP	200000
1.3	Forwarding	Designated	No	Yes	RSTP	200000
1.4	Forwarding	Designated	No	Yes	RSTP	200000
1.5	Forwarding	Designated	No	Yes	RSTP	200000
1.6	Forwarding	Designated	No	Yes	RSTP	200000
1.7	Forwarding	Designated	No	Yes	RSTP	200000
1.8	Forwarding	Designated	No	Yes	RSTP	200000
1.9	Forwarding	Designated	No	Yes	RSTP	200000
1.10	Forwarding	Designated	No	Yes	RSTP	200000
1.11	Forwarding	Designated	No	Yes	RSTP	200000

Figure 39. Example of the SHOW RSTP PORTSTATE Command

The information displayed by the command is as follows:

- ❑ Port — The port number.
- ❑ State — The RSTP state of the port. The possible states for a port connected to another device running RSTP are Discarding and Forwarding.

The possible states for a port connected to a device running STP are Listening, Learning, Forwarding, and Blocking.

The possible states for a port not being used or where spanning tree is not activated is Disabled.

- ❑ Role — The RSTP role of the port. Possible roles are:

Root - The port is connected to the root switch, directly or through other switches, with the least path cost.

Alternate - The port offers an alternate path to the root switch.

Backup - The port on a designated switch that provides a backup for the path provided by the designated port.

Designated - The port has the least cost path to the root switch.

- ❑ 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

This command displays the bridge's RSTP settings:

```
show rstp
```

This command displays the RSTP port settings for ports 3.1 to 3.4:

```
show rstp portconfig=3.1-3.4
```

This command displays RSTP port status for port 4.15:

```
show rstp portstate=4.15
```

## Section VI

# Virtual LANs

---

This section has the following chapter:

- ❑ Chapter 21, “Port-based and Tagged VLAN Commands” on page 373



## Chapter 21

# Port-based and Tagged VLAN Commands

---

This chapter contains the following commands:

- ❑ “ADD VLAN” on page 374
- ❑ “CREATE VLAN” on page 376
- ❑ “DELETE VLAN” on page 379
- ❑ “DESTROY VLAN” on page 382
- ❑ “SET SWITCH INFILTERING” on page 383
- ❑ “SET VLAN” on page 384
- ❑ “SHOW VLAN” on page 385

---

**Note**

Remember to use the SAVE CONFIGURATION command to save your changes on the stack.

---

---

**Note**

For overview information on port-based and tagged VLANs, refer to the *AT-S63 Management Software Features Guide*.

---

## ADD VLAN

---

### Syntax 1

```
add vlan=name [vid=vid] ports=ports|all
frame=untagged|tagged
```

### Syntax 2

```
add vlan=name [vid=vid] taggedports=ports|all
untaggedports=ports|all
```

### Parameters

vlan	Specifies the name of the VLAN to modify.
vid	Specifies the VID of the VLAN you want to modify. This parameter is optional.
ports	Specifies the ports to be added to the VLAN. Port numbers are entered in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
frame	Identifies the new ports as either tagged or untagged. This parameter must be used with the PORTS parameter.
taggedports	Specifies the ports to be added as tagged ports to the VLAN. To include all ports on the stack as tagged ports in the VLAN, use ALL.
untaggedports	Specifies the ports to be added as untagged ports to the VLAN. Specifying ALL adds all ports on the stack as untagged ports to the VLAN.

### Description

This command adds tagged and untagged ports to an existing port-based or tagged VLAN.

---

#### Note

To initially create a VLAN, see “CREATE VLAN” on page 376. To remove ports from a VLAN, see “DELETE VLAN” on page 379.

---

This command has two syntaxes. Either syntax can be used to add ports to a VLAN. The difference between the two is that Syntax 1 can add only one type of port, tagged or untagged, at a time to a VLAN, while Syntax 2 can add both in the same command. This is illustrated in Examples below.

When you add an untagged port to a VLAN, the port is automatically removed from its current untagged VLAN assignment, because a port can be an untagged member of only one VLAN at a time. For example, if you add port 4 as an untagged port to a VLAN, it is automatically removed from whichever VLAN it is currently an untagged member.

Adding a tagged port to a VLAN does not change the port's current tagged and untagged VLAN assignments, because this type of port can belong to more than one VLAN at a time. For instance, if you add port 6 as an tagged port to a new VLAN, it remains a tagged and untagged member of its other VLAN assignments.

### Examples

The following command uses Syntax 1 to add ports 2.4 and 2.7 as untagged members to a VLAN called Sales:

```
add vlan=sales ports=2.4,2.7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
add vlan=sales untaggedports=2.4,2.7
```

The following command uses Syntax 1 to add port 4.3 as a tagged member to a VLAN called Production:

```
add vlan=production ports=4.3 frame=tagged
```

The following command does the same thing using Syntax 2:

```
add vlan=production untaggedports=4.3
```

Adding both tagged and untagged ports to a VLAN using Syntax 1 takes two commands, one command for each port type. For example, if you had a VLAN called Service and you wanted to add port 5.5 as a tagged port and ports 1.7 and 1.8 as untagged ports, the commands would be:

```
add vlan=Service ports=5.5 frame=tagged
```

```
add vlan=Service ports=1.7,1.8 frame=untagged
```

Using Syntax 2, you can add both types of ports with just one command:

```
add vlan=Service untaggedports=1.7,1.8 taggedports=5.5
```

## CREATE VLAN

---

### Syntax 1

```
create vlan=name vid=vid [type=port] ports=ports|all
frame=untagged|tagged
```

### Syntax 2

```
create vlan=name vid=vid [type=port] taggedports=ports|all
untaggedports=ports|all
```

### Parameters

vlan	<p>Specifies a name of up to 20 alphanumeric characters for the new VLAN. A VLAN must have a name. It should reflect the function of the member nodes of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).</p> <p>The name cannot be the same as an existing VLAN on the stack.</p> <p>If the VLAN is unique in your network, then the name should be unique as well. If the VLAN spans multiple switches or stacks, then the name of the VLAN should be the same on each switch or stack.</p>
vid	<p>Specifies a VLAN identifier. The range is 2 to 4094. A VLAN must have a VID. You cannot use the VID 1, which is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the stack.</p> <p>If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches or stacks, then the VID value for the VLAN should be the same on each switch or stack. For example, if you are creating a VLAN called Sales that spans three stacks, assign the Sales VLAN the same VID value on each stack.</p>
type	<p>Specifies the type of VLAN to be created. The option PORT signifies a port-based or tagged VLAN. This parameter is optional.</p>



ports	<p>Specifies the ports on the stack that are tagged or untagged members of the new VLAN. This parameter must be followed by the FRAME parameter. Port numbers are specified in the following format:</p> <pre>module ID.port number</pre> <p>For instructions, refer to “Port Numbers in Commands” on page 42.</p>
frame	<p>Specifies whether the ports of the VLAN are to be tagged or untagged. This parameter must be used with the PORTS parameter.</p>
taggedports	<p>Specifies the tagged ports for the VLAN. To specify all ports on the stack, use ALL. Omit this parameter if the VLAN does not contain tagged ports.</p>
untaggedports	<p>Specifies the untagged ports for the VLAN. To specify all ports on the stack, use ALL. Omit this parameter if the VLAN does not contain untagged ports.</p>

### Description

This command creates port-based and tagged VLANs. It has two syntaxes. You can use either syntax to create a VLAN. The difference between the two is how the member ports of the VLAN are specified. Syntax 1 can create a VLAN with either tagged or untagged ports, but not both. Alternatively, Syntax 2 can create a VLAN that has both types of ports. This is illustrated in the Examples section below.

When you create a new VLAN, the untagged ports of the VLAN are automatically removed from their current untagged VLAN assignment, because a port can be an untagged member of only one VLAN at a time. For example, creating a new VLAN with untagged Ports 2.1 to 2.4 automatically removes these ports from whichever VLAN they are currently untagged members.

The PVID of an untagged port is automatically changed to match the VID number of the VLAN where it is added. For instance, if you add port 4 as an untagged member of a VLAN with a VID of 15, the PVID for port 4 is automatically changed to 15.

Tagged ports of the new VLAN remain as tagged and untagged members of their current VLAN assignments. No change is made to a tagged port's current VLAN assignments, other than its addition to the new VLAN. This is because a tagged port can belong to more than one VLAN at a time. For example, if you add port 1.6 as a tagged port to a new VLAN, the port remains a member of its other current untagged and tagged VLAN

assignments.

### Examples

The following command uses Syntax 1 to create a port-based VLAN called Sales with a VID of 3. The VLAN consists of ports 1.4 to 1.8 and ports 2.12 to 2.16. All ports will be untagged ports in the VLAN:

```
create vlan=Sales vid=3 ports=1.4-1.8,2.12-2.16
frame=untagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan=Sales vid=3 untaggedports=1.4-1.8,2.12-2.16
```

In the following command, Syntax 1 is used to create a tagged VLAN called Production with a VID of 22. The VLAN consists of two tagged ports, ports 2.3 and 2.6:

```
create vlan=Production vid=22 ports=2.3,2.6 frame=tagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan=Sales vid=22 taggedports=2.3,2.6
```

You cannot use Syntax 1 to create a VLAN containing both untagged and tagged ports. For instance, suppose you wanted to create a VLAN called Service with a VID of 16 and untagged ports 4.1, 4.4, 5.5-5.7 and tagged ports 4.11 and 4.12. Creating this VLAN using Syntax 1 would actually require two commands. You would first need to create the VLAN, specifying either the untagged or tagged ports. As an example, the following command creates the VLAN and specifies the untagged ports:

```
create vlan=Service vid=16 ports=4.1,4.4,5.5-5.7
frame=untagged
```

Then, to add the other ports (in this case tagged ports), you would need to use the ADD VLAN command.

Syntax 2 can create a VLAN of both tagged and untagged ports all in one command. Here is the command that would create our example:

```
create vlan=Service vid=16 untaggedports=4.1,4.4,5.5-5.7
taggedports=4.11-4.12
```

The advantage of Syntax 2 over Syntax 1 is that you can create VLANs containing both types of ports with one rather than two commands.

## DELETE VLAN

---

### Syntax 1

```
delete vlan=name [vid=vid] ports=ports frame=untagged|tagged
```

### Syntax 2

```
delete vlan=name [vid=vid] taggedports=ports  
untaggedports=ports
```

### Parameters

vlan	Specifies the name of the VLAN to be modified.
vid	Specifies the VID of the VLAN to be modified. This parameter is optional.
ports	Specifies the ports to be removed from the VLAN. This parameter must be used with the FRAME parameter. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
frame	Identifies the ports to be removed as tagged or untagged. This parameter must be used with the PORT parameter.
taggedports	Specifies the tagged ports to be removed from the VLAN.
untaggedports	Specifies the untagged ports to be removed from the VLAN.

### Description

This command removes tagged and untagged ports from a port-based or tagged VLAN.

This command has two syntaxes. You can use either command to delete ports from a VLAN. The difference between the two is that Syntax 1 can remove only one type of port, tagged or untagged, at a time from a VLAN, while Syntax 2 allows you to remove both port types in the same command. This is illustrated in the Examples section below.

**Note**

To delete a VLAN, see “DESTROY VLAN” on page 382.

**Note**

You cannot change a VLAN’s name or VID.

When you remove an untagged port from a VLAN, the following happens:

- ❑ The port is returned to the Default\_VLAN as an untagged port.
- ❑ If the port is also a tagged member of other VLANs, those VLAN assignments are not changed. The port remains a tagged member of the other VLANs. For example, if you remove Port 4 from a VLAN, the port is automatically returned as an untagged port to the Default VLAN. If Port 4 is functioning as a tagged member in one or more other VLANs, it remains as a tagged member of those VLANs.
- ❑ If you remove an untagged port from the Default\_VLAN without assigning it to another VLAN, the port is excluded as an untagged member from all VLANs on the stack.

When you remove a tagged port from a VLAN, all of its other tagged and untagged VLAN assignments remain unchanged.

**Examples**

The following command uses Syntax 1 to delete untagged ports 1.4 and 2.7 from a VLAN called Sales:

```
delete vlan=sales ports=1.4,2.7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
delete vlan=sales untaggedports=1.4,2.7
```

The following command uses Syntax 1 to delete tagged port 5.12 from a VLAN called Production:

```
delete vlan=production ports=5.12 frame=tagged
```

The following command does the same thing using Syntax 2:

```
delete vlan=production untaggedports=5.12
```

To delete both tagged and untagged ports from a VLAN using Syntax 1 takes two commands. For example, if you had a VLAN called Service and you wanted to delete tagged port 1.2 and untagged ports 5.6 to 5.8, the commands would be:

```
delete vlan=Service ports=1.2 frame=tagged
```

```
delete vlan=Service ports=5.6-5.8 frame=untagged
```

Using Syntax 2, you can do the whole thing with just one command:

```
delete vlan=Service untaggedports=5.6-5.8 taggedports=1.2
```

## DESTROY VLAN

---

### Syntax

```
destroy vlan=name|vid|all
```

### Parameters

**vlan** Specifies the name or VID of the VLAN to be deleted. To delete all VLANs, use the ALL option.

### Description

This command deletes port-based VLANs from the stack. You can use the command to delete selected VLANs or all the VLANs on the stack. Note the following before using this command:

- ❑ You cannot delete the Default\_VLAN.
- ❑ You cannot delete a VLAN if it has a routing interface. You must first delete the interface from the VLAN. To delete an interface, refer to “DELETE IP INTERFACE” on page 397.
- ❑ All untagged ports in a deleted VLAN are returned to the Default\_VLAN as untagged ports.
- ❑ Static addresses assigned to the ports of a deleted VLAN become obsolete and should be deleted from the MAC address table. For instructions, refer to “DELETE SWITCH FDB|FILTER” on page 154.

### Examples

The following command deletes the Sales VLAN from the stack:

```
destroy vlan=Sales
```

The following command deletes the Sales VLAN using both the name and the VID:

```
destroy vlan=Sales vid=102
```

The following command deletes all port-based and tagged VLANs on the stack:

```
destroy vlan=all
```

## SET SWITCH INFILTERING

---

### Syntax

```
set switch infiltering=yes|no|on|off|true|false
```

### Parameters

infiltering	Specifies the operating status of ingress filtering. The options are:
yes, on, true	Activates ingress filtering. The options are equivalent. This is the default setting.
no, off, false	Deactivates ingress filtering. The options are equivalent.

### Description

This command controls the status of ingress filtering. When ingress filtering is activated, which is the default setting, tagged frames are filtered when they are received on a port. When ingress filtering is deactivated, tagged frames are filtered before they are transmitted out a port. To view the current setting, use the “SHOW SWITCH” on page 97.

### Example

The following command deactivates ingress filtering:

```
set switch infiltering=off
```

## SET VLAN

---

### Syntax

```
set vlan=name|vid port=ports frame=tagged|untagged
```

### Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
ports	Specifies the port whose VLAN type is to be changed. You can specify more than one port at a time. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
frame	Identifies the new VLAN type for the port. The type can be tagged or untagged.

### Description

This command changes a port's VLAN type. You can use this command to change a tagged port to an untagged port and vice versa.

Note the following before using this command:

- ❑ Changing an untagged port to a tagged port adds the port to the Default\_VLAN as an untagged port.
- ❑ Changing a port in the Default\_VLAN from untagged to tagged results in the port being an untagged member of no VLAN.
- ❑ Changing a port from tagged to untagged removes the port from its current untagged port assignment.

### Examples

The following command changes port 2.4 in the Sales VLAN from tagged to untagged:

```
set vlan=Sales port=2.4 frame=untagged
```



## SHOW VLAN

### Syntax

```
show vlan[=name|vid]
```

### Parameter

vlan                      Specifies the name or VID of the VLAN.

### Description

This command displays the VLANs on the stack. An example of the information displayed by this command for port-based and tagged VLANs is shown in Figure 40.

```

VLAN Name ..... Sales
VLAN ID ..... 4
VLAN Type ..... Port Based
Protected Ports ..... No
Untagged Port(s)
    Configured ..... 1.2,2.8-2.12
    Actual ..... 1.2,2.8-2.12
Tagged Port(s) ..... 2.24

VLAN Name ..... Engineering
VLAN ID ..... 5
VLAN Type ..... Port Based
Protected Ports ..... No
Untagged Port(s)
    Configured ..... 4.5-4.7
    Actual ..... 4.5-4.
Tagged Port(s) ..... 2.24

```

Figure 40. SHOW VLAN Command for Port-based and Tagged VLANs

The information displayed by the command is described here:

- ❑ VLAN name - The name of the VLAN.
- ❑ VLAN ID - The ID number assigned to the VLAN.
- ❑ VLAN Type - The type of VLAN. This will be Port Based for port-based and tagged VLANs.
- ❑ Protected Ports - The status of protected ports. Since port-based and tagged VLANs are not protected ports VLANs, this will be No.
- ❑ Untagged port(s) - The untagged ports of the VLAN. The untagged ports are listed as follows.
  - Configured: The untagged ports of the VLAN.

- Actual: The current untagged ports of the VLAN. This applies to 802.1x port-based network access control. Since version 3.0.0 of the AT-S63 Management Software does not support this feature in a stack, you can ignore this field. The ports in the Configured and Actual fields will always be the same.
- ❑ Tagged port(s) - The tagged ports of the VLAN. A tagged port can belong to more than one VLAN at a time.

### Examples

The following command displays all the VLANs on the stack:

```
show vlan
```

The following command displays information on just the Sales VLAN:

```
show vlan=sales
```

The following command displays information for the VLAN with the VID of 22:

```
show vlan=22
```

## Section VII

# Internet Protocol Routing

---

This section has the following chapter:

- ❑ Chapter 22, “Internet Protocol Version 4 Packet Routing Commands” on page 389



# Internet Protocol Version 4 Packet Routing Commands

---

This chapter has the following commands:

- ❑ “ADD IP ARP” on page 390
- ❑ “ADD IP INTERFACE” on page 392
- ❑ “ADD IP ROUTE” on page 394
- ❑ “DELETE IP ARP” on page 396
- ❑ “DELETE IP INTERFACE” on page 397
- ❑ “DELETE IP ROUTE” on page 398
- ❑ “PURGE IP” on page 399
- ❑ “SET IP ARP” on page 400
- ❑ “SET IP ARP TIMEOUT” on page 402
- ❑ “SET IP INTERFACE” on page 403
- ❑ “SET IP LOCAL INTERFACE” on page 405
- ❑ “SET IP ROUTE” on page 406
- ❑ “SHOW IP ARP” on page 408
- ❑ “SHOW IP COUNTER” on page 410
- ❑ “SHOW IP INTERFACE” on page 412
- ❑ “SHOW IP ROUTE” on page 414

---

**Note**

Remember to save your changes with the `SAVE CONFIGURATION` command.

---

---

**Note**

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## ADD IP ARP

---

### Syntax

```
add ip arp=ipaddress interface=interface port=port
ethernet=macaddress
```

### Parameters

arp	Specifies the IP address of the host. The IP address must be a member of a local subnet or network that has a routing interface on the stack.
interface	Specifies the name of the interface from where the host is reached. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).
port	Specifies the physical port on the stack where the host is reached. Port numbers are entered in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
ethernet	Specifies the MAC address of the host. The MAC address can be entered in either of the following formats:  xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

### Description

This command adds a static ARP entry to the ARP cache. This is typically used to add entries for local hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist in the cache. The stack can support up to 1024 static ARP entries.

### Examples

This command adds a static ARP entry for a host with an IP address of 149.42.67.8 and a MAC address of 00:06:5B:BB:72:88. The host is a member of the subnet of the VLAN8-0 interface and is located on port 2.15:

```
add ip arp=149.42.67.8 interface=vlan8-0 port=2.15
ethernet=00:06:5b:bb:72:88
```

This command adds a static ARP entry for a host with an IP address of 149.124.85.14 and a MAC address of 00:06:7A:22:11:A4. The host is located on port 3.6 in the VLAN14-1 interface:

```
add ip arp=149.124.85.14 interface=vlan14-1 port=3.6  
ethernet=00:06:7a:22:11:a4
```

## ADD IP INTERFACE

---

### Syntax

```
add ip interface=interface ipaddress=ipaddress [dhcp|bootp
[mask|netmask=subnetmask] [ripmetric=value]
```

### Parameters

interface	Specifies a name for the new routing interface. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). The range of the interface number is 0 to 15.
ipaddress	<p>Specifies an IP address for the interface. The address must be a unique member of the subnet or network where the interface is to be assigned.</p> <p>You can assign an address manually or activate the DHCP or BOOTP client and have a DHCP or BOOTP server on the network assign the address automatically. When there is more than one interface in a VLAN, only one of the interfaces can obtain its IP address from a DHCP or BOOTP server. The IP addresses of the other interfaces in the same VLAN must be assigned manually.</p>
mask <b>or</b> netmask	<p>Specifies the subnet mask of the IP address of the routing interface. Do not specify a mask if the IP address will be assigned by a DHCP or BOOTP server. The default value is based on the address’ network type. The default values are:</p> <p>Class A address - 255.0.0.0</p> <p>Class B address - 255.255.0.0</p> <p>Class C address - 255.255.255.0</p>

---

### Note

In version 2.0.0, the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths, provided that the “1” bits are consecutive (e.g., 128, 192, 224, etc.).

---

ripmetric	Specifies the cost of crossing the interface for RIP. The range is 1 to 16. The default is 1.
-----------	---



## Description

This command creates a new interface for routing IPv4 packets to a local network or subnet. Note the following before using this command:

- ❑ The VLAN must already exist on the stack.
- ❑ You cannot assign more than one interface to the same local network or subnet on a stack.
- ❑ When there are multiple interfaces within a VLAN, each must be assigned a unique interface number.
- ❑ Only one interface in a VLAN can obtain its IP configuration from a DHCP or BOOTP server.
- ❑ If an interface is configured to use the DHCP or BOOTP client to obtain its IP address and subnet mask, it does not participate in IP routing until its IP address and subnet mask have been obtained from the DHCP or BOOTP server.

## Examples

This command creates an interface with an IP address 149.123.44.56 and a mask of 255.255.255.0. The interface is assigned to the VLAN with the VID of 6 and given the interface number 0. Since no RIP metric is specified, the default value of 1 is applied to the interface:

```
add ip interface=vlan6-0 ipaddress=149.123.44.56
netmask=255.255.255.0
```

This command creates an interface with an IP address 149.211.126.14 and a mask of 255.255.240.0. The interface is assigned to the VLAN with the VID of 24 and given the interface number 2. The RIP hop count for the interface is set to 2:

```
add ip interface=vlan24-2 ipaddress=149.211.126.14
netmask=255.255.240.0 ripmetric=2
```

This command creates an interface with an IP address and subnet mask set by a DHCP server. The interface is assigned to the VLAN with the VID of 18 and given the interface number 1. The hop count for RIP is increased to 4:

```
add ip interface=vlan18-1 ipaddress=dhcp ripmetric=4
```

## ADD IP ROUTE

---

### Syntax

```
add ip route=ipaddress [interface=interface]
nextthop=ipaddress [mask=subnetmask] [metric=value]
[preference=value]
```

### Parameters

route	Specifies the IP address of the destination network, subnet, or node. The IP address for a default route is 0.0.0.0.
interface	<p>Specifies the name of the routing interface where the static route is to be added. To view the interfaces on the stack, refer to “SHOW IP INTERFACE” on page 412.</p> <p>This parameter is optional. The stack automatically determines the appropriate interface by adding a route to the interface whose IP address is a member of the same subnet as the next hop. (An error message is displayed if you try to add a route to an interface whose IP address is a member of a different subnet than the next hop in the route.)</p>
nextthop	Specifies the IP address of the next hop for the route. The next hop’s IP address must be a member of a local subnet on the stack and the subnet must have an interface.
mask	<p>Specifies the subnet mask of the destination IP address of the static route. The default value is based on the address’ network type. The default values are:</p> <p>Class A address - 255.0.0.0</p> <p>Class B address - 255.255.0.0</p> <p>Class C address - 255.255.255.0</p> <p>Do not include a mask for the default route.</p>

---

### Note

In version 2.0.0, the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths, provided that the “1” bits are consecutive (e.g., 128, 192, 224, etc.).

---

metric	Specifies the cost of crossing the route. The range is 1 to 16. The default is 1.
preference	Assigns a preference value to the static route. The stack uses the preference values to select the active routes when there are more than eight static or dynamic routes in the routing table to the same remote destination. The range is 0 to 65535. The lower the value, the higher the preference. The default value for a static route is 60. The default value for the default route is 360.

## Description

This command is used to create new static routes and a default route.

## Examples

This command adds a static route to a remote subnet with the IP address 149.124.55.0 and a mask of 255.255.255.0. The IP address of the next hop is 149.111.12.4. Specifying an interface is unnecessary since the management software automatically adds the route to whichever interface is a member of the same subnet as the next hop:

```
add ip route=149.124.55.0 nexthop=149.111.12.4
mask=255.255.255.0
```

This command adds a static route to a remote subnet with the IP address 149.14.150.0 and the mask 255.255.224.0. The IP address of the next hop is 162.76.44.12. The metric for the route is 5 and the preference is 25:

```
add ip route=162.14.150.0 nexthop=162.76.44.12
mask=255.255.224.0 metric=5 preference=25
```

This command adds a default route. The IP address of the next hop is 172.211.16.12. No mask is specified for a default route. As with a static route, specifying an interface for the default route is unnecessary since the stack automatically adds the route to the interface on the same subnet as the next hop:

```
add ip route=0.0.0.0 nexthop=172.211.16.12
```

## DELETE IP ARP

---

### Syntax

```
delete ip arp=ipaddress
```

### Parameters

arp	Specifies the IP address of the host to be deleted from the ARP cache.
-----	--

### Description

This command deletes static and dynamic ARP entries from the ARP cache. This command can delete only one ARP entry at a time. To view the entries in the cache, refer to “SHOW IP ARP” on page 408.

### Example

This command deletes the ARP entry for a host with the IP address 149.42.67.8:

```
delete ip arp=149.42.67.8
```

## DELETE IP INTERFACE

---

### Syntax

```
delete ip interface=interface
```

### Parameters

interface	Specifies the name of the interface to be deleted from the stack. An interface name consists of "VLAN" followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).
-----------	---

### Description

This command deletes an interface from the stack. You can only delete one interface at a time. To display the names of the existing interfaces, refer to "SHOW IP INTERFACE" on page 412.

Note the following before performing this command:

- ❑ All IPv4 packet routing to the local network or subnet of a deleted interface ceases.
- ❑ All static routes assigned to the interface are deleted from the routing table.
- ❑ Deleting an interface that the AT-S63 Management Software is using to access a network management device (e.g., a RADIUS or syslog server) causes the stack to stop performing the corresponding management function.
- ❑ Deleting the local interface on a stack during a remote Telnet or web browser management session immediately ends the session. To continue managing the stack, you must start a local management session using the Terminal Port on the master switch.

### Examples

This command deletes the VLAN6-2 interface from the stack:

```
delete ip interface=vlan6-2
```

This command deletes an interface using its VLAN name, in this case Sales, instead of the VID:

```
delete ip interface=vlan-Sales-2
```

## DELETE IP ROUTE

---

### Syntax

```
delete ip route=ipaddress [interface=interface]  
nexthop=ipaddress mask=subnetmask
```

### Parameters

route	Specifies the destination IP address of the static, dynamic, or default route to be deleted. The IP address for the default route is 0.0.0.0.
interface	Specifies the name of the interface where the static or dynamic route is assigned. An interface name consists of "VLAN" followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). This parameter is optional.
nexthop	Specifies the IP address of the next hop of the route. The next hop is required when deleting a static or dynamic route, but not when deleting a default route.
mask	Specifies the subnet mask for the destination IP address. The mask for the default route is 255.255.255.255.

### Description

This command deletes static, dynamic, and default routes from the routing table. To display the existing routes, refer to "SHOW IP ROUTE" on page 414.

### Examples

This command deletes the static route to the remote subnet 149.124.55.0 with the subnet mask 255.255.255.0 and the next hop 149.124.22.12

```
delete ip route=149.124.55.0 mask=255.255.255.0  
nexthop=149.124.22.12
```

This command deletes the default route:

```
delete ip route=0.0.0.0 mask=255.255.255.255
```

## PURGE IP

---

### Syntax

```
purge ip
```

### Parameters

None.

### Description

This command deletes all routing interfaces on the stack. Note the following before performing this command:

- ❑ All IPv4 packet routing on the stack ceases. The device, however, continues to switch packets among the ports within the VLANs (but not across the VLAN boundaries) using Layer 2.
- ❑ All static routes are deleted from the route table.
- ❑ The AT-S63 Management Software stops performing those management functions that require access to a network management device (e.g., a RADIUS server).
- ❑ Deleting all interfaces deletes the local interface. This prohibits you from remotely managing the device with a Telnet or SSH client, or with a web browser.
- ❑ Deleting all interfaces during a remote Telnet or web browser management session immediately ends your session. To continue managing the stack, you must start a local management session using the Terminal Port on the master switch.

### Example

This command deletes all routing interfaces on the stack:

```
purge ip interface
```

## SET IP ARP

---

### Syntax

```
set ip arp=ipaddress [interface=interface] [port=port]  
[ethernet=macaddress]
```

### Parameters

arp	Specifies the IP address of the static route entry to be modified.
interface	Specifies the interface where the host is located. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). The interface must already exist on the stack.
port	Specifies the new physical port on the stack where the host is located. Port numbers are entered in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
ethernet	Specifies a new MAC address of the host. The MAC address can be entered in either of the following formats:  xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

### Description

This command modifies an existing static ARP entry in the ARP cache. You can change all of the settings of an entry, except the IP address. To change the IP address, you must delete the entry and add it again. To view the ARP entries, refer to “SHOW IP ARP” on page 408.

### Examples

This command modifies the port number for the static ARP entry with the IP address 149.42.67.8:

```
set ip arp=149.42.67.8 port=24
```



This command changes the MAC address for the static ARP entry with the IP address 149.124.85.14:

```
set ip arp=149.124.85.14 ethernet=00:06:7a:22:11:24
```

## SET IP ARP TIMEOUT

---

### Syntax

```
set ip arp timeout=integer
```

### Parameter

timeout	Specifies the ARP cache timeout value. The range is 150 to 260000 seconds. The default setting is 600 seconds.
---------	--

### Description

This command sets the ARP cache timeout value. The timer prevents the ARP table from becoming full with inactive entries. An entry that is not used for the length of the timeout period is designated as inactive and deleted from the table.

### Example

The following command sets the timer to 400 seconds:

```
set ip arp timeout=400
```

## SET IP INTERFACE

---

### Syntax

```
set ip interface=interface|eth0
[ipaddress=ipaddress|dhcp|bootp] [mask|netmask=subnetmask]
[ripmetric=value]
```

### Parameters

interface	Specifies the name of the routing interface to be modified. An interface name consists of "VLAN" followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). The "eth0" value can be used in place of the interface name to specify the local interface.
ipaddress	Specifies a new IP address for the interface.
mask <b>or</b> netmask	Specifies a new subnet mask for the interface. Do not specify a mask if the IP address is assigned by a DHCP or BOOTP server. To change the subnet mask, you must also include the IP address of the interface. The default value is based on the address' network type. The default values are:  Class A address - 255.0.0.0  Class B address - 255.255.0.0  Class C address - 255.255.255.0

---

#### Note

In version 2.0.0 the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths so long as the "1" bits are consecutive (e.g., 128, 192, 224, etc.).

---

ripmetric	Specifies the new cost of crossing the interface for RIP. The range is 1 to 16. The default is 1.
-----------	---

### Description

This command modifies the IP address, subnet mask and RIP metric attribute of an existing routing interface. To initially create an interface, refer to "ADD IP INTERFACE" on page 392. To view the interfaces, refer to "SHOW IP INTERFACE" on page 412

Note the following before performing this command:

- ❑ Modifying the IP address of a routing interface deletes all static routes assigned to the interface.
- ❑ Modifying the IP address of a routing interface that has RIP removes the routing protocol from the interface and deletes all RIP routes learned on the interface from the routing table.
- ❑ You cannot change the name of a routing interface. You must delete the interface and recreate it to change its VID or interface number.
- ❑ You can specify the local interface two ways. You can specify its interface name (for example, VLAN5-1) or use the “eth0” value. The “0” in the value is not a VID, as in an interface name. Rather, the “eth0” value signifies the local interface. To designate the local interface of a stack, refer to “SET IP LOCAL INTERFACE” on page 405.

### Examples

This command changes the IP address of the VLAN7-0 interface to 149.188.27.55 and the subnet mask to 255.255.255.0:

```
set ip interface=vlan7-0 ipaddress=149.188.27.55
mask=255.255.255.0
```

This command activates the DHCP client on the VLAN 28-5 interface so that it obtain its IP address and subnet mask from a DHCP server:

```
set ip interface=vlan28-5 ipaddress=dhcp
```

This command changes the RIP metric for the VLAN12-0 interface to 2:

```
set ip interface=vlan12-0 ripmetric=2
```

This command changes the IP address and subnet mask of the local interface to 149.24.252.6 and 255.255.240.0, respectively. The example uses “eth0” rather than the interface name to designate the local interface:

```
set ip interface=eth0 ipaddress=149.24.252.6
mask=255.255.240.0
```

## SET IP LOCAL INTERFACE

---

### Syntax

```
set ip local interface=interface|none
```

### Parameters

**interface** Specifies the name of the interface to act as the local interface on the stack. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

Use the NONE option to remove the currently assigned local interface without assigning a new one. The default is no local interface.

### Description

This command specifies the local interface of the stack. The selected interface must already exist on the stack. The local interface is used for enhanced stacking and for remote management of the unit with a Telnet or SSH client, or a web browser. A stack can have only one local interface at a time. To view the interfaces on the stack, refer to “SHOW IP INTERFACE” on page 412.

### Examples

This command specifies the VLAN6-0 interface as the local interface on the stack:

```
set ip local interface=vlan6-0
```

This command specifies the interface with the interface number 2 in the Sales VLAN as the local interface on the stack:

```
set ip local interface=vlan-sales-2
```

This command removes the currently assigned local interface without assigning a new one:

```
set ip local interface=none
```

## SET IP ROUTE

---

### Syntax

```
set ip route=ipaddress [interface=interface]  
nexthop=ipaddress mask=subnetmask [metric=value]  
[preference=value]
```

### Parameters

route	<p>Specifies the IP address of the remote destination of the static route to be modified. The IP address of the default route is 0.0.0.0.</p> <p>You cannot change the destination IP address of a static route. If the destination address changes, you must delete the old route and enter a new route.</p>
interface	<p>Specifies the name of the interface where the next hop is located. To view the interfaces on the stack, refer to “SHOW IP INTERFACE” on page 412.</p> <p>Allied Telesis recommends omitting this optional parameter. The appropriate interface for a static route is determined automatically by the stack when it examines the IP address of the next hop and adds the route to the interface of the same subnet.</p>
nexthop	<p>Specifies the IP address of the next hop of the route. You must specify the next hop even if you are not changing it.</p> <p>If the IP address of the next hop belongs to a different subnet than the original IP address, the stack automatically moves the route to the appropriate interface.</p>
mask	<p>Specifies the subnet mask for the destination IP address. The default value is based of the address' network type. The default values are:</p> <p>Class A address - 255.0.0.0</p> <p>Class B address - 255.255.0.0</p> <p>Class C address - 255.255.255.0</p> <p>Do not include a mask for a default route.</p>

**Note**

In version 2.0.0, the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths, provided that the “1” bits are consecutive (e.g., 128, 192, 224, etc.).

metric	Specifies a new cost for crossing the route. The range is 1 to 16. The default is 1.
preference	Assigns a preference value to the static route. The stack uses the preference values to select the active routes when there are more than eight static or dynamic routes in the routing table to the same remote destination. The range is 0 to 65535. The lower the value, the higher the preference. The default value for a static route is 60. The default value for the default route is 360.

**Description**

This command modifies the attributes of an existing static route or default route. You can use the command to change the IP address of the next hop or the subnet mask of the destination address. The command can also change the metric cost of a route. This command cannot change the destination address. Changing the destination address requires deleting the static route and recreating it with the new address. To view the static routes, refer to “SHOW IP ROUTE” on page 414.

**Examples**

This command changes the IP address of the next hop for the static route to the remote subnet 149.124.55.0. The IP address of the next hop is changed to 149.124.52.4:

```
set ip route=149.124.55.0 nexthop=149.124.52.4
mask=255.255.255.0
```

This command changes the metric value to 7 for the static route to the remote subnet 172.55.156.0:

```
set ip route=172.55.156.0 nexthop=172.55.101.2
mask=255.255.255.0 metric=7
```

This command changes the IP address of the next hop to 149.211.16.12 for the default route:

```
set ip route=0.0.0.0 nexthop=149.211.16.12
```

## SHOW IP ARP

---

### Syntax

```
show ip arp
```

### Parameters

None.

### Description

This command displays the entries in the ARP cache. The ARP cache contains mappings of IP addresses to physical addresses for hosts where the stack has recently routed packets. Figure 41 is an example of the information displayed by this command.

Interface	IP Address	MAC Address	Port	Type
vlan2-0	149.122.34.4	00:06:5B:B2:44:21	2.2	Dynamic
vlan2-0	149.122.34.12	00:A0:D2:18:EE:A1	2.3	Dynamic
vlan2-0	149.122.34.21	00:A0:C3:57:32:14	1.4	Dynamic
vlan8-1	149.122.35.1	00:A0:64:B1:76:A5	1.7	Dynamic

Figure 41. SHOW IP ARP Command

The columns in the display are:

- ❑ Interface - Interface from where the network device is accessed.
- ❑ IP Address - IP address of the node.
- ❑ MAC Address - MAC address of the node.
- ❑ Port - Port on the stack from where the node is accessed.
- ❑ Type - Type of entry. This is one of the following:
  - Static: Static entry added with “ADD IP ARP” on page 390.
  - Dynamic: Entry learned from ARP request/reply exchanges.
  - Invalid: Possible nonexistent entry.
  - Other: Entry automatically generated by the system.

To set the ARP timeout value, refer to “SET IP ARP TIMEOUT” on page 402.



**Example**

This command displays the entries in the ARP cache:

```
show ip arp
```

## SHOW IP COUNTER

---

### Syntax

```
show ip counter [port=ports|all]
```

### Parameters

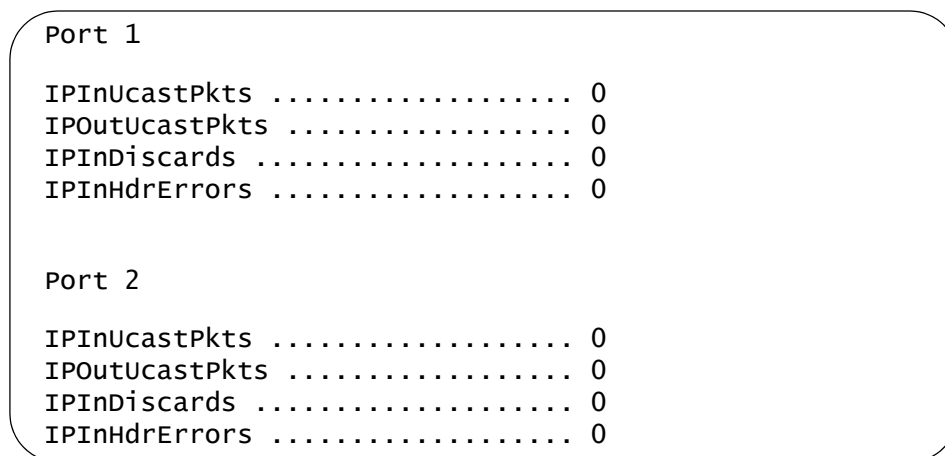
**port** Specifies the ports whose IP statistics you want to view. Omitting this parameter displays the statistics for all the ports. Port numbers are entered in the following format:

```
module ID.port number
```

For instructions, refer to “Port Numbers in Commands” on page 42.

### Description

This command displays Layer 3 counters for the individual ports on a stack. Figure 42 is an example of the information displayed by this command.



```

Port 1
IPInUcastPkts ..... 0
IPOutUcastPkts ..... 0
IPInDiscards ..... 0
IPInHdrErrors ..... 0

Port 2
IPInUcastPkts ..... 0
IPOutUcastPkts ..... 0
IPInDiscards ..... 0
IPInHdrErrors ..... 0

```

Figure 42. SHOW IP COUNTER Command

The lines in the display are:

- ❑ IPInUcastPkts - Number of IP packets received on a port.
- ❑ IPOutUcastPkts - Number of IP packets transmitted from a port.
- ❑ IPInDiscards - Number of IP packets received but discarded due to resource limitations at the IP level.
- ❑ IPInHdrErrors - Number of IP packets received with header errors.

**Examples**

This command displays the statistics for all the ports:

```
show ip counter
```

This command displays the statistics for ports 1.1 to 1.4:

```
show ip counter port=1.1-1.4
```

## SHOW IP INTERFACE

---

### Syntax

```
show ip interface[=interface|eth0]
```

### Parameters

**interface** Specifies the interface name. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). If no interface value is specified, the stack displays all the interfaces.

The “eth0” value can be used to designate the local interface.

### Description

This command displays the routing interfaces on a stack. An example of the information displayed by this command is shown in Figure 43.

Interface	IPAddress	NetMask	RipMet
eth0	149.55.14.8	255.255.255.0	1
vlan2-0	149.123.11.21	255.255.255.0	1
vlan5-0#	149.55.12.15	255.255.255.0	2
vlan8-0	149.55.13.2	255.255.255.0	1
vlan8-1	149.55.14.8	255.255.255.0	1

Figure 43. SHOW IP INTERFACE Command

The local interface of a stack, if one has been designated, is listed twice in the table, as “eth0” at the top of the table and again as a regular entry. For instance, the local interface on the stack in the above example is the VLAN8-1 interface because its values and those of the “eth0” interface are identical. The “eth0” entry contains null values (i.e., 0.0.0.0) if no local interface is designated on the unit.

The columns in the display are:

- ❑ **Interface** - The interface name consisting of the VLAN’s identification (VID) and interface number. A hash symbol (#) marks IP interfaces where there are no active nodes in the VLAN on the stack.
- ❑ **IPAddress** - The interface’s IP address. The address is assigned manually to the interface or automatically by a DHCP or BOOTP server. If the address is 0.0.0.0, the interface is configured to receive

its IP configuration from a DHCP or BOOTP server, but the server has not responded.

- ❑ NetMask - The interface's subnet mask. The subnet mask is assigned manually to the interface or automatically by a DHCP or BOOTP server. If the mask is 0.0.0.0, the DHCP or BOOTP server has not responded.
- ❑ RipMet - The hop count for this interface when routing packets with RIP.

### Examples

This command displays all the routing interfaces on a stack:

```
show ip interface
```

This command displays just the VLAN2-6 interface:

```
show ip interface=vlan2-6
```

## SHOW IP ROUTE

---

### Syntax

```
show ip route [general] [fdb] [full]
```

### Parameters

general	Displays general routing information, such as the total number of routes in the cache and the cache size.
fdb	Displays the status of the static and dynamic routes.
full	Displays both the routes and the general routing information.

### Description

Entering this command without any parameters displays all of the IPv4 interface, static and RIP routes. An example of the information displayed by this command without the parameters is shown in Figure 44.

IP Routes			
Destination	Mask Protocol	NextHop RipMetric	Interface Preference
0.0.0.0	0.0.0.0 Static	202.24.124.2 1	VLAN2-0 60
149.102.34.0	255.255.255.0 Interface	149.211.54.6 1	VLAN14-0 1
149.102.37.0	255.255.255.0 Interface	149.211.54.6 1	VLAN14-0 1

Figure 44. SHOW IP ROUTE Command

The columns are described here:

- ❑ Destination - Destination IP address of the network or subnet. The default route is 0.0.0.0.
- ❑ Mask - Subnet mask of the destination IP address.
- ❑ Protocol - Source of the route. Possible options are:
  - Interface - Route was learned by a routing interface.
  - Static - Route was entered manually as a static route.
  - RIP - Route was learned by RIP.

- ❑ NextHop - IP address of the next hop to the destination network or subnet.
- ❑ RipMetric - RIP metric (cost) to reaching the destination.
- ❑ Interface - Name of the interface where the next hop of the route is located. A hash symbol (#) following the name signifies that the route is physically “down,” meaning there are no active nodes in the VLAN of the interface.
- ❑ Preference - The preference value of the route. The preference value is used by the stack to select a route when there is more than one route to a remote destination.

Though this command always displays interface and static routes, RIP routes are only displayed when the outgoing interface is up. Note that routes are only propagated by RIP when their status at the physical level is up. This means that a VLAN's interface route is propagated if at least one port in the VLAN is active.

The FDB parameter allows you to view the status of the static and RIP routes on the stack. Figure 45 is an example of the information provided by the FDB parameter.

IP FDB			
Destination Installed	Mask Protocol	NextHop RipMetric	Interface Preference
0.0.0.0 Yes	255.255.255.0 Static	149.111.44.22 1	VLAN4-0 60
149.222.66.0 Yes	255.255.255.0 Static	149.111.22.11 1	VLAN2-0 60
149.222.66.0 Yes	255.255.255.0 Static	149.111.44.22 1	VLAN4-0 60
149.222.66.0 Yes	255.255.255.0 Static	149.111.55.17 1	VLAN8-0 60
149.125.10.0 Yes	255.255.255.0 Static	149.111.22.11 1	VLAN2-0 60

Figure 45. SHOW IP ROUTE Command with the FDB Parameter

Most of the information displayed by the FDB parameter is identical to that displayed when the command is entered without any parameters. The difference is the addition of the Installed variable which displays the status of the static and RIP routes, and the default route. (The FDB parameter does not display interface routes.) A route with an Installed status of Yes has been installed by the stack in its routing hardware. The route is ready for use (or is already being used) and meets both of the following conditions:

- ❑ The interface with the next hop of the route is up (i.e., there is at least one active port in the VLAN)
- ❑ There is a static or dynamic ARP entry for the next hop in the routing table.

A route with a status of No has not been installed by the stack in its routing hardware and is not currently being used. Any one of the following conditions can cause a route to have this status:

- ❑ The interface for the next hop of the route is down (i.e., there are no active ports in the VLAN)
- ❑ The ARP table does not contain a static or dynamic entry for the next hop.
- ❑ There are already eight active routes to the same remote destination in the routing table and the route has been placed in the standby mode.

Figure 46 is an example of the information provided by the GENERAL parameter.

```

IP Route General Information
Number of routes..... 25
Interface routes..... 11
RIP routes..... 0
Static routes..... 2
Cache size..... 1024
Source route byte counting ..... no
Route debugging..... no
Multipath routing..... yes

```

Figure 46. SHOW IP ROUTE Command with the GENERAL Parameter

The information displayed by the GENERAL parameter is described here:

- ❑ Number of routes - Total number of routing interfaces, static routes, and dynamic RIP routes.
- ❑ Interface routes - Number of routing interfaces on the stack.
- ❑ RIP routes - Number of routes learned by RIP.
- ❑ Static routes - Number of static routes.
- ❑ Cache size - Size of the route cache (the maximum number of entries)
- ❑ Source route byte counting - Whether source route byte counting is enabled.
- ❑ Route debugging - Whether route debugging is enabled.
- ❑ Multipath routing - Whether ECMP routing is enabled or disabled on the stack.



## Examples

This command displays the IPv4 packet routes on the stack:

```
show ip route
```

This command displays general routing information:

```
add ip route general
```

This command displays both the routes and the general routing information:

```
add ip route full
```



## Section VIII

# Port Security

---

This section has the following chapter:

- ❑ Chapter 23, "802.1x Port-based Network Access Control Commands" on page 421
- ❑ Chapter 24, "RADIUS Commands" on page 447



## Chapter 23

# 802.1x Port-based Network Access Control Commands

---

This chapter contains the following commands:

- ❑ “DISABLE PORTACCESS|PORTAUTH” on page 422
- ❑ “DISABLE RADIUSACCOUNTING” on page 423
- ❑ “ENABLE PORTACCESS|PORTAUTH” on page 424
- ❑ “ENABLE RADIUSACCOUNTING” on page 425
- ❑ “SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR” on page 426
- ❑ “SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT” on page 435
- ❑ “SET RADIUSACCOUNTING” on page 437
- ❑ “SHOW PORTACCESS|PORTAUTH” on page 439
- ❑ “SHOW PORTACCESS|PORTAUTH PORT” on page 441
- ❑ “SHOW RADIUSACCOUNTING” on page 444

---

### Note

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

### Note

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## DISABLE PORTACCESS|PORTAUTH

---

### Syntax

```
disable portaccess|portauth
```

---

### Note

The PORTACCESS and PORTAUTH keywords are equivalent.

---

### Parameters

None.

### Description

This command disables 802.1x Port-based Network Access Control on the switch. This is the default setting.

### Example

The following command disables 802.1x Port-based Network Access Control on the switch:

```
disable portaccess
```

## DISABLE RADIUSACCOUNTING

---

### Syntax

```
disable radiusaccounting
```

### Parameters

None

### Description

This command disables RADIUS accounting on the switch.

### Example

The following command disables RADIUS accounting:

```
disable radiusaccounting
```

### Equivalent Command

```
set radiusaccounting status=disabled
```

For information, see “SET RADIUSACCOUNTING” on page 437.

## ENABLE PORTACCESS|PORTAUTH

---

### Syntax

```
enable portaccess|portauth
```

---

#### Note

The PORTACCESS and PORTAUTH keywords are equivalent.

---

### Parameters

None.

### Description

This command activates 802.1x Port-based Network Access Control on the switch. The default setting for this feature is disabled.

---

#### Note

You should activate and configure the RADIUS client software on the switch before activating port-based access control. Refer to “SET AUTHENTICATION” on page 452.

---

### Example

The following command activates 802.1x Port-based Network Access Control on the switch:

```
enable portaccess
```



## ENABLE RADIUSACCOUNTING

---

### Syntax

```
enable radiusaccounting
```

### Parameters

None

### Description

This command activates RADIUS accounting on the switch.

### Example

The following command activates RADIUS accounting:

```
enable radiusaccounting
```

### Equivalent Command

```
set radiusaccounting status=enabled
```

For information, see “SET RADIUSACCOUNTING” on page 437.

# SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR

## Syntax

```
set portaccess|portauth=8021x|macbased port=port
type|role=authenticator|none [mode=single|multi]
[control=auto|authorised|forceauthenticate|
unauthorised|forceunauthenticate]
[quietperiod=value] [txperiod=value]
[reauthenabed=enabled|disabled] [reauthperiod=value]
[suptimeout=value] [servertimeout|servtimeout=value]
[maxreq=value] [ctrlldirboth=ingress|both]
[piggyback=enabled|disabled] [guestvlan=vlan-name|vid|none]
[vlanassignment=enabled|disabled] [securevlan=on|off]
```

## Parameters

portaccess <b>or</b> portauth	Specifies the authentication method. The two choices are:	
	8021x	Specifies 802.1x username and password authentication. With this authentication method the supplicant must provide, either manually or automatically, a username and password. This authentication method requires 802.1x client software on the supplicant nodes.
	macbased	Specifies MAC address-based authentication. The authenticator port extracts the source MAC address from the initial frames received from a supplicant and automatically sends the address as both the username and password of the supplicant to the authentication server. This authentication method does not require 802.1x client software on the supplicant nodes.
port	Specifies the port to set to the Authenticator role or whose Authenticator settings you want to adjust. You can specify more than one port at a time.	

Port numbers are specified in the following format:

`module ID.port number`

For instructions, refer to “Port Numbers in Commands” on page 42.

type *or*  
role

Specifies the role of the port. The parameters are equivalent. The options are:

authenticator                      Specifies the authenticator role.

none                                  Disables port-based access control on the port.

mode

Controls the operating mode of an authenticator port. The options are:

single                                  Configures the port to accept only one authentication. This authenticator mode should be used together with the piggy-back mode. When an authenticator port is set to the single mode and the piggy-back mode is disabled, only the one client who is authenticated can use the port. Packets from or to other clients on the port are discarded. If piggy-back mode is enabled, other clients can piggy-back onto another client's authentication and so be able to use the port. This is the default setting.

multi                                  Configures the port to accept up to 320 authentications. Every client using an authenticator port in this mode must have a username and password combination and log on separately.

control

Specifies the authenticator state. The options are:

auto                                  Sets the port state to 802.1X port-based authentication. The port begins in the unauthorized state, allowing only EAPOL frames to be sent and received

	through the port. The authentication process begins when the link state of the port changes. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch by using the client's MAC address. This is the default setting.
	<p>authorised <b>or</b> forceauthenticate</p> <p>Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The parameters are equivalent.</p>
	<p>unauthorised <b>or</b> forceunauthenticate</p> <p>Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch blocks all authentication on the port. The parameters are equivalent.</p>
quietperiod	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.
txperiod	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.
reauthenable	Controls whether the client must periodically reauthenticate. The options are:
	<p>enabled</p> <p>Specifies that the client must periodically reauthenticate. This is the default setting. The time period between</p>

	reauthentications is set with the reauthperiod parameter.
disabled	Specifies that reauthentication by the client is not required after the initial authentication. Reauthentication is only required if there is a change to the status of the link between the supplicant and the switch or the switch is reset or power cycled.
reauthperiod	Enables periodic reauthentication of the client, which is disabled by default. The default value is 3600 seconds. The range is 1 to 65,535 seconds.
supptimeout	Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.
servertimeout <b>or</b> servtimeout	Sets the timer used by the switch to determine authentication server timeout conditions. The default value is 30 seconds. The range is 1 to 600 seconds. The parameters are equivalent.
maxreq	Specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The range is 1 to 10 retransmissions and the default is 2.
ctrlldirboth	Specifies how the port is to handle ingress and egress broadcast and multicast packets when in the unauthorized state.

When a port is set to the authenticator role, it remains in the unauthorized state until a client is authenticated by the authentication server. In the unauthorized state, the port accepts only EAP packets from the client. All other ingress packets the port might receive from the supplicant, including multicast and broadcast traffic, are discarded until the supplicant has been authenticated.

You can use this selection to control how an authenticator port handles egress broadcast and multicast traffic when in the unauthorized state. You can instruct the port to forward this traffic to the client, even though the client has not logged on, or you can have the port discard the traffic.

The options are:

- |         |  |
|---------|--|
| ingress | An authenticator port, when in the unauthorized state, discards all ingress broadcast and multicast packets from the client while forwarding all egress broadcast and multicast traffic to the same client. This is the default setting. |
| both    | An authenticator port, when in the unauthorized state, does not forward ingress or egress broadcast and multicast packets from or to the client until the client has logged on.  |

This parameter is only available when the authenticator's operating mode is set to single. When set to multiple, an authenticator port does not forward ingress or egress broadcast or multicast packets until at least one client has logged on.

#### piggyback

Controls who can use the switch port in cases where there are multiple clients using the port, for example the port is connected to an Ethernet hub. This parameter is applicable when the authenticator's operating mode is set to single. The options are:

- |          |  |
|----------|--|
| enabled  | Allows all clients on the port to piggy-back onto the initial client's authentication, causing the port to forward all packets after one client is authenticated. This is the default setting. |
| disabled | Specifies that the switch port forward only those packets from the client who is authenticated and discard packets from all other users.   |

#### guestvlan

Specifies the name or VID of a Guest VLAN. The authenticator port is a member of a Guest VLAN when no supplicant is logged on. Clients do not log on to access a Guest VLAN.

If an authenticator port where a Guest VLAN has been defined starts to receive EAPOL packets, signalling that a supplicant is logging on, it changes to the unauthorized state and moves from the Guest VLAN to its predefined VLAN. The port remains in the unauthorized state until the log on process between the supplicant and the RADIUS server is completed.

The options are:

- vlan-name Specifies the name of the Guest VLAN.
- vlan-id Specifies the VID of the Guest VLAN.
- none Removes a predefined Guest VLAN from an authenticator port.

A Guest VLAN is only supported when the operating mode of the port is set to Single. The specified VLAN must already exist on the switch.

- vlanassignment Specifies whether to use the VLAN assignments entered in the user accounts on the RADIUS server. Options are:
  - enabled Specifies that the authenticator port is to use the VLAN assignments returned by the RADIUS server when a supplicant logs on. This is the default setting.
  - disabled Specifies that the authenticator port ignore any VLAN assignment information returned by the RADIUS server when a supplicant logs on. The authenticator port remains in its predefined VLAN assignment even when the RADIUS server returns a VLAN assignment when a supplicant logs on.
- securevlan Controls the action of an authenticator port to subsequent authentications after the initial authentication where VLAN assignments have been added to the user accounts on the RADIUS server. This parameter only applies when the port is operating in the Multiple operating mode. Options are:
  - on Specifies that only those supplicants with the same VLAN assignment as the initial supplicant are authenticated. Supplicants with a different or no VLAN assignment are denied entry to the port. This is the default setting.
  - off Specifies that all supplicants, regardless of their assigned VLANs, are authenticated. However, the port remains in the VLAN specified in the initial authentication, regardless of the VLAN assignments of subsequent authentications.

## Description

This command sets ports to the authenticator role and configures the authenticator role parameters. This command also removes port-based access control from a port.

## Examples

The following command sets ports 1.4 to 1.6 to the authenticator role. The authentication method is set to 802.1x, meaning that the supplicants must have 802.1x client software and provide a username and password, either automatically or manually, when logging on and during reauthentications. The operating mode is set to Single and the piggy back mode to disabled. With these settings, only one supplicant can use each port. After a supplicant logs on, access by any other client to the same port is denied:

```
set portaccess=8021x port=1.4-1.6 role=authenticator  
mode=single piggyback=disabled
```

The next command is identical to the previous example, except the authentication method is set to MAC address-based, meaning the authenticator ports use the MAC addresses of the supplicants as the usernames and passwords. With MAC address-based authentication, an authenticator port automatically extracts the MAC address from the initial frames received from a supplicant and sends it to the RADIUS server. The supplicants do not need 802.1x client software. Again, as in the previous example, since the operating mode is Single and the piggy back mode is disabled, only one supplicant can use each port.

```
set portaccess=macbased port=1.4-1.6 role=authenticator  
mode=single piggyback=disabled
```

---

### Note

The remaining examples are limited to the 802.1x authentication method, but apply equally to the MAC address-based authentication method.

---

The following command sets port 2.12 to the authenticator role and the operating mode to Single. The difference between this and the previous example is here the piggy back mode is enabled. This feature is useful when authenticator ports support multiple clients and you do not want to give all of the supplicants separate username and password combinations on the RADIUS server. When piggy back is enabled on an authenticator port only one client has to log on for all of the clients to use the port:

```
set portaccess=8021x port=2.12 role=authenticator  
mode=single piggyback=enabled
```



The following command sets port 4.22 to the authenticator role and the operating mode to Multiple. This configuration is also appropriate where there is more than one supplicant on a port. But an authenticator port in the Multiple mode requires that all supplicants have their own username and password combinations on the RADIUS server and that they log on before they can use the authenticator port on the switch:

```
set portaccess=8021x port=4.22 role=authenticator mode=multi
```

The following command assigns the Guest VLAN "Product\_show" to authenticator ports 3.5 and 4.12. The ports function as untagged members of the VLAN and allow any network user access to the VLAN without logging on. However, should a port start to receive EAPOL packets, it assumes that a supplicant is initiating a log on and changes to the unauthorized state. After the log on is completed, the port moves to its predefined VLAN:

```
set portaccess=8021x port=3.5,4.12 role=authenticator
guestvlan=product_show
```

The following command configures port 2.15 as an authenticator port. This example assumes that the user accounts on the RADIUS server have VLAN assignments. With the VLANASSIGNMENT parameter set to enabled, the port processes the VLAN assignments it receives from the RADIUS server. Had this parameter been disabled, the port would ignore the VLAN assignments and leave the port in its predefined VLAN assignment. The VLAN assignment of the port is determined by the initial log on by a client. With the SECUREVLAN parameter set to enabled, only those subsequent supplicants having the same VLAN assignment as the initial supplicant are allowed to use the port:

```
set portaccess=8021x port=2.15 role=authenticator mode=multi
vlanassignment=enabled securevlan=on
```

The following command sets port 1.7 to the authenticator role, the quiet period on the port to 30 seconds, and the server timeout period to 200 seconds:

```
set portaccess=8021x port=1.7 role=authenticator
quietperiod=30 servtimeout=200
```

The following command configures authenticator port 3.11 to the multiple operating mode:

```
set portaccess=8021x port=3.11 role=authenticator mode=multi
```

The following command configures authenticator port 5.17 to the single operating mode and disables piggybacking:

```
set portaccess=8021x port=5.17 role=authenticator
mode=single piggyback=disabled
```

The following command removes port-based access control from ports 4.12 and 4.15:

```
set portaccess port=4.12,4.15 role=none
```

## SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT

---

### Syntax

```
set portaccess|portauth port=port type|role=supplicant|none
[authperiod=value] [heldperiod=value] [maxstart=value]
[startperiod=value] [username|name=name]
[password=password]
```

---

### Note

The PORTACCESS and PORTAUTH keywords are equivalent.

---

### Parameters

port	Specifies the port that you want to set to the supplicant role or whose supplicant settings you want to adjust. You can specify more than one port at a time. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.
type <i>or</i> role	Specifies the role of the port. The parameters are equivalent. The options are:  supplicant      Specifies the supplicant role.  none              Disables port-based access control on the port.
authperiod	Specifies the period of time in seconds that the supplicant will wait for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 300 seconds. The default is 30 seconds.
heldperiod	Specifies the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. After the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535. The default value is 60.
maxstart	Specifies the maximum number of times the supplicant will send EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

startperiod	Specifies the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60. The default is 30.
username <b>or</b> name	Specifies the username for the switch port. The parameters are equivalent. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case-sensitive.
password	Specifies the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case-sensitive.

### Description

This command sets ports to the supplicant role and configures the supplicant role parameters. This command also removes port-based access control on a port.

### Examples

The following command sets ports 5.14 to 5.16 to the supplicant role:

```
set portaccess port=5.14-5.16 role=supplicant
```

The following command sets port 2.8 to the supplicant role, the name to "switch22," and the password to "bluebird":

```
set portaccess port=2.8 role=supplicant name=switch22
password=bluebird
```

The following command removes port-based access control on ports 1.12 and 2.15:

```
set portaccess port=1.12,2.15 role=none
```

## SET RADIUSACCOUNTING

---

### Syntax

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

### Parameters

status	Activates and deactivates RADIUS accounting on the switch. The options are:
enabled	Activates RADIUS accounting. This option is equivalent to “ENABLE RADIUSACCOUNTING” on page 425.
disabled	Deactivates the feature. This is the default. This option is equivalent to “DISABLE RADIUSACCOUNTING” on page 423.
serverport	Specifies the UDP port for RADIUS accounting. The default is port 1813.
type	Specifies the type of RADIUS accounting. The default is Network. This value cannot be changed.
trigger	Specifies the action that causes the switch to send accounting information to the RADIUS server. The options are:
start_stop	The switch sends accounting information whenever a client logs on or logs off the network. This is the default.
stop_only	The switch sends accounting information only when a client logs off.
updateenable	Specifies whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled. If you enable this feature, use the INTERVAL parameter to specify the intervals at which the switch is to send the accounting updates.
interval	Specifies the intervals at which the switch is to send interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

## Description

RADIUS accounting is supported on those switch ports operating in the Authenticator role. The accounting information sent by the switch to a RADIUS server includes the date and time when clients log on and log off, as well as the number of packets sent and received by a switch port during a client session. This feature is disabled by default on the switch.

## Examples

The following command activates RADIUS accounting and sets the trigger to stop only:

```
set radiusaccounting status=enabled trigger=stop_only
```

The following command enables the update feature and sets the interval period to 200 seconds:

```
set radiusaccounting updateenable=enabled interval=200
```

## SHOW PORTACCESS|PORTAUTH

---

### Syntax

```
show portaccess|portauth=8021x|macbased
```

### Parameters

portaccess <b>or</b> portauth	Specifies the authenticator method of the port. Options are:
8021x	Displays information for an 802.1x authenticator port.
macbased	Displays information for a MAC address-based authenticator port.
config	Displays whether port-based access control is enabled or disabled on the switch.
status	Displays the role and status of each port.

### Description

This command displays the port roles. Figure 47 is an example of the information displayed by this command.

802.1x Authentication Information			
-----			
SystemAuthControl.....		Disabled	
Number of 802.1x Supplicants.....		0 (480)	
Port	Role	Supplicant Mode	Protocol Version
-----			
1.1	Authenticator	Single	1
1.2	Authenticator	Single	1
1.3	Authenticator	Single	1
1.4	Authenticator	Single	1
1.5	Authenticator	Single	1
1.6	Authenticator	Single	1
1.7	Authenticator	Single	1
1.8	Authenticator	Single	1

Figure 47. SHOW PORTACCESS|PORTAUTH Command

### **Examples**

The following command displays the 802.1x authenticator ports:

```
show portaccess=8021x
```

The following command displays the MAC address-based authenticator ports:

```
show portaccess=macbased
```



## SHOW PORTACCESS|PORTAUTH PORT

---

### Syntax

```
show portaccess|portauth=8021x|macbased port=port
authenticator|supplicant [config] [status]
```

### Parameters

portaccess <b>or</b> portauth	Specifies the authenticator method of the port. Options are:				
	<table> <tr> <td>8021x</td><td>Displays information for an 802.1x authenticator port.</td></tr> <tr> <td>macbased</td><td>Displays information for a MAC address-based authenticator port.</td></tr> </table>	8021x	Displays information for an 802.1x authenticator port.	macbased	Displays information for a MAC address-based authenticator port.
8021x	Displays information for an 802.1x authenticator port.				
macbased	Displays information for a MAC address-based authenticator port.				
port	Specifies the port whose port-based access control settings you want to view. You can specify more than one port at a time. Port numbers are specified in the following format:  module ID.port number  For instructions, refer to “Port Numbers in Commands” on page 42.				
authenticator	Indicates that the port is an authenticator.				
supplicant	Indicates that the port is a supplicant.				
config	Displays the port-based access control settings for the port. Omitting this option and the STATUS option displays information on both.				
status	Displays the status and role of the port. Omitting this option and the CONFIG option displays information on both.				

### Description

This command displays information about authenticator and supplicant ports.

Figure 48 illustrates the information displayed by this command for an authenticator port. For an explanation of the parameters, refer to “SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR” on page 426.

```

Port 1

PAE Type..... Authenticator
Supplicant Mode..... Single
AuthControlPortControl.... Auto
quietPeriod..... 60
txPeriod..... 30
suppTimeout..... 30
serverTimeout..... 30
maxReq..... 2
reAuthPeriod..... 3600
reAuthEnabled..... Enabled
vlanAssignment..... Enabled
secureVlan..... On
guestVlan..... None (VID=0)
adminControlDirection..... Both
piggyBack..... Disabled

Attached Supplicant(s)
MAC Address..... -
    Authenticator PAE State..... Connecting
    Port Status..... Unauthorized
    Backend Authenticator State..... Initialize

```

Figure 48. Authenticator Port Information

Figure 49 illustrates the information displayed for a supplicant port. For an explanation of the parameters, refer to “SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT” on page 435.

```

Port 5

PAE Type..... Supplicant
heldPeriod..... 60
authPeriod..... 30
startPeriod..... 30
maxStart..... 3
Supplicant PAE State..... Connecting

```

Figure 49. Supplicant Port Information

## Examples

The following command displays the configuration and status for port 1.10, which is an 802.1x authenticator port:

```
show portaccess=8021x port=1.10 authenticator
```

The following command displays the configuration and status for port 3.12 which is a MAC address-based authenticator port:

```
show portaccess=8021x=macbased port=3.12 authenticator
```

This command displays the port access configuration of port 4.17, which is a supplicant port:

```
show portaccess port=4.17 supplicant
```

## SHOW RADIUSACCOUNTING

---

### Syntax

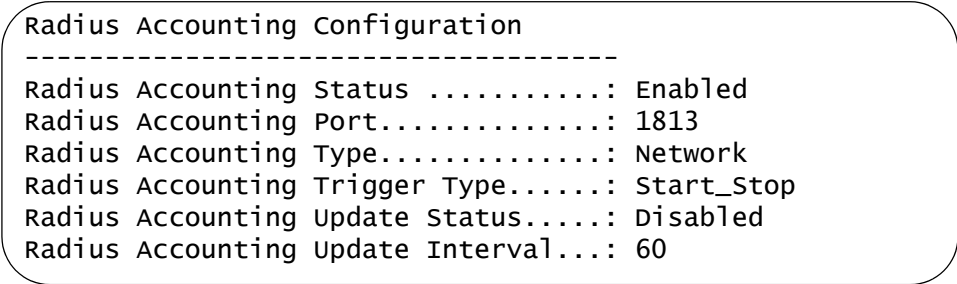
```
show radiusaccounting
```

### Parameters

None.

### Description

This command displays the current parameter settings for RADIUS accounting, which sends updates of supplicant activity on the switch's authenticator ports to the RADIUS server. Figure 50 is an example of the information displayed by this command.



```
Radius Accounting Configuration
-----
Radius Accounting Status .....: Enabled
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 50. SHOW RADIUSACCOUNTING Command

The information displayed by this command is described here:

- ❑ Radius Accounting Status - Specifies the status of RADIUS accounting on the switch. A status of Enabled means that the switch is sending supplicant updates to the RADIUS server; A status of Disabled means that the feature is not activated. The default is disabled.
- ❑ Radius Accounting Port - Specifies the UDP port for RADIUS accounting. The default is port 1813.
- ❑ Radius Accounting Type - Specifies the type of RADIUS accounting. The only possible setting is Network.
- ❑ Radius Accounting Trigger Type - Specifies the action that causes the switch to send accounting information to the RADIUS server. An action of Start\_Stop sends accounting information whenever a client logs on or logs off the network. This is the default. An action of Stop\_Only sends accounting information only when a client logs off.
- ❑ Radius Accounting Update Status - Specifies whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled.

- ❑ Radius Accounting Update Interval - Specifies the interval at which the switch sends interim accounting updates to the RADIUS server. The default is 60 seconds.

**Example**

The following command displays the current parameter settings for RADIUS accounting:

```
show radiusaccounting
```



# RADIUS Commands

---

This chapter contains the following commands:

- ❑ “ADD RADIUSSERVER” on page 448
- ❑ “DELETE RADIUSSERVER” on page 450
- ❑ “PURGE AUTHENTICATION” on page 451
- ❑ “SET AUTHENTICATION” on page 452
- ❑ “SHOW AUTHENTICATION” on page 453

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

**Note**

In Version 3.2.0 of the AT-S63 Management Software, stacks support the RADIUS protocol only for 802.1x port-based network access control. Stacks do not support RADIUS or TACACS+ manager accounts.

---

---

**Note**

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## ADD RADIUSSERVER

---

### Syntax

```
add radiusserver server|ipaddress=ipaddress order=value
[secret=string] [port=value] [accport=value]
```

### Parameters

server <b>or</b> ipaddress	Specifies an IP address of a RADIUS server. The parameters are equivalent.
order	Specifies the order that the RADIUS servers are queried by the stack. This value can be from 1 to 3. The servers are queried starting with 1.
secret	Specifies the encryption key used for this server. The maximum length is 39 characters.
port	Specifies the UDP (User Datagram Protocol) port of the RADIUS server. The default is port 1812.
accport	Specifies the UDP port for RADIUS accounting. The default is port 1813.

### Description

This command specifies the IP addresses of the RADIUS servers and the order they are to be queried by the stack. There can be up to three servers, but you can specify only one at a time with this command. You may specify an encryption key, a RADIUS UDP port, and a RADIUS accounting UDP port.

---

#### Note

The stack must have a routing interface on the local subnet where the authentication server is a member. The stack uses the IP address of the interface as its source address when sending packets to the server. For instructions on how to add a routing interface to the stack, refer to “ADD IP INTERFACE” on page 392.

---

### Examples

The following command adds a RADIUS server with the 149.245.22.22 IP address and specifies it as the first server in the list:

```
add radiusserver ipaddress=149.245.22.22 order=1
```



The following command adds the RADIUS server with the IP address 149.245.22.22. In addition, it specifies the server as the third RADIUS server to be queried by the stack and has a UDP port of 3:

```
add radiusserver ipaddress=149.245.22.22 order=3 port=3
```

The following command adds a RADIUS server with an IP address of 149.245.22.22. It specifies the order is 2, the encryption key is tiger74, and the UDP port is 1811:

```
add radiusserver ipaddress=149.245.22.22 order=2  
secret=tiger74 port=1811
```

## DELETE RADIUSSERVER

---

### Syntax

```
delete radiusserver server|ipaddress=ipaddress
```

### Parameter

server <b>or</b> ipaddress	Specifies the IP address of a RADIUS server to be deleted from the management software. The parameters are equivalent.
-------------------------------	--

### Description

This command deletes the IP address of a RADIUS from your stack.

### Example

The following command deletes the RADIUS server with the IP address 149.245.22.22:

```
delete radiusserver ipaddress=149.245.22.22
```

## PURGE AUTHENTICATION

---

### Syntax

```
purge authentication
```

### Parameters

None.

### Description

This command disables authentication, returns the authentication method to TACACS+, deletes any global secret, and returns the timeout value to its default setting of 10 seconds. This command does not delete the IP address or secret of any RADIUS or TACACS+ authentication servers you may have specified.

### Example

The following command returns the authentication settings to their default values:

```
purge authentication
```

## SET AUTHENTICATION

---

### Syntax

```
set authentication method=radius [secret=string]  
[timeout=value]
```

### Parameters

method	Specifies the active authenticator protocol on the stack. Stacks only support RADIUS.
secret	Specifies the global encryption key of the RADIUS servers. If the servers use different encryption keys, you can leave this parameter blank and set individual encryption keys with “ADD RADIUSSERVER” on page 448. To remove a previously assigned global key without specifying a new value, enter the string as “none”. The maximum length is 39 characters.
timeout	Specifies the maximum amount of time the stack waits for a response from an authentication server before the stack assumes the server will not respond. If the timeout expires and the server has not responded, the stack queries the next server in the list. The default is 30 seconds. The range is 1 to 300 seconds.

### Description

This command designates the active authentication protocol on the stack. Stacks support only the RADIUS protocol. You may specify a global encryption code and the maximum number of seconds the stack waits for a response from an authenticator server.

### Examples

The following command selects RADIUS as the authentication protocol with a global encryption key of leopard09 and a timeout of 15 seconds:

```
set authentication method=radius secret=leopard09 timeout=15
```

The following command removes the current global secret from the RADIUS client without assigning a new value:

```
set authentication method=radius secret=none
```

## SHOW AUTHENTICATION

---

### Syntax

```
show authentication[=radius]
```

### Parameters

None.

### Description

This command displays the following information about the RADIUS authentication protocol on the stack:

- ☐ Status - The status of your authenticated protocol: enabled or disabled.
- ☐ Authentication Method - The authentication protocol activated on your stack.
- ☐ The IP addresses of up to three authentication servers.
- ☐ The server encryption keys, if defined.
- ☐ TAC global secret - The global encryption code that applies to all authentication servers.
- ☐ Timeout - The length of the time, in seconds, before the stack assumes the server will not respond.

Entering the command without specifying RADIUS displays the current status of the authentication feature and the specifics of the currently selected authentication protocol. Specifying RADIUS in the command displays the specifics for that authentication protocol.

### Example

The following command displays authentication protocol information on your stack:

```
show authentication
```

The following command displays the information for the RADIUS protocol:

```
show authentication=radius
```



## Section IX

# Management Security

---

This section contains the following chapter:

- ❑ Chapter 25, “Web Server Commands” on page 457





## Chapter 25

# Web Server Commands

---

This chapter contains the following commands:

- ❑ “DISABLE HTTP SERVER” on page 458
- ❑ “ENABLE HTTP SERVER” on page 459
- ❑ “PURGE HTTP SERVER” on page 460
- ❑ “SHOW HTTP SERVER” on page 461

---

**Note**

Remember to save your changes with the SAVE CONFIGURATION command.

---

---

**Note**

For overview information on this feature, refer to the *AT-S63 Management Software Features Guide*.

---

## DISABLE HTTP SERVER

---

### Syntax

```
disable http server
```

### Parameters

None.

### Description

This command disables the web server on the stack. When the server is disabled, you cannot manage the stack from a web browser. To view the current status of the web server, see “SHOW HTTP SERVER” on page 461. The default setting for the web server is enabled.

### Example

The following command disables the web server:

```
disable http server
```

## ENABLE HTTP SERVER

---

### Syntax

```
enable http server
```

### Parameters

None.

### Description

This command activates the web server on the stack. Activating the server allows you to manage the unit from a web browser. To view the current status of the web server, see “SHOW HTTP SERVER” on page 461. The default setting for the web server is enabled.

### Example

The following command activates the web server:

```
enable http server
```

## PURGE HTTP SERVER

---

### Syntax

```
purge http server
```

### Parameters

None.

### Description

This command resets the HTTP server to its default values, as specified in Appendix A, “AT-S63 Default Settings” in the *AT-S63 Management Software Menus Interface User’s Guide*. To view the current web server settings, refer to “SHOW HTTP SERVER” on page 461.

### Example

The following command resets the web server parameters to their default values:

```
purge http server
```

## SHOW HTTP SERVER

---

### Syntax

```
show http server
```

### Parameters

None.

### Description

This command displays the following information about the web server on the stack:

- ☐ Status
- ☐ SSL security
- ☐ SSL key ID
- ☐ Listen port

SSL security and key ID are not supported in a stack.

### Example

The following command displays the status of the web server:

```
show http server
```



# Index

---

## Numerics

- 802.1x Port-based Network Access Control 437
  - authenticator port
    - configuring 426
    - displaying 439
  - disabling 422
  - displaying 439, 441
  - enabling 424
  - supplicant port
    - configuring 435
    - displaying 439

## A

- access control
  - authenticator port, displaying 439
  - supplicant port, displaying 439
- ACTIVATE RSTP command 358
- ACTIVATE STP command 344
- ADD IP ARP command 390
- ADD IP INTERFACE command 392
- ADD IP ROUTE command 394
- ADD LACP PORT command 176
- ADD LOG OUTPUT command 236
- ADD RADIUS SERVER command 448
- ADD SNMP COMMUNITY command 104
- ADD SNMPV3 USER command 285, 328
- ADD SWITCH FDB/FILTER command 152
- ADD SWITCH TRUNK command 166
- ADD VLAN command 374
- Address Resolution Protocol (ARP)
  - adding entries 390
  - deleting entries 396
  - displaying entries 408
  - modifying entries 400
  - setting cache timeout 402
- aging timer 157
- AT-S63 software image
  - downloading 216, 218, 223
  - uploading 227, 229, 232
- AT-S63 software, resetting to factory defaults 81
- AT-StackXG Stacking Module 29
- authentication
  - displaying 453
  - protocol, selecting 452
  - resetting to defaults 451
- authentication failure traps
  - disabling 113
  - displaying 120
  - enabling 116

- authenticator port
  - configuring 426
  - displaying 439, 441

## B

- back pressure 130
- boot configuration file names, displaying 212
- BPDU 363
- bridge forwarding delay 348, 362
- bridge hello time 348, 362
- bridge max age 348, 362
- bridge priority 348
- broadcast filter 130

## C

- Class of Service. *See* CoS
- CLEAR SCREEN command 62
- command line prompt 67
- commands, formatting 58
- compact flash card
  - configuration file on 209
  - copying files 201
  - directory, selecting 208
  - displaying files 213
  - files on 211
  - renaming files 206
  - space available 211
- configuration file
  - creating 203
  - described 36
  - downloading 218, 223
  - name 212
  - setting 209
  - uploading 229, 232
- console timeout 88
- console timer, setting 88
- contact name, configuring 80, 89
- COPY command 201
- CREATE CONFIG command 203
- CREATE LACP AGGREGATOR command 178
- CREATE LOG OUTPUT command 238
- CREATE SNMP COMMUNITY command 106
- CREATE SNMPV3 ACCESS command 287
- CREATE SNMPV3 COMMUNITY command 290
- CREATE SNMPV3 GROUP command 292
- CREATE SNMPV3 NOTIFY command 294
- CREATE SNMPV3 TARGETADDR command 296
- CREATE SNMPV3 TARGETPARAMS command 298
- CREATE SNMPV3 VIEW command 300

CREATE SWITCH TRUNK command 168  
CREATE VLAN command 376

## D

default route  
  adding 394  
  deleting 398  
  displaying 414  
  modifying 406  
DELETE FILE command 204  
DELETE IP ARP command 396  
DELETE IP INTERFACE command 397  
DELETE IP ROUTE command 398  
DELETE LACP PORT command 180  
DELETE RADIUS SERVER command 450  
DELETE SNMP COMMUNITY command 109  
DELETE SNMPV3 USER command 302  
DELETE SWITCH FDB|FILTER command 154  
DELETE SWITCH TRUNK command 170  
DELETE VLAN command 379  
destination port 192  
DESTROY LACP AGGREGATOR command 181  
DESTROY LOG OUTPUT command 242  
DESTROY SNMP COMMUNITY command 111  
DESTROY SNMPV3 ACCESS command 303  
DESTROY SNMPV3 COMMUNITY command 305  
DESTROY SNMPV3 GROUP command 306  
DESTROY SNMPV3 NOTIFY command 307  
DESTROY SNMPV3 TARGETADDR command 308  
DESTROY SNMPV3 TARGETPARAMS command 309  
DESTROY SNMPV3 VIEW command 310  
DESTROY SWITCH TRUNK command 171  
DESTROY VLAN command 382  
DISABLE HTTP SERVER command 458  
DISABLE IGMP SNOOPING command 270  
DISABLE LACP command 182  
DISABLE LOG command 243  
DISABLE LOG OUTPUT command 244  
DISABLE PORT ACCESS|PORT AUTH command 422  
DISABLE RADIUS ACCOUNTING command 423  
DISABLE RSTP command 359  
DISABLE SNMP AUTHENTICATED TRAP command 113  
DISABLE SNMP command 112  
DISABLE SNMP COMMUNITY command 114  
DISABLE STP command 345  
DISABLE SWITCH PORT command 124  
DISABLE SWITCH PORT FLOW command 125  
DISABLE TELNET command 76  
discovery process  
  described 34  
  troubleshooting 48  
distinguished name  
  displaying 100  
document conventions 19  
dynamic module ID numbers  
  described 38  
  displaying 72  
  setting 70

## E

edge port 365  
ENABLE HTTP SERVER command 459  
ENABLE IGMP SNOOPING command 271  
ENABLE LACP command 183  
ENABLE LOG command 245  
ENABLE LOG OUTPUT command 246  
ENABLE PORT ACCESS|PORT AUTH command 424  
ENABLE RADIUS ACCOUNTING command 425  
ENABLE RSTP command 360  
ENABLE SNMP AUTHENTICATED TRAP command 116  
ENABLE SNMP command 115  
ENABLE SNMP COMMUNITY command 117  
ENABLE STP command 346  
ENABLE SWITCH PORT command 126  
ENABLE SWITCH PORT FLOW command 127  
ENABLE TELNET command 77  
enhanced stacking 31  
event log  
  configuring 250  
  disabling 243  
  displaying 254, 261  
  enabling 245  
  resetting to defaults 247  
  saving 248  
EXIT command 63

## F

factory defaults 81  
files  
  copying 201  
  deleting 204  
  displaying file list 213  
  downloading 218, 223  
  renaming 206  
  uploading 229, 232  
flash memory  
  configuration file in 209  
  copying files 201  
  displaying files 213  
  files in 214  
  formatting 205  
  renaming files 206  
  space available in 214  
flow control  
  disabling 125  
  enabling 127, 130  
force version 362  
FORMAT DEVICE command 205  
forwarding delay 348, 362

## H

head of line blocking 132  
hello time 348, 362  
help, context-sensitive 57  
HOL blocking 130  
HTTP server  
  disabling 458



- displaying 461
- enabling 459
- resetting to defaults 460

## I

- IGMP snooping
  - configuring 272
  - disabling 270
  - displaying 275, 277
  - enabling 271
- ingress filtering 383
- IP address, stack 44

## K

- keyword abbreviations 57

## L

- LACP
  - disabling 182, 187
  - displaying status 188
  - enabling 183, 187
- LACP aggregator
  - adding ports 176
  - changing adminkey 184
  - changing load distribution method 184
  - creating 178
  - deleting ports 180
  - destroying 181
  - displaying status 188
  - setting system priority 186
- LOAD METHOD=LOCAL command 216
- LOAD METHOD=TFTP command 218
- LOAD METHOD=XMODEM command 223
- local interface
  - displaying 412
  - specifying 405
- local management session
  - quitting 56
  - starting 52
- location, configuring 80, 89
- log output
  - adding 236
  - creating 238
  - destroying 242
  - disabling 244
  - displaying 259
  - enabling 246
  - modifying 251
- LOGOFF command 65
- LOGOUT command 65

## M

- MAC address aging timer 157
- MAC address table
  - addresses
    - adding 152
    - deleting 154, 156
    - displaying 159
  - aging time 157

- multicast groups 272
- MAC addresses
  - adding 152
  - deleting 154, 156
- manager password, setting 86, 92
- master switch 35
- max age 348, 362
- Mcheck 365
- MDI mode 130
- member switches 35
- migration check 365
- module ID numbers
  - described 38
  - displaying 72
  - setting 70
- multicast router port 272

## N

- NULL character 90, 98

## O

- operator password, setting 87, 92

## P

- packet filtering 134
- password, default 53
- PING command 78
- PKI certificates
  - downloading 218, 223
  - uploading 229, 232
- point-to-point port 365
- port
  - back pressure
    - disabling 132
    - enabling 132
  - back pressure, limit 132
  - broadcast filter 132
  - configuring 130
  - cost 351, 365
  - description, setting 130
  - disabling 124
  - displaying parameters 140
  - enabling 126
  - flow control
    - disabling 125
    - enabling 127
  - head of line blocking 132
  - negotiation 130
  - packet filtering 134
  - priority 351, 365
  - rate limit 137
  - resetting 129, 132
  - speed, setting 130
  - statistics counter
    - displaying 150
    - resetting 146
  - status, specifying 130

- port mirror
  - described 192
  - destination port 192
  - destination port, setting 193
  - displaying 195
  - setting 194
  - source port 192
- port trunk
  - adding 166
  - creating 168
  - deleting 170
  - destroying 171
  - displaying 173
  - load distribution 172
  - setting 172
  - speed, setting 172
- port-based access control
  - authenticator port, configuring 426
  - disabling 422
  - displaying 439, 441
  - enabling 424
  - RADIUS accounting 437
  - supplicant port, configuring 435
- port-based VLAN
  - adding ports 374
  - creating 376
  - deleting ports 379
  - destroying 382
  - displaying 385
- protected ports VLANs
  - changing port type 384
- PURGE AUTHENTICATION command 451
- PURGE HTTP SERVER command 460
- PURGE IP INTERFACE command 399
- PURGE LOG command 247
- PURGE RSTP command 361
- PURGE SNMPV3 ACCESS command 311
- PURGE SNMPV3 COMMUNITY command 312
- PURGE SNMPV3 NOTIFY command 313
- PURGE SNMPV3 TARGETADDR command 314
- PURGE SNMPV3 VIEW command 315
- PURGE STP command 347
- PURGE SWITCH PORT command 128

## Q

- QUIT command 65

## R

- RADIUS accounting
  - configuring 437
  - disabling 423
  - displaying 444
  - enabling 425
- RADIUS server
  - adding 448
  - deleting 450
- rate limiting 137
- remote management session
  - starting 54

- RENAME command 206
- RESET SWITCH command 79
- RESET SWITCH FDB command 156
- RESET SWITCH PORT command 129
- RESET SWITCH PORT COUNTER command 146
- RESET SYSTEM command 80
- RESTART REBOOT command 81
- RESTART SWITCH command 82
- Routing Information Protocol (RIP)
  - displaying routes 414
- routing interfaces
  - creating 392
  - deleting 397
  - deleting all 399
  - displaying 412
  - displaying routes 414
  - modifying 403
- RSTP
  - activating 358
  - disabling 359
  - displaying 368
  - enabling 360
  - port, setting 365
  - resetting to defaults 361
  - setting 362

## S

- SAVE CONFIGURATION command 66
- SAVE LOG command 248
- serial terminal port
  - settings, displaying 93
  - speed, setting 84
- SET ASYN command 84
- SET AUTHENTICATION command 452
- SET CONFIG command 209
- SET DATE TIME command 85, 91
- SET IP ARP command 400
- SET IP ARP TIMEOUT command 402
- SET IP IGMP command 272
- SET IP INTERFACE command 403
- SET IP LOCAL INTERFACE command 405
- SET IP ROUTE command 406
- SET LACP AGGREGATOR command 184
- SET LACP STATE command 187
- SET LACP SYSPRIORITY command 186
- SET LOG FULLACTION command 250
- SET LOG OUTPUT command 251
- SET MANAGER OPERATOR command 92
- SET PASSWORD MANAGER command 86
- SET PASSWORD OPERATOR command 87, 92
- SET PORTACCESS|PORT AUTH PORT AUTHENTICATOR command 426
- SET PORTACCESS|PORT AUTH PORT SUPPLICANT command 435
- SET PROMPT command 67
- SET RADIUSACCOUNTING command 437
- SET RSTP command 362
- SET RSTP PORT command 365
- SET SNMP COMMUNITY command 118

SET SNMPV3 ACCESS command 316  
 SET SNMPV3 COMMUNITY command 318  
 SET SNMPV3 GROUP command 320  
 SET SNMPV3 NOTIFY command 322  
 SET SNMPV3 TARGETADDR command 324  
 SET SNMPV3 TARGETPARAMS command 326  
 SET SNMPV3 VIEW command 330  
 SET STACK command 70  
 SET STP command 348  
 SET STP PORT command 351  
 SET SWITCH AGINGTIMER|AGEINGTIMER command 157  
 SET SWITCH CONSOLETIMER command 88  
 SET SWITCH INFILTERING command 383  
 SET SWITCH MIRROR command 193  
 SET SWITCH MULTICASTMODE command 353  
 SET SWITCH PORT command 130  
 SET SWITCH PORT FILTERING command 134  
 SET SWITCH PORT MIRROR command 194  
 SET SWITCH PORT PRIORITY OVERRIDEPRIORITY command 264  
 SET SWITCH PORT RATELIMITING command 137  
 SET SWITCH TRUNK command 172  
 SET SYSTEM command 89  
 SET TELNET INSERTNULL command 90  
 SET VLAN command 384  
 SHOW ASYN command 93  
 SHOW AUTHENTICATION command 453  
 SHOW CONFIG command 212  
 SHOW CONFIG DYNAMIC command 94  
 SHOW CONFIG INFO command 96  
 SHOW FILE command 213  
 SHOW HTTP SERVER command 461  
 SHOW IGMP Snooping command 275  
 SHOW IP ARP command 408  
 SHOW IP COUNTER command 410  
 SHOW IP IGMP command 277  
 SHOW IP INTERFACE command 412  
 SHOW IP ROUTE command 414  
 SHOW LACP command 188  
 SHOW LOG command 254  
 SHOW LOG OUTPUT command 259  
 SHOW LOG STATUS command 261  
 SHOW PORTACCESS|PORTAUTH command 439  
 SHOW PORTACCESS|PORTAUTH PORT command 441  
 SHOW RADIUSACCOUNTING command 444  
 SHOW RSTP command 368  
 SHOW SNMP command 120  
 SHOW SNMPV3 ACCESS command 332  
 SHOW SNMPV3 COMMUNITY command 333  
 SHOW SNMPV3 GROUP command 334  
 SHOW SNMPV3 NOTIFY command 335  
 SHOW SNMPV3 TARGETADDR command 336  
 SHOW SNMPV3 TARGETPARAMS command 337  
 SHOW SNMPV3 USER command 338  
 SHOW SNMPV3 VIEW command 339  
 SHOW STACK command 72  
 SHOW STP command 355  
 SHOW SWITCH AGINGTIMER|AGEINGTIMER command 158  
 SHOW SWITCH command 97  
 SHOW SWITCH FDB command 159  
 SHOW SWITCH MIRROR command 195  
 SHOW SWITCH MODULE COUNTER command 147  
 SHOW SWITCH PORT command 140  
 SHOW SWITCH PORT COUNTER command 150  
 SHOW SWITCH TRUNK command 173  
 SHOW SYSTEM command 100  
 SHOW TIME command 102  
 SHOW USER command 68  
 SHOW VLAN command 385  
 SNMP  
     disabling 112  
     information, displaying 120  
 SNMP community  
     adding 104  
     creating 106  
     deleting 109  
     destroying 111  
     disabling 114  
     enabling 115, 117  
     modifying 118  
 SNMP management access 104  
 SNMPv3 Access Table entry  
     creating 287  
     deleting 303  
     modifying 316  
 SNMPv3 Community Table entry  
     creating 290  
     deleting 305  
     modifying 318  
 SNMPv3 Notify Table entry  
     creating 294  
     deleting 307  
     modifying 322  
 SNMPv3 SecurityToGroup Table entry  
     creating 292  
     deleting 306  
     modifying 320  
 SNMPv3 Target Address Table entry  
     creating 296  
     deleting 308  
     modifying 324  
 SNMPv3 Target Parameters Table entry  
     creating 298  
     deleting 309  
     displaying 337  
     modifying 326  
 SNMPv3 User Table entry  
     adding 285  
     deleting 302  
     displaying 338  
 SNMPv3 View Table entry  
     creating 300  
     deleting 310  
     displaying 339  
     source port 192

- stacking
  - maximum number of switches 30
  - topology 32
- static module ID numbers
  - described 38
  - displaying 72
  - setting 70
- static multicast address 152
- static port trunk
  - described 164
- static routes
  - adding 394
  - deleting 398
  - displaying 414
  - modifying 406
- static unicast address 152
- STP
  - activating 344
  - disabling 345
  - displaying 355
  - enabling 346
  - port, setting 351
  - resetting values to defaults 347
  - setting 348
- supplicant port
  - configuring 435
  - displaying 439, 441
- switch
  - configuration, displaying 94, 96, 212
  - distinguished name 100
  - information, displaying 100
  - parameters, displaying 97
  - restarting 82
  - statistics counters, displaying 147
- system date
  - displaying 102
  - setting 85, 91
- system files
  - downloading 218, 223
  - uploading 229, 232
- system name, configuring 80, 89
- system time
  - displaying 102
  - setting 85, 91

## T

- tagged VLAN
  - adding ports 374
  - creating 376
  - deleting ports 379
  - destroying 382
  - displaying 385
- Telnet server
  - disabling 76
  - enabling 77
- temperature, switch, displaying 100
- trap receiver 104

## U

- UPLOAD METHOD=LOCAL command 227
- UPLOAD METHOD=TFTP command 229
- UPLOAD METHOD=XMODEM command 232
- uploading files 229, 232

## V

- VLAN. *See* port-based VLAN and tagged VLAN